Padrões

Recomendações da AWS



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

Recomendações da AWS: Padrões

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

AWS Padrões de orientação prescritiva 1
Fundamentos da nuvem 3
Automatize a criação de contas usando o Landing Zone Accelerator em AWS 4
Resumo 4
Pré-requisitos e limitações 4
Arquitetura 5
Ferramentas 6
Práticas recomendadas 9
Épicos 9
Recursos relacionados 35
Mais informações 36
Inventário automático de AWS recursos 38
Resumo 38
Pré-requisitos e limitações 39
Arquitetura 40
Ferramentas 40
Práticas recomendadas 42
Épicos 42
Solução de problemas 49
Recursos relacionados 50
Configure os logs de fluxo da VPC em todas as contas 51
Resumo 51
Pré-requisitos e limitações 51
Arquitetura 52
Ferramentas 53
Práticas recomendadas 53
Épicos 55
Recursos relacionados 57
Mais informações 57
Marque anexo do gateway de trânsito automaticamente 59
Resumo 59
Pré-requisitos e limitações 59
Arquitetura 59
Ferramentas 61

Épicos 62
Recursos relacionados 69
Mais padrões 70
IA e aprendizado de máquina 71
Dados agregados do DynamoDB para previsão de ML no Athena 73
Resumo 73
Pré-requisitos e limitações 73
Arquitetura 73
Ferramentas 74
Épicos 76
Recursos relacionados 86
Associe um AWS CodeCommit repositório ao Amazon SageMaker AI Studio Classic em todas as contas 87
Resumo 87
Pré-requisitos e limitações 87
Arquitetura 87
Ferramentas 88
Épicos 89
Mais informações 95
Extraia automaticamente conteúdo de arquivos PDF 97
Resumo 97
Pré-requisitos e limitações 97
Arquitetura 98
Ferramentas 99
Épicos 100
Recursos relacionados 105
Anexos 105
Crie um modelo de previsão de inicialização a frio usando o SageMaker AI DeepAR 106
Resumo 106
Pré-requisitos e limitações 106
Arquitetura 107
Ferramentas 108
Práticas recomendadas 109
Épicos 109
Recursos relacionados 111
Crie um MLOps fluxo de trabalho usando SageMaker IA e Azure DevOps 112

Resumo 112
Pré-requisitos e limitações 112
Arquitetura 113
Ferramentas 115
Práticas recomendadas 116
Épicos 117
Solução de problemas 126
Recursos relacionados 127
Configure o registro no Amazon Bedrock usando CloudFormation 129
Resumo 129
Pré-requisitos e limitações 129
Arquitetura 130
Ferramentas 131
Épicos 132
Recursos relacionados 134
Crie contêineres Docker SageMaker para treinamento de modelos em Step Functions 136
Resumo 136
Pré-requisitos e limitações 136
Arquitetura 137
Ferramentas 137
Épicos 138
Recursos relacionados 152
Crie controles de acesso no Amazon EKS com agentes do Amazon Bedrock 153
Resumo 153
Pré-requisitos e limitações 153
Arquitetura 154
Ferramentas 155
Práticas recomendadas 156
Épicos 156
Solução de problemas 175
Recursos relacionados 175
Implemente um caso de uso do RAG em AWS 177
Resumo 177
Pré-requisitos e limitações 177
Arquitetura 178
Ferramentas 180

Práticas recomendadas 181
Épicos 182
Recursos relacionados 185
Mais informações 186
Implemente vários objetos de modelo de pipeline em um único SageMaker endpoint 188
Resumo 188
Pré-requisitos e limitações 188
Arquitetura 189
Ferramentas 189
Épicos 190
Recursos relacionados 200
Desenvolva assistentes baseados em bate-papo com IA usando RAG e prompting ReAct 201
Resumo 201
Pré-requisitos e limitações 202
Arquitetura 203
Ferramentas 204
Práticas recomendadas 206
Épicos 207
Solução de problemas 214
Recursos relacionados 214
Mais informações 215
Desenvolva um assistente baseado em bate-papo usando o Amazon Bedrock 216
Resumo 216
Pré-requisitos e limitações 217
Arquitetura 217
Ferramentas 218
Práticas recomendadas 220
Épicos 221
Recursos relacionados 225
Mais informações 226
Documente o conhecimento institucional a partir de entradas de voz 228
Resumo 228
Pré-requisitos e limitações 228
Arquitetura 229
Ferramentas 230
Práticas recomendadas 232

Épicos 232
Recursos relacionados 238
Gere recomendações personalizadas usando o Amazon Personalize 240
Resumo 240
Pré-requisitos e limitações 240
Arquitetura 240
Ferramentas 242
Épicos 243
Recursos relacionados 245
Mais informações 246
Simplifique os fluxos de trabalho de ML usando SageMaker IA e Hydra 250
Resumo 250
Pré-requisitos e limitações 250
Arquitetura 251
Ferramentas 252
Práticas recomendadas 253
Épicos 254
Solução de problemas 261
Recursos relacionados 261
Mais informações 261
Treinar e implantar um modelo de ML personalizado compatível com GPU 263
Resumo 263
Pré-requisitos e limitações 263
Arquitetura 264
Ferramentas 264
Épicos 264
Recursos relacionados 281
Mais informações 281
..... 284
Resumo 284
Pré-requisitos e limitações 285
Arquitetura 288
Ferramentas 290
Práticas recomendadas 291
Épicos 291
Recursos relacionados 298

Mais informações 299
Use o Amazon Q Developer como assistente de codificação 304
Resumo 304
Pré-requisitos e limitações 304
Ferramentas 305
Práticas recomendadas 305
Épicos 306
Solução de problemas 314
Recursos relacionados 314
Use o SageMaker processamento para engenharia de recursos distribuídos de conjuntos de dados de ML em escala de terabytes 315
Resumo 315
Pré-requisitos e limitações 315
Arquitetura 316
Ferramentas 319
Épicos 319
Recursos relacionados 332
Anexos 333
Visualize os resultados do modelo de IA/ML usando o Flask e o AWS Elastic Beanstalk 334
Resumo 334
Pré-requisitos e limitações 334
Arquitetura 335
Ferramentas 337
Épicos 337
Recursos relacionados 348
Mais informações 348
Mais padrões 353
Analytics 354
Analisar dados do Amazon Redshift no Microsoft SQL Server Analysis Services 356
Resumo 356
Pré-requisitos e limitações 356
Arquitetura 356
Ferramentas 357
Épicos 357
Recursos relacionados 359
..... 360

Resumo 360
Pré-requisitos e limitações 360
Arquitetura 361
Ferramentas 361
Épicos 362
Recursos relacionados 367
Automatize a ingestão de dados a partir do Amazon AWS Data Exchange S3 368
Resumo 368
Pré-requisitos e limitações 368
Arquitetura 368
Ferramentas 369
Épicos 370
Recursos relacionados 372
Anexos 372
Automatize a aplicação da criptografia no AWS Glue 373
Resumo 373
Pré-requisitos e limitações 373
Arquitetura 373
Ferramentas 374
Práticas recomendadas 375
Épicos 375
Recursos relacionados 378
Crie um pipeline de dados para processar dados do Google Analytics usando o AWS DataOps Development Kit 379
Resumo 379
Pré-requisitos e limitações 379
Arquitetura 379
Ferramentas 380
Épicos 381
Solução de problemas 383
Recursos relacionados 384
Mais informações 384
Crie um pipeline de processamento de vídeo 387
Resumo 387
Pré-requisitos e limitações 387
Arquitetura 388

Ferramentas ... 388
Épicos ... 389
Recursos relacionados ... 397
Mais informações ... 398
Anexos ... 398
Crie um pipeline de ETL do Amazon S3 para o Amazon Redshift usando o AWS Glue ... 399
Resumo ... 399
Pré-requisitos e limitações ... 399
Arquitetura ... 400
Ferramentas ... 400
Épicos ... 401
Recursos relacionados ... 409
Mais informações ... 409
Crie uma malha de dados corporativa com a Amazon DataZone ... 411
Resumo ... 411
Pré-requisitos e limitações ... 411
Arquitetura ... 412
Ferramentas ... 413
Épicos ... 414
Recursos relacionados ... 427
Mais informações ... 428
Calcule o value at risk (VaR – valor em risco) usando os serviços da AWS ... 430
Resumo ... 430
Pré-requisitos e limitações ... 431
Arquitetura ... 431
Ferramentas ... 432
Práticas recomendadas ... 433
Épicos ... 434
Recursos relacionados ... 437
Configurar o acesso entre contas para um Catálogo de Dados do AWS Glue compartilhado usando o Athena ... 438
Resumo ... 438
Pré-requisitos e limitações ... 438
Arquitetura ... 438
Ferramentas ... 440
Épicos ... 440

Recursos relacionados 453
Mais informações 453
Converta NORMALIZE em Amazon Redshift SQL 454
Resumo 454
Pré-requisitos e limitações 454
Arquitetura 454
Ferramentas 455
Épicos 460
Recursos relacionados 460
Converter o RESET WHEN para Amazon Redshift SQL 462
Resumo 462
Pré-requisitos e limitações 462
Arquitetura 462
Ferramentas 463
Épicos 467
Recursos relacionados 467
Implante e gerencie um data lake de tecnologia sem servidor na AWS 469
Resumo 469
Pré-requisitos e limitações 469
Arquitetura 470
Ferramentas 471
Épicos 472
Recursos relacionados 474
..... 476
Resumo 476
Pré-requisitos e limitações 476
Arquitetura 477
Ferramentas 477
Épicos 478
Recursos relacionados 481
Anexos 482
Garanta o registro do Amazon EMR no Amazon S3 483
Resumo 483
Pré-requisitos e limitações 484
Arquitetura 484
Ferramentas 485

Épicos 485
Recursos relacionados 488
Anexos 488
Gerar dados de teste usando o AWS Glue 489
Resumo 489
Pré-requisitos e limitações 489
Arquitetura 490
Ferramentas 490
Práticas recomendadas 490
Épicos 491
Recursos relacionados 502
Mais informações 503
Ingerir dados de IoT diretamente no Amazon S3 508
Resumo 508
Pré-requisitos e limitações 508
Arquitetura 509
Ferramentas 510
Práticas recomendadas 510
Épicos 511
Solução de problemas 519
Recursos relacionados 519
Mais informações 520
Executar uma tarefa do Spark no Amazon EMR usando uma função do Lambda 524
Resumo 524
Pré-requisitos e limitações 524
Arquitetura 525
Ferramentas 525
Épicos 526
Recursos relacionados 529
Mais informações 530
Anexos 532
Migre as cargas de trabalho do Apache Cassandra para o Amazon Keyspaces 533
Resumo 533
Pré-requisitos e limitações 533
Arquitetura 533
Ferramentas 534

Práticas recomendadas 535
Épicos 535
Solução de problemas 548
Recursos relacionados 548
Mais informações 548
Migre dados do Hadoop para o Amazon S3 usando o Migrator WANdisco LiveData 550
Resumo 550
Pré-requisitos e limitações 550
Arquitetura 551
Épicos 552
Recursos relacionados 557
Mais informações 558
Migrar o Oracle Business Intelligence 12c para a Nuvem AWS 559
Resumo 559
Pré-requisitos e limitações 559
Arquitetura 560
Ferramentas 561
Épicos 562
Recursos relacionados 576
Mais informações 577
Migre um cluster do Kafka para o Amazon MSK usando MirrorMaker 582
Resumo 582
Pré-requisitos e limitações 582
Arquitetura 583
Ferramentas 583
Práticas recomendadas 584
Épicos 584
Recursos relacionados 588
Mais informações 589
Migre uma pilha ELK para a Nuvem AWS 590
Resumo 590
Pré-requisitos e limitações 590
Arquitetura 592
Ferramentas 594
Épicos 595
Recursos relacionados 603

Mais informações 605
Migre dados para AWS usar o Starburst 606
Resumo 606
Pré-requisitos e limitações 606
Arquitetura 606
Ferramentas 608
Épicos 609
Recursos relacionados 612
Otimize a ingestão de ETL do tamanho do arquivo de entrada 613
Resumo 613
Pré-requisitos e limitações 613
Arquitetura 613
Ferramentas 614
Épicos 614
Recursos relacionados 617
Mais informações 618
Orquestre um pipeline de ETL com o AWS Step Functions 619
Resumo 619
Pré-requisitos e limitações 619
Arquitetura 620
Ferramentas 621
Épicos 622
Solução de problemas 630
Recursos relacionados 630
Mais informações 630
Execute análises de ML usando o Amazon Redshift ML 631
Resumo 631
Pré-requisitos e limitações 631
Arquitetura 632
Ferramentas 633
Épicos 634
Recursos relacionados 637
Consulte o Amazon DynamoDB usando o Amazon Athena 639
Resumo 639
Pré-requisitos e limitações 639
Arquitetura 640

Ferramentas ... 640
Épicos ... 641
Solução de problemas ... 644
Recursos relacionados ... 645
Consulte tabelas do DynamoDB usando o Athena ... 646
Resumo ... 646
Pré-requisitos e limitações ... 646
Arquitetura ... 647
Ferramentas ... 647
Épicos ... 648
Recursos relacionados ... 656
Mais informações ... 657
Configure um espaço de dados mínimo viável ... 658
Resumo ... 658
Pré-requisitos e limitações ... 659
Arquitetura ... 660
Ferramentas ... 661
Práticas recomendadas ... 662
Épicos ... 663
Solução de problemas ... 717
Recursos relacionados ... 717
Mais informações ... 717
Configure a classificação específica do idioma para os resultados da consulta do Amazon Redshift ... 723
Resumo ... 723
Pré-requisitos e limitações ... 723
Arquitetura ... 724
Ferramentas ... 724
Épicos ... 724
Recursos relacionados ... 729
Mais informações ... 729
Assine uma função do Lambda para receber notificações de eventos de buckets S3 entre regiões ... 733
Resumo ... 733
Pré-requisitos e limitações ... 733
Arquitetura ... 733

Ferramentas ... 734
Épicos ... 735
Recursos relacionados ... 738
Três tipos de trabalho de ETL do AWS Glue para converter dados ... 740
Resumo ... 740
Pré-requisitos e limitações ... 740
Arquitetura ... 740
Ferramentas ... 741
Épicos ... 742
Recursos relacionados ... 745
Mais informações ... 745
Anexos ... 751
Visualize os registros de auditoria do Amazon Redshift usando o Athena e QuickSight ... 752
Resumo ... 752
Pré-requisitos e limitações ... 752
Arquitetura ... 752
Ferramentas ... 753
Épicos ... 753
Recursos relacionados ... 758
Anexos ... 759
Visualize relatórios de credenciais do IAM usando a Amazon QuickSight ... 760
Resumo ... 760
Pré-requisitos e limitações ... 761
Arquitetura ... 761
Ferramentas ... 762
Épicos ... 763
Mais informações ... 769
Mais padrões ... 771
Computação ... 773
Contêineres e microsserviços ... 774
Acesse o Amazon Neptune a partir do Amazon EKS ... 776
Acesse aplicativos de contêineres no Amazon ECS ... 788
Acesse aplicativos de contêineres no Amazon ECS com um tipo de execução do AWS Fargate ... 805
Acesse aplicativos de contêineres de forma privada no Amazon EKS ... 820
Ativar mTLS no App Mesh do Amazon EKS ... 828

Automatize backups para instâncias de banco de dados do Amazon RDS para PostgreSQL. ... 836
Automatize a implantação do Manipulador do término do nó ... 849
Compilar e implantar automaticamente uma aplicação em Java no Amazon EKS ... 864
Crie uma definição de tarefa do Amazon ECS em EC2 instâncias usando o Amazon EFS ... 889
Implantar funções do Lambda com imagens de contêiner ... 896
Implante microsserviços Java no Amazon ECS usando o AWS Fargate ... 905
Implante pacotes Kubernetes usando o Amazon EKS e o Helm ... 912
Implante um microsserviço Java no Amazon EKS e o exponha com um Application Load Balancer ... 923
Implante um aplicativo em cluster no Amazon ECS usando o AWS Copilot ... 938
Implemente um aplicativo baseado em gRPC no Amazon EKS ... 949
Implantar e depure clusters do Amazon EKS ... 961
Implantar contêineres usando o Elastic Beanstalk ... 989
Gere um endereço IP de saída estático usando Lambda e Amazon VPC ... 995
Identifique automaticamente imagens duplicadas de contêineres ... 1010
Instale o SSM Agent nos nós de processamento do Amazon EKS ... 1040
Instale o agente SSM e o CloudWatch agente nos nós de trabalho do Amazon EKS usando preBootstrapCommands ... 1046
Migrar controladores de entrada NGINX para o modo automático EKS ... 1053
Migre cargas de trabalho de contêineres do ARO para o ROSA ... 1074
Otimize as imagens do Docker geradas ... 1090
Coloque os pods do Kubernetes em nós compatíveis no Amazon EKS ... 1100
Replique imagens filtradas de contêineres do Amazon ECR entre contas ou regiões ... 1117
Alternar as credenciais sem reiniciar os contêineres ... 1135
Execute tarefas do Amazon ECS na Amazon WorkSpaces ... 1141
Execute um contêiner do Docker da API web ASP.NET na AWS ... 1151
Executar workloads orientadas por mensagens usando o AWS Fargate ... 1163
Executar workloads monitoradas com armazenamento de dados persistente ... 1172
Configure o escalonamento automático usando o Amazon EKS Pod Identity e o KEDA ... 1197
... 1220
Use TLS mútuo no Amazon ECS com ALB ... 1243
Mais padrões ... 1273
Sem servidor ... 1275
Crie um aplicativo React Native usando o AWS Amplify ... 1276
Gerencie centralmente os locatários em vários produtos SaaS ... 1295

Crie uma conexão entre contas da Amazon EventBridge 1309
Entregue registros do DynamoDB para o Amazon S3 usando o Kinesis Data Streams e o Firehose 1324
Implemente o controle de versão da API baseado em caminhos usando o API Gateway ... 1331
Importe a biblioteca psycopg2 para AWS Lambda 1344
Integre o API Gateway com o Amazon SQS 1353
Processe de forma APIs assíncrona com o AWS Lambda 1369
Processe de forma APIs assíncrona com o Amazon DynamoDB Streams 1379
Processe de forma APIs assíncrona com o Amazon SQS 1389
Execute tarefas do Systems Manager Automation de forma síncrona a partir do Step Functions 1400
Execute leituras paralelas de objetos do S3 com AWS Lambda 1414
Envie dados de telemetria do Lambda para OpenSearch 1426
Configurar um roteador celular sem servidor 1443
Configurar o acesso privado a um bucket do Amazon S3 1462
Solucionar problemas de estados do Step Functions 1469
Use uma abordagem de tecnologia sem servidor para reunir os serviços da AWS 1479
Mais padrões 1485
Redes 1487
Automatizar o emparelhamento para o AWS Transit Gateway 1488
Centralize a conectividade de rede usando o AWS Transit Gateway 1496
Configurar a criptografia HTTPS para Oracle JD Edwards EnterpriseOne usando um Application Load Balancer 1503
Conecte-se ao ambiente de gerenciamento e dados do Application Migration Service em uma rede privada 1515
Crie objetos Infoblox usando recursos personalizados da AWS CloudFormation 1529
Personalize CloudWatch alertas para o Network Firewall 1543
Implante recursos em uma zona de Wavelength usando o Terraform 1562
Migre registros de DNS em massa para uma zona hospedada privada do Route 53 1571
Modifique os cabeçalhos HTTP ao migrar de F5 para um Application Load Balancer na AWS 1581
Acesse de forma privada um endpoint de serviço da AWS a partir de vários VPCs 1587
Relate as descobertas do Network Access Analyzer em vários Contas da AWS 1598
Configure a resolução de DNS para redes híbridas em um ambiente com várias contas AWS 1630
..... 1645

Visualize registros e métricas do AWS Network Firewall usando o Splunk 1651
Mais padrões 1661
Entrega de conteúdo 1663
Envie AWS WAF registros para o Splunk usando o Firehose 1664
Ofereça conteúdo estático em um bucket do S3 por meio de uma VPC usando CloudFront 1672
Mais padrões 1681
Bancos de dados e armazenamento 1682
Bancos de dados 1683
Acesse dados on-premises do SQL Server usando servidores vinculados 1686
Adicione HA ao Oracle PeopleSoft na AWS 1692
Avaliar o desempenho das consultas para migrar bancos de dados do SQL Server para o MongoDB Atlas na AWS 1717
Automatize as implantações azul/verdes dos bancos de dados globais Aurora com IaC 1727
Automatize as tarefas do banco de dados com o Agendador AWS Lambda de Tarefas 1762
Automatize o failover e o failback com o DR Orchestrator Framework 1775
Automatize a replicação de instâncias do Amazon RDS em Contas da AWS 1803
Fazer backup automático dos bancos de dados SAP HANA 1818
Gere automaticamente modelos PyNamoDB e funções CRUD para o DynamoDB 1826
Bloqueie o acesso público ao Amazon RDS 1834
Configurar o acesso entre contas ao Amazon DynamoDB 1841
Configurar o roteamento somente leitura em um grupo de disponibilidade Always On (Sempre ativo) 1854
Conecte-se usando um túnel SSH no pgAdmin 1863
Converta consultas JSON Oracle em SQL do banco de dados PostgreSQL 1868
Copie tabelas do Amazon DynamoDB entre contas 1898
Copie tabelas do Amazon DynamoDB entre contas 1904
Crie relatórios de custos e uso para o Amazon RDS e o Amazon Aurora 1917
Implante o SQL Server FCIs na Amazon EC2 e na Amazon FSx 1924
Emule workloads do Oracle RAC usando o Aurora PostgreSQL 1941
Habilite conexões criptografadas para instâncias de banco de dados PostgreSQL 1947
Criptografe uma instância de banco de dados Amazon RDS para PostgreSQL existente .. 1956
Aplique a marcação automática dos bancos de dados do Amazon RDS no lançamento 1965
Estime os custos do DynamoDB 1971
Estime os custos de armazenamento de uma tabela do Amazon DynamoDB 1983

Estime o tamanho do mecanismo Amazon RDS para um banco de dados Oracle usando relatórios AWR ... 1987
Exportar tabelas do Amazon RDS para SQL Server para um bucket do S3 ... 2021
Manipule blocos anônimos em instruções de SQL dinâmico ... 2033
Lide com funções sobrecarregadas do Oracle no Aurora compatível com PostgreSQL ... 2041
Ajude a aplicar a marcação no DynamoDB ... 2048
Implemente DR entre regiões ... 2054
Migre funções Oracle com mais de 100 argumentos para o PostgreSQL ... 2072
Migre instâncias do banco de dados Amazon RDS para Oracle para contas da AMS ... 2078
Migrar variáveis de ligação Oracle OUT para o PostgreSQL ... 2089
Migre o SAP HANA para a AWS usando o HSR ... 2097
Migre o SQL Server para a AWS usando grupos de disponibilidade distribuídos ... 2111
Migre do Oracle 8i ou 9i para o Amazon RDS for Oracle usando o AWS DMS SharePlex ... 2123
Monitore a criptografia do Amazon Aurora ... 2132
Monitore GoldenGate os registros usando a Amazon CloudWatch ... 2137
Replataforma do Oracle Database EE para o Amazon RDS for Oracle SE2 ... 2151
Replique bancos de dados de mainframe para AWS usando o Precisely Connect ... 2163
Agende trabalhos para o Amazon RDS e o Aurora PostgreSQL ... 2183
Enviar notificações para o RDS for SQL Server usando um servidor SMTP on-premises ... 2189
Configure o DR para SAP no IBM Db2 na AWS ... 2204
Configure um pipeline de CI/CD para migração de banco de dados usando o Terraform ... 2225
Configure uma arquitetura de HA/DR para o Oracle E-Business Suite no Amazon RDS Custom ... 2234
Configure a replicação de dados entre o RDS for MySQL e o MySQL na Amazon EC2 ... 2243
Funções de transição para um PeopleSoft aplicativo Oracle ... 2249
Descarregue dados do Amazon Redshift em todas as contas ... 2286
Padrões de migração de base de dados por workload ... 2317
Mais padrões ... 2328
Armazenamento e backup ... 2334
Permitir às EC2 instâncias acesso de gravação aos buckets do S3 no AMS ... 2335
Automatize a ingestão do fluxo de dados em um banco de dados Snowflake ... 2341
Criptografe automaticamente volumes do EBS ... 2352
Faça backup dos servidores Sun SPARC no emulador Charon-SSP na AWS ... 2363
Faça backup e arquive dados no Amazon S3 com a Veeam ... 2388
Configure NetBackup para a VMware nuvem na AWS ... 2417
Copie objetos do S3 entre contas e regiões usando o AWS CLI ... 2424

Copie objetos do S3 entre contas e regiões usando a replicação em lote do S3 2439
Migre dados do Hadoop para o Amazon S3 usando DistCp e AWS para o Amazon S3 PrivateLink 2452
Mais padrões 2468
Ferramentas de desenvolvedor 2470
DevOps 2471
Automatize as operações de AWS infraestrutura 2475
Automatize CloudFront as atualizações para alterações nos endpoints do balanceador de carga 2484
Automatize as CodeGuru avaliações de aplicativos em AWS CDK Python 2493
Automatize a avaliação de recursos da AWS 2505
Automatize a instalação de sistemas SAP 2520
Automatize o portfólio e a implantação de produtos do Service Catalog usando o AWS CDK 2533
Automatize os backups da AWS CodeCommit para o Amazon S3 2552
Automatize a exclusão de pilhas CloudFormation 2560
Automatize o gerenciamento dinâmico do pipeline para implantar soluções de hotfix 2572
Automatize a ingestão de métricas personalizadas do Amazon MWAA 2601
Automatize o gerenciamento dos recursos do Amazon Lex usando o e AWS CDK CloudFormation 2619
Automatize a implantação de conjuntos de pilhas usando a AWS e a AWS CodePipeline CodeBuild 2639
Anexe automaticamente uma política gerenciada do Systems Manager aos perfis de EC2 instância 2668
Criar automaticamente pipelines de CI/CD e clusters do Amazon ECS para microsserviços 2684
Crie uma arquitetura de acoplamento fraco com microsserviços 2697
Crie e envie imagens do Docker para o Amazon ECR 2709
Crie e teste aplicativos iOS com os serviços da AWS 2715
Verifique os aplicativos ou CloudFormation modelos do AWS CDK para obter as melhores práticas usando pacotes de regras 2721
Configurar a autenticação de TLS mútuo para aplicativos no Amazon EKS 2726
Crie recursos AppStream 2.0 usando a AWS CloudFormation 2737
Crie um analisador de log personalizado para o Amazon ECS usando o Firelens 2743
Crie um pipeline e uma AMI usando CodePipeline um HashiCorp Packer 2753
Crie um pipeline e implante atualizações em EC2 instâncias locais usando CodePipeline . 2760

Criar pipelines dinâmicos de CI para projetos Java e Python 2770
Implante CloudWatch canários Synthetics 2787
Implementar um pipeline de CI/CD para microsserviços Java no Amazon ECS 2795
Implemente uma ChatOps solução para gerenciar os resultados do escaneamento SAST 2804
Implante um firewall usando o AWS Network Firewall e o AWS Transit Gateway 2822
..... 2835
Implante um cluster Amazon EKS a partir do AWS Cloud9 usando um perfil de instância EC2 2840
Implantar código em várias regiões da AWS 2852
Execute consultas SQL do Amazon Redshift 2864
Exporte relatórios do AWS Backup como um arquivo CSV 2877
Exportar tags de EC2 instância da Amazon para um arquivo CSV 2886
Gere um CloudFormation modelo da AWS contendo as regras gerenciadas do AWS Config 2893
Conceda às instâncias do SageMaker notebook acesso entre contas a um repositório CodeCommit 2900
Implemente uma estratégia GitHub de ramificação do Flow 2912
Implemente uma estratégia de ramificação do Gitflow 2923
Implemente uma estratégia de ramificação de troncos 2935
Implemente o escaneamento Checkov personalizado e centralizado 2942
Inicie diferentes pipelines de CI/CD após detectar alterações em um monorepo 2953
Integrar um repositório Bitbucket com o AWS Amplify 2970
Lance um CodeBuild projeto em várias contas da AWS usando o Lambda 2979
Gerencie o failover Multi-AZ para clusters do EMR usando o Application Recovery Controller 2993
Gerencie implantações azul/verdes de microsserviços em várias contas e regiões 3010
Monitore os repositórios do Amazon ECR para obter permissões curinga 3044
Otimize implantações sem servidor em várias contas 3049
Execute ações personalizadas a partir de CodeCommit eventos da AWS 3070
Provisionar AWS Service Catalog produtos usando GitHub ações 3075
Provisione funções do IAM com privilégios mínimos 3086
Publique CloudWatch métricas da Amazon em um arquivo CSV 3100
Remova EC2 as entradas da Amazon em frente Contas da AWS ao AWS Managed Microsoft AD 3106
Remover EC2 entradas da Amazon no mesmo Conta da AWS de AWS Managed Microsoft AD 3124

Execute testes de unidade para trabalhos de ETL do Python em AWS Glue 3135
Configurar charts do Helm v3 no Amazon S3 3146
Configure um pipeline de CI/CD com CodePipeline 3155
Configure o registro centralizado em grande escala usando o Terraform 3171
Configure a end-to-end criptografia para aplicativos no Amazon EKS 3197
Simplifique a implantação de aplicativos multilocatários do Amazon EKS 3210
Assinar vários endpoints de e-mail em um tópico do SNS 3229
Use a construção do AWS Fargate WaitCondition gancho 3234
Use repositórios Git de terceiros na AWS CodePipeline 3247
Valide as configurações do Terraform usando a AWS CodePipeline 3257
Mais padrões 3273
Infraestrutura 3277
Acesse um bastion host usando o Session Manager e o Amazon EC2 Instance Connect .. 3279
Centralize a resolução de DNS usando AWS Managed Microsoft AD 3296
Centralize o monitoramento com o Gerente de Acesso à Observabilidade 3308
Verifique as EC2 instâncias para ver as tags obrigatórias no lançamento 3322
Limpe os recursos AFT com segurança após a perda do arquivo de estado 3328
Conecte-se a uma EC2 instância usando o Gerenciador de Sessões 3342
Crie um pipeline em regiões da AWS que não oferecem suporte à AWS CodePipeline 3349
Personalize os nomes das funções padrão usando AWS CDK aspectos e escotilhas de escape 3357
Implemente um cluster Cassandra na Amazon EC2 com estática privada IPs 3366
Estenda VRFs para a AWS usando o Transit Gateway Connect 3373
Receber notificações do Amazon SNS sobre mudanças de estado nas chaves do AWS KMS 3390
Preserve o espaço IP roteável em projetos de VPC com várias contas para sub-redes sem workload 3397
Provisionar um produto Terraform no Service Catalog a partir de um repositório de código 3403
Registrar várias contas da AWS com um único endereço de e-mail 3424
Configure a resolução de DNS para redes híbridas em um ambiente de conta única da AWS 3441
Configure bots UiPath de RPA automaticamente na Amazon EC2 3447
Configure uma PeopleSoft arquitetura altamente disponível na AWS 3463
Configurar a recuperação de desastres para o Oracle JD Edwards EnterpriseOne 3491
Configure a detecção e a geração de relatórios de desvios 3521
Importe com sucesso um bucket do S3 como uma CloudFormation pilha 3526

Sincronize sistemas de arquivos Amazon EFS em diferentes regiões ... 3539
Teste a AWS infraestrutura usando LocalStack testes do Terraform ... 3547
Atualize os clusters do SAP Pacemaker de para ENSA1 ENSA2 ... 3555
Use zonas de disponibilidade consistentes VPCs em diferentes contas ... 3577
Use o usuário IDs nas políticas do IAM ... 3583
Valide o código do Account Factory for Terraform localmente ... 3594
Mais padrões ... 3614
Aplicativos para web e dispositivos móveis ... 3618
Autenticar usuários do aplicativo web React ... 3619
Implementar continuamente um aplicativo web Amplify ... 3629
Crie um aplicativo React usando o AWS Amplify e o Amazon Cognito ... 3637
Crie um portal para microfrontends ... 3653
Implante um SPA baseado em React no Amazon S3 e CloudFront ... 3684
Implante uma API do Amazon API Gateway usando endpoints privados e um Application Load Balancer ... 3692
Incorpore um QuickSight painel da Amazon em um aplicativo Angular local ... 3700
Explore o desenvolvimento de aplicativos web com o Green Boost ... 3722
Execute testes unitários usando a AWS CodeBuild ... 3751
Estruture um projeto Python em arquitetura hexagonal ... 3760
Mais padrões ... 3786
IoT ... 3788
Configurar o registro em log e o monitoramento de eventos de segurança em seu ambiente de IoT ... 3789
Resumo ... 3789
Pré-requisitos e limitações ... 3789
Arquitetura ... 3790
Ferramentas ... 3792
Épicos ... 3793
Recursos relacionados ... 3798
Extraia e consulte atributos de AWS IoT SiteWise metadados ... 3799
Resumo ... 3799
Pré-requisitos e limitações ... 3799
Arquitetura ... 3800
Ferramentas ... 3800
Épicos ... 3801
Recursos relacionados ... 3804

Mais informações 3805
..... 3807
Resumo 3807
Pré-requisitos e limitações 3808
Arquitetura 3808
Ferramentas 3809
Práticas recomendadas 3809
Épicos 3810
Solução de problemas 3825
Recursos relacionados 3827
Mais informações 3828
Mais padrões 3830
Migração e modernização 3831
Migração 3832
Crie CloudFormation modelos da AWS para o AWS DMS 3833
Conceitos básicos de descoberta automatizada de portfólio 3837
Migre as workloads on-premises da Cloudera para a AWS 3846
Resolva erros de conexão após migrar o SQL Server para a AWS 3863
Reinicie o AWS Replication Agent automaticamente sem desabilitar SELinux 3866
Redefinir arquitetura 3874
Redefinir a hospedagem 4286
Realocar 4568
Redefinir a plataforma 4624
Padrões de migração por workload 5268
Mais padrões 5277
Modernização 5279
Analisar e visualizar a arquitetura de software no CAST Imaging 5280
Avaliar a prontidão do aplicativo antes da migração para a AWS usando o CAST Highlight 5289
Arquivar automaticamente dados expirados do DynamoDB no Amazon S3 5314
Crie uma arquitetura sem servidor multilocatário no Amazon Service OpenSearch 5331
Implante aplicativos de várias pilhas 5380
Implante aplicativos aninhados usando o AWS SAM 5389
Implementar o isolamento de inquilinos SaaS para o Amazon S3 usando uma TVM do AWS Lambda 5398
Implementar o padrão de saga com tecnologia sem servidor usando o AWS Step Functions 5422

Gerencie aplicativos de contêineres on-premises com o Amazon ECS Anywhere 5437
Modernize aplicativos ASP.NET Web Forms na AWS 5447
Execute workloads orientadas por eventos com o AWS Fargate 5463
Integração de locatários na arquitetura SaaS 5473
Use o CQRS e o fornecimento de eventos 5499
Mais padrões 5526
Mainframes 5529
Acesse Serviços da AWS a partir do IBM z/OS instalando o AWS CLI 5531
Faça backup e arquive dados do mainframe no Amazon S3 5552
Crie programas COBOL Db2 usando e AWS Mainframe Modernization AWS CodeBuild ... 5579
Crie um PAC do Micro Focus Enterprise Server 5603
Crie um visualizador de arquivos de mainframe na Nuvem AWS 5624
Containerize aplicativos Blu Age modernizados 5640
Converta dados EBCDIC em ASCII na AWS 5650
Converta arquivos EBCDIC de mainframe em arquivos ASCII usando o AWS Lambda 5669
Converta arquivos de dados de mainframe com layouts de registro complexos 5691
Implante um ambiente para aplicativos conteinerizados 5710
Gere insights de dados do Db2 z/OS 5721
Gere insights usando o AWS Mainframe Modernization e o Amazon Q em QuickSight 5773
Integre o controlador universal Stonebranch com a AWS 5791
Migre e replique arquivos VSAM para a Nuvem AWS usando o Precisely 5825
Modernize o gerenciamento de saída do mainframe em AWS 5843
Modernize o aplicativo de CardDemo mainframe usando AWS Transform 5894
Modernize suas cargas de trabalho de impressão em lote de mainframe em AWS 5913
Modernize seu ambiente de mainframe com o Rocket Software Enterprise Suite 5943
Modernize suas workloads de impressão on-line de mainframe na AWS 5960
Mova arquivos de mainframe para o Amazon S3 usando o Transfer Family 5995
Acesso seguro do usuário em um banco de dados de federação Db2 6008
Transferir dados do Db2 z/OS para a AWS 6017
Mais padrões 6045
Gerenciamento 6046
Gerenciamento de custos 6047
Crie relatórios detalhados de custo e uso para trabalhos do AWS Glue 6048
Crie relatórios detalhados de custo e uso para clusters do Amazon EMR 6054
Mais padrões 6059
Computação de alta performance 6060

Implante um sistema de arquivos Lustre usando o Terraform e o DRA 6061
Configure um painel de monitoramento da Grafana para a AWS ParallelCluster 6070
Configurar uma VDI de ajuste de escala automático usando NICE DCV 6084
Nuvem híbrida 6097
Configurar uma extensão de datacenter para a VMware nuvem na AWS 6098
Configurar o vRealize Automation para provisionar VMs na VMware nuvem na AWS 6104
Integre o VMware vRealize Network Insight com a VMware nuvem na AWS 6116
Migre VMs para a VMware nuvem na AWS usando o HCX OSAM 6121
Envie registros do VMware Cloud on AWS para o Splunk 6127
Configure um pipeline de CI/CD para workloads híbridas no Amazon ECS Anywhere 6134
Mais padrões 6154
Gerenciamento e governança 6155
Alerta quando os recursos do Amazon Data Firehose não estiverem criptografados 6156
Automatizar a adição ou atualização de entradas de registro do Windows 6161
Crie automaticamente um RFC usando Python 6166
Parar e iniciar uma instância de banco de dados do Amazon RDS automaticamente 6173
Centralize a distribuição de pacotes de software no AWS Organizations usando o Terraform 6188
Configurar o registro em log para aplicativos.NET em CloudWatch Logs 6202
Copie os produtos do AWS Service Catalog em contas e regiões da AWS 6212
Crie uma matriz RACI para operações em nuvem 6222
Crie alarmes para métricas personalizadas usando CloudWatch 6229
Crie um AWS Cloud9 IDE com volumes EBS criptografados padrão 6237
Crie CloudWatch painéis baseados em tags automaticamente 6243
Documente o design da sua landing zone 6252
Habilite o Amazon DevOps Guru em toda a organização com o AWS CDK 6256
Implemente o AFT usando um pipeline de bootstrap 6283
Gerencie produtos do AWS Service Catalog em várias contas e regiões da AWS 6308
Migre uma conta da AWS do AWS Organizations para o AWS Control Tower 6316
Monitore clusters SAP RHEL Pacemaker 6331
Monitore a atividade do aplicativo usando o CloudWatch Logs Insights 6351
Monitore o uso de uma AMI em Contas da AWS 6362
Configure alertas para encerramentos programáticos de contas no AWS Organizations 6379
Ver os detalhes do snapshot do EBS para sua conta ou organização da AWS 6389
Mais padrões 6396
Mensagens e comunicações 6399

Automatize a configuração RabbitMQ no Amazon MQ 6400
Melhore a qualidade das chamadas nas estações de trabalho dos atendentes no Amazon Connect 6408
Mais padrões 6424
Segurança, identidade e conformidade 6425
Acesso a Serviços da AWS partir do ASP.NET usando o Amazon Cognito 6428
Resumo 6428
Pré-requisitos e limitações 6428
Arquitetura 6429
Ferramentas 6429
Épicos 6430
Solução de problemas 6434
Recursos relacionados 6435
Anexos 6435
Autenticar o SQL Server usando o AWS Directory Service 6436
Resumo 6436
Pré-requisitos e limitações 6436
Arquitetura 6436
Ferramentas 6437
Épicos 6437
Recursos relacionados 6441
Automatize a resposta a incidentes e forense 6442
Resumo 6442
Pré-requisitos e limitações 6442
Arquitetura 6443
Ferramentas 6445
Épicos 6446
Recursos relacionados 6450
Mais informações 6450
Anexos 6451
Automatize a remediação das descobertas do padrão do Security Hub 6452
Resumo 6452
Pré-requisitos e limitações 6453
Arquitetura 6453
Ferramentas 6454
Práticas recomendadas 6454

Épicos 6455
Recursos relacionados 6458
Anexos 6458
Automatize as verificações de segurança para workloads entre contas usando o Amazon Inspector 6459
Resumo 6459
Pré-requisitos e limitações 6459
Arquitetura 6460
Ferramentas 6461
Épicos 6462
Recursos relacionados 6466
Anexos 6466
Audite automaticamente o acesso de endereços IP públicos 6467
Resumo 6467
Pré-requisitos e limitações 6467
Arquitetura 6468
Ferramentas 6470
Práticas recomendadas 6471
Épicos 6471
Solução de problemas 6475
Recursos relacionados 6476
Reative automaticamente a AWS CloudTrail usando as melhores práticas de segurança 6477
Resumo 6477
Pré-requisitos e limitações 6477
Arquitetura 6478
Ferramentas 6478
Épicos 6479
Recursos relacionados 6485
Anexos 6486
Corrija automaticamente instâncias e clusters de banco de dados Amazon RDS não criptografados 6487
Resumo 6487
Pré-requisitos e limitações 6487
Arquitetura 6489
Ferramentas 6489
Práticas recomendadas 6491

Épicos 6491
Recursos relacionados 6498
Mais informações 6499
Gire automaticamente as chaves de acesso do usuário do IAM 6500
Resumo 6500
Pré-requisitos e limitações 6501
Arquitetura 6502
Ferramentas 6504
Épicos 6506
Recursos relacionados 6516
Valide e implante automaticamente políticas e perfis do IAM em uma conta da AWS 6517
Resumo 6517
Pré-requisitos e limitações 6518
Arquitetura 6519
Ferramentas 6519
Épicos 6520
Recursos relacionados 6524
Integre bidirecionalmente o Security Hub e o Jira 6526
Resumo 6526
Pré-requisitos e limitações 6527
Arquitetura 6528
Ferramentas 6529
Épicos 6530
Recursos relacionados 6540
Mais informações 6540
Crie um pipeline para imagens de contêineres reforçadas 6542
Resumo 6542
Pré-requisitos e limitações 6542
Arquitetura 6543
Ferramentas 6546
Épicos 6547
Solução de problemas 6554
Recursos relacionados 6555
Centralize o gerenciamento de chaves de acesso do IAM no AWS Organizations usando o Terraform 6556
Resumo 6556

Pré-requisitos e limitações 6557
Arquitetura 6557
Ferramentas 6559
Práticas recomendadas 6560
Épicos 6560
Solução de problemas 6570
Recursos relacionados 6570
Verifique a versão de registro de acesso, HTTPS e TLS em uma CloudFront distribuição da Amazon 6571
Resumo 6571
Pré-requisitos e limitações 6572
Arquitetura 6572
Ferramentas 6573
Épicos 6573
Recursos relacionados 6576
Anexos 6576
Verifique as entradas de rede de host único nas regras de entrada do grupo de segurança para e IPv4 IPv6 6577
Resumo 6577
Pré-requisitos e limitações 6577
Arquitetura 6577
Ferramentas 6578
Épicos 6579
Recursos relacionados 6582
Anexos 6582
Escolha um fluxo de autenticação do Amazon Cognito 6583
Resumo 6583
Pré-requisitos e limitações 6583
Arquitetura 6584
Ferramentas 6588
Épicos 6589
Recursos relacionados 6592
Mais informações 6593
Crie regras AWS Config personalizadas usando o Guard 6594
Resumo 6594
Pré-requisitos e limitações 6595

Arquitetura 6595
Ferramentas 6600
Épicos 6600
Solução de problemas 6602
Recursos relacionados 6603
Crie um relatório das descobertas do Prowler a partir de várias Contas da AWS 6605
Resumo 6605
Pré-requisitos e limitações 6606
Arquitetura 6607
Ferramentas 6608
Épicos 6609
Solução de problemas 6634
Recursos relacionados 6634
Mais informações 6634
Exclua volumes não utilizados do Amazon EBS usando AWS Config 6637
Resumo 6637
Pré-requisitos e limitações 6637
Arquitetura 6638
Ferramentas 6638
Épicos 6639
Solução de problemas 6642
Recursos relacionados 6642
Implemente AWS Control Tower controles usando AWS CDK 6643
Resumo 6643
Pré-requisitos e limitações 6644
Arquitetura 6645
Ferramentas 6646
Práticas recomendadas 6647
Épicos 6647
Recursos relacionados 6654
Mais informações 6655
Implemente AWS Control Tower controles usando o Terraform 6658
Resumo 6658
Pré-requisitos e limitações 6658
Arquitetura 6660
Ferramentas 6660

Práticas recomendadas 6661
Épicos 6661
Solução de problemas 6667
Recursos relacionados 6669
Mais informações 6669
Implemente um pipeline que detecte problemas de segurança no código 6672
Resumo 6672
Pré-requisitos e limitações 6672
Arquitetura 6673
Ferramentas 6674
Épicos 6674
Solução de problemas 6677
Recursos relacionados 6678
Mais informações 6678
Implemente controles de detetive para sub-redes públicas 6680
Resumo 6680
Pré-requisitos e limitações 6681
Arquitetura 6681
Ferramentas 6682
Práticas recomendadas 6683
Épicos 6683
Recursos relacionados 6691
Mais informações 6692
Implemente controles preventivos para sub-redes públicas 6694
Resumo 6694
Pré-requisitos e limitações 6694
Arquitetura 6695
Ferramentas 6696
Épicos 6697
Recursos relacionados 6703
Mais informações 6703
Implante as automações de segurança para a AWS WAF solução usando o Terraform 6706
Resumo 6706
Pré-requisitos e limitações 6706
Arquitetura 6707
Ferramentas 6707

Práticas recomendadas 6708
Épicos 6708
Solução de problemas 6711
Recursos relacionados 6712
Detecte instâncias do Amazon RDS com certificados CA expirados 6713
Resumo 6713
Pré-requisitos e limitações 6713
Arquitetura 6714
Ferramentas 6716
Práticas recomendadas 6717
Épicos 6717
Solução de problemas 6721
Recursos relacionados 6722
Gere dinamicamente uma política do IAM com o IAM Access Analyzer 6723
Resumo 6723
Pré-requisitos e limitações 6723
Arquitetura 6724
Ferramentas 6725
Épicos 6727
Recursos relacionados 6733
Habilitar GuardDuty o uso CloudFormation de modelos 6734
Resumo 6734
Pré-requisitos e limitações 6734
Arquitetura 6734
Ferramentas 6735
Épicos 6736
Recursos relacionados 6737
Mais informações 6738
Suporte para criptografia de dados transparente no Amazon RDS para SQL Server 6742
Resumo 6742
Pré-requisitos e limitações 6742
Arquitetura 6742
Ferramentas 6743
Épicos 6743
Recursos relacionados 6746
Garanta que os balanceadores de carga da AWS usem protocolos receptores seguros 6747

Resumo 6747
Pré-requisitos e limitações 6747
Arquitetura 6748
Ferramentas 6748
Práticas recomendadas 6749
Épicos 6749
Solução de problemas 6752
Recursos relacionados 6753
Anexos 6753
Garantir a criptografia para dados em repouso do Amazon EMR 6754
Resumo 6754
Pré-requisitos e limitações 6754
Arquitetura 6755
Ferramentas 6755
Épicos 6756
Recursos relacionados 6759
Anexos 6759
Certifique-se de que um perfil do IAM esteja associado a uma EC2 instância 6760
Resumo 6760
Pré-requisitos e limitações 6760
Arquitetura 6761
Ferramentas 6761
Épicos 6762
Recursos relacionados 6765
Anexos 6765
Garanta que os novos clusters do Amazon Redshift sejam criptografados 6766
Resumo 6766
Pré-requisitos e limitações 6766
Arquitetura 6766
Ferramentas 6767
Épicos 6768
Recursos relacionados 6770
Anexos 6770
Exporte um relatório das identidades do Centro de Identidade do AWS IAM e suas atribuições 6771
Resumo 6771

Pré-requisitos e limitações 6771
Arquitetura 6773
Ferramentas 6773
Épicos 6774
Solução de problemas 6775
Recursos relacionados 6777
Mais informações 6777
Ajude a evitar a exclusão programada da chave KMS 6779
Resumo 6779
Pré-requisitos e limitações 6779
Arquitetura 6780
Ferramentas 6781
Épicos 6782
Recursos relacionados 6785
Mais informações 6786
Anexos 6786
Identifique buckets públicos do Amazon S3 em AWS Organizations 6787
Resumo 6787
Pré-requisitos e limitações 6787
Arquitetura 6788
Ferramentas 6789
Épicos 6790
Solução de problemas 6794
Recursos relacionados 6795
Mais informações 6795
Ingira registros de segurança da AWS no Microsoft Sentinel 6796
Resumo 6796
Pré-requisitos e limitações 6796
Arquitetura 6798
Ferramentas 6799
Práticas recomendadas 6800
Épicos 6800
Recursos relacionados 6811
Gerencie AWS Organizations políticas como código 6813
Resumo 6813
Pré-requisitos e limitações 6813

Arquitetura 6814
Ferramentas 6815
Práticas recomendadas 6817
Épicos 6817
Solução de problemas 6836
Recursos relacionados 6838
Mais informações 6839
Gerencie os conjuntos de permissões do IAM Identity Center usando CodePipeline 6841
Resumo 6841
Pré-requisitos e limitações 6841
Arquitetura 6843
Ferramentas 6844
Práticas recomendadas 6845
Épicos 6845
Solução de problemas 6855
Recursos relacionados 6856
Gerenciar credenciais com o AWS Secrets Manager 6857
Resumo 6857
Pré-requisitos e limitações 6857
Arquitetura 6857
Ferramentas 6858
Épicos 6858
Recursos relacionados 6860
Mais informações 6860
..... 6863
Resumo 6863
Pré-requisitos e limitações 6863
Arquitetura 6864
Ferramentas 6864
Épicos 6865
Recursos relacionados 6868
Anexos 6868
Monitorar clusters do Amazon EMR para criptografia em trânsito na execução 6869
Resumo 6869
Pré-requisitos e limitações 6870
Arquitetura 6870

Ferramentas 6871
Épicos 6872
Recursos relacionados 6874
Anexos 6874
Monitore ElastiCache clusters da Amazon para criptografia em repouso 6875
Resumo 6875
Pré-requisitos e limitações 6876
Arquitetura 6876
Ferramentas 6877
Épicos 6878
Recursos relacionados 6880
Anexos 6880
Monitore os pares de chaves da EC2 instância 6881
Resumo 6881
Pré-requisitos e limitações 6881
Arquitetura 6881
Ferramentas 6882
Épicos 6883
Recursos relacionados 6887
Anexos 6887
Monitorar a atividade do usuário raiz do IAM 6888
Resumo 6888
Pré-requisitos e limitações 6888
Arquitetura 6889
Ferramentas 6889
Épicos 6891
Recursos relacionados 6896
Mais informações 6896
Notificar quando um usuário do IAM for criado 6897
Resumo 6897
Pré-requisitos e limitações 6897
Arquitetura 6897
Ferramentas 6898
Épicos 6899
Recursos relacionados 6901
Anexos 6902

Impeça o acesso à Internet usando um SCP 6903
Resumo 6903
Pré-requisitos e limitações 6903
Ferramentas 6904
Práticas recomendadas 6904
Épicos 6905
Recursos relacionados 6907
Restrinja o acesso com base no endereço IP ou geolocalização 6908
Resumo 6908
Pré-requisitos e limitações 6908
Ferramentas 6909
Épicos 6910
Recursos relacionados 6915
Examine os repositórios Git em busca de informações confidenciais 6917
Resumo 6917
Pré-requisitos e limitações 6917
Arquitetura 6917
Ferramentas 6918
Práticas recomendadas 6918
Épicos 6918
Recursos relacionados 6922
Envie alertas do AWS Network Firewall para um canal do Slack 6923
Resumo 6923
Pré-requisitos e limitações 6923
Arquitetura 6924
Ferramentas 6925
Épicos 6926
Recursos relacionados 6932
Mais informações 6932
Simplificar o gerenciamento de certificados privados usando a CA privada da AWS e o AWS RAM 6937
Resumo 6937
Pré-requisitos e limitações 6937
Arquitetura 6938
Ferramentas 6939
Épicos 6940

Recursos relacionados 6948
Mais informações 6949
Desative os controles padrão de segurança em todas as contas de membros do Security Hub 6950
Resumo 6950
Pré-requisitos e limitações 6950
Arquitetura 6951
Ferramentas 6952
Épicos 6953
Recursos relacionados 6957
Atualize as credenciais da AWS CLI do IAM Identity Center usando PowerShell 6958
Resumo 6958
Pré-requisitos e limitações 6958
Arquitetura 6959
Ferramentas 6959
Práticas recomendadas 6960
Épicos 6960
Solução de problemas 6962
Recursos relacionados 6963
Mais informações 6963
Use o AWS Config para monitorar o Amazon Redshift 6966
Resumo 6966
Pré-requisitos e limitações 6966
Arquitetura 6967
Ferramentas 6967
Épicos 6968
Recursos relacionados 6971
Mais informações 6972
Use o Network Firewall para capturar nomes de domínio DNS do tráfego de rede de saída ... 6973
Resumo 6973
Pré-requisitos e limitações 6973
Arquitetura 6974
Ferramentas 6974
Épicos 6975
Use o Terraform para ativar automaticamente GuardDuty 6992
Resumo 6992

Pré-requisitos e limitações 6993
Arquitetura 6995
Ferramentas 6996
Épicos 6997
Recursos relacionados 7006
Mais informações 7007
Verifique as melhores práticas para o PCI DSS 4.0 7008
Resumo 7008
Pré-requisitos e limitações 7009
Ferramentas 7010
Épicos 7011
Recursos relacionados 7013
Mais informações 7013
Anexos 7014
..... 7015
Resumo 7015
Pré-requisitos e limitações 7015
Arquitetura 7016
Ferramentas 7016
Épicos 7017
Recursos relacionados 7020
Anexos 7020
..... 7021
Resumo 7021
Pré-requisitos e limitações 7021
Arquitetura 7022
Ferramentas 7022
Épicos 7023
Recursos relacionados 7026
Anexos 7026
Mais padrões 7027
..... 7030

AWS Padrões de orientação prescritiva

Os padrões de orientação prescritiva da Amazon Web Services (AWS) fornecem step-by-step instruções, arquitetura, ferramentas e código para implementar cenários específicos de migração, modernização e implantação na nuvem. Esses padrões, que são examinados por especialistas no assunto AWS, são destinados a criadores e usuários práticos que planejam ou estão em processo de migração. AWS Eles também oferecem suporte a usuários que já estão AWS conectados e estão procurando maneiras de otimizar ou modernizar suas operações na nuvem.

Você pode usar esses padrões para mover suas cargas de trabalho locais ou na nuvem de complexidade variável AWS e acelerar seus esforços de adoção, otimização e modernização da nuvem, independentemente de você estar na fase de prova de conceito, planejamento ou implementação do seu projeto. Por exemplo, para um projeto de migração para a nuvem:

- Na fase de planejamento, você pode avaliar as diferentes opções disponíveis para migrar para AWS. Você pode escolher o padrão certo que atenda às suas necessidades, dependendo se você deseja realocar, redefinir a hospedagem, redefinir a plataforma, ou redefinir a arquitetura. Você também pode entender as diferentes ferramentas disponíveis para migração e começar a planejar a aquisição de licenças ou iniciar conversas iniciais com fornecedores.
- Nas fases de prova de conceito e implementação, você pode seguir as step-by-step instruções fornecidas no padrão para migrar sua carga de trabalho para o. AWS Cada padrão inclui detalhes como pré-requisitos, arquiteturas de referência de destino, ferramentas, step-by-step tarefas, melhores práticas, solução de problemas e código.
- Se você já estiver usando o Nuvem AWS, poderá encontrar padrões que ajudarão você a modernizar, otimizar, escalar e proteger o uso dos recursos da nuvem.

Para visualizar listas de padrões por domínio técnico, use os links a seguir ou as opções de filtragem e pesquisa na página inicial da Orientação Prescritiva da AWS.

- Fundamentos da nuvem
- IA e aprendizado de máquina
- Analytics
- Computação
- Bancos de dados e armazenamento
- Ferramentas para desenvolvedores

- IoT
- Migração e modernização
- Gestão
- Segurança, identidade e conformidade

Para ver todas as publicações, incluindo guias, estratégias e padrões, consulte a página inicial da Orientação Prescritiva da AWS.

Fundamentos da nuvem

Tópicos

- Automatize a criação de contas usando o Landing Zone Accelerator em AWS
- Faça o inventário automático de AWS recursos em várias contas e regiões
- Configure os logs de fluxo da VPC para centralização em todas as contas da AWS
- Marque anexo do gateway de trânsito automaticamente usando o AWS Organizations
- Mais padrões

Automatize a criação de contas usando o Landing Zone Accelerator em AWS

Criado por Justin Kuskowski (AWS), Joe Behrens (AWS) e Nathan Scott (AWS)

Resumo

Esse padrão explica como usar a AWS solução Landing Zone Accelerator on para implantar automaticamente uma nova Conta da AWS quando um usuário autorizado envia uma solicitação. Ele é usado AWS Step Functions para orquestrar várias funções AWS Lambda . As funções do Lambda adicionam as informações da conta a um repositório Git, iniciam um AWS CodePipeline pipeline e validam se os recursos necessários foram provisionados. AWS Quando o processo for concluído, o usuário receberá uma notificação de que a conta foi criada.

Opcionalmente, você pode integrar grupos de ID do Microsoft Entra e atribuir conjuntos de AWS IAM Identity Center permissões durante o processo de criação da conta. Se sua organização estiver usando o Microsoft Entra ID como fonte de identidade, esse recurso opcional ajuda você a gerenciar e configurar automaticamente o acesso à nova conta.

Pré-requisitos e limitações

Pré-requisitos

- Acesso à conta de gerenciamento em AWS Organizations
- AWS Cloud Development Kit (AWS CDK) versão 2.118.0 ou posterior, instalada e configurada
- Python versão 3.9 ou posterior, instalado
- AWS Command Line Interface (AWS CLI) versão 2.13.19 ou posterior, instalada
- Docker versão 24.0.6 ou posterior, instalado
- Landing Zone Accelerator na AWS solução, implantada na conta de gerenciamento
- (Opcional) Microsoft Entra ID e IAM Identity Center, integrados

Limitações

O fluxo de trabalho de criação de contas suporta execuções sequenciais para implantar uma única. Conta da AWS Essa limitação garante que o fluxo de trabalho de criação da conta seja concluído com êxito sem precisar competir por recursos durante uma execução paralela.

Arquitetura

Arquitetura de destino

A imagem a seguir mostra a arquitetura de alto nível de automatização da criação de um novo Conta da AWS usando o Landing Zone Accelerator ativado. AWS AWS Step Functions orquestra a automação. Cada tarefa no fluxo de trabalho do Step Functions é executada por uma ou mais AWS Lambda funções.

O diagrama mostra o seguinte fluxo de trabalho:

1. O usuário solicita uma conta executando um script Python ou usando o Amazon API Gateway.
2. O fluxo de trabalho do Account Creation Orchestrator começa em. AWS Step Functions
3. O fluxo de trabalho atualiza o `account-config.yaml` arquivo no repositório do código-fonte. Ele também inicia o Landing Zone Accelerator na AWS tubulação e verifica o status da tubulação. Esse pipeline cria e configura a nova conta. Para obter mais informações sobre como isso funciona, consulte a visão geral da arquitetura do Landing Zone Accelerator em AWS.
4. (Opcional) Quando o pipeline é concluído, o fluxo de trabalho verifica se o grupo existe no Microsoft Entra ID. Se o grupo não existir no Microsoft Entra ID, o fluxo de trabalho adiciona o grupo ao Microsoft Entra ID.
5. O fluxo de trabalho executa etapas adicionais que a AWS solução Landing Zone Accelerator on não pode realizar. As etapas padrão incluem:
   - Criação de um alias de conta no AWS Identity and Access Management (IAM)
   - Anexando tags à conta em AWS Organizations
   - Criação de AWS Systems Manager parâmetros no Parameter Store com base nas tags atribuídas à conta
6. (Opcional) O fluxo de trabalho atribui um ou mais conjuntos de permissões ao grupo Microsoft Entra ID que você especificou anteriormente. Os conjuntos de permissões permitem que os usuários do grupo acessem a nova conta e executem as ações que você configura.
7. Uma AWS Lambda função executa testes de controle de qualidade e validação. Ele valida a criação de recursos, verifica se as tags foram criadas e valida se os recursos de segurança foram implantados.
8. O fluxo de trabalho libera a conta e usa o Amazon Simple Email Service (Amazon SES) para notificar o usuário de que o processo foi concluído com êxito.

Para obter mais informações sobre o fluxo de trabalho do Step Functions, consulte o diagrama do fluxo de trabalho do Step Functions na seção Informações adicionais desse padrão.

Aplicativos Microsoft Entra ID

Se você optar pela integração com o Microsoft Entra ID, você cria os dois aplicativos a seguir ao implantar esse padrão:

- Um aplicativo vinculado ao IAM Identity Center e garante que os grupos de ID do Microsoft Entra estejam disponíveis no IAM Identity Center. Neste exemplo, esse aplicativo Microsoft Entra ID é denominado`LZA2`.
- Um aplicativo que permite que uma função Lambda se comunique com o Microsoft Entra ID e chame o Microsoft Graph. APIs Nesse padrão, esse aplicativo é denominado`create_aws_account`.

Esses aplicativos coletam dados que são usados para sincronizar o grupo Microsoft Entra ID e atribuir conjuntos de permissões.

Ferramentas

Serviços da AWS

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala. Nesse padrão, você usa o API Gateway para verificar a disponibilidade de Conta da AWS nomes, iniciar o AWS Step Functions fluxo de trabalho e verificar o status da execução do Step Functions.
- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS Essa solução usa uma EventBridge regra que inicia uma função Lambda se o estado do fluxo de trabalho do Step Functions mudar para `FailedTimed-out`, ou. `Aborted`
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.

- AWS IAM Identity Centerajuda você a gerenciar centralmente o acesso de login único (SSO) a todos os seus Contas da AWS aplicativos e à nuvem.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados. Nesse padrão, AWS KMS as chaves são usadas para criptografar dados, como dados armazenados no Amazon Simple Storage Service (Amazon S3), variáveis de ambiente Lambda e dados em Step Functions.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- Amazon Simple Email Service (Amazon SES): ajuda você a enviar e receber e-mails usando seus próprios endereços de e-mail e domínios. Depois que uma nova conta for criada com sucesso, você receberá uma notificação por meio do Amazon SES.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail. Se ocorrer um erro durante o processo de criação da conta, o Amazon SNS enviará uma notificação para os endereços de e-mail que você configura.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.
- AWS Systems Manager O Parameter Store fornece armazenamento seguro e hierárquico para gerenciamento de dados de configuração e gerenciamento de segredos.

Outras ferramentas

- O awscurl automatiza o processo de assinatura de solicitações de AWS API e ajuda você a fazer solicitações como um comando curl padrão.
- O Microsoft Entra ID, anteriormente conhecido como Azure Active Directory, é um serviço de gerenciamento de identidade e acesso baseado em nuvem.
- O Microsoft Graph APIs ajuda você a acessar dados e inteligência nos serviços de nuvem da Microsoft, como o Microsoft Entra e o Microsoft 365.

Repositório de código

O código desse padrão está disponível no GitHub lza-account-creation-workflowrepositório.

O diretório lambda_layer contém as seguintes camadas, que são referenciadas em mais de uma função Lambda:

- account_creation_helper — Essa camada inclui os módulos para assumir funções e verificar o progresso. AWS Service Catalog
- boto3 — Essa camada inclui o AWS SDK para Python (Boto3)módulo para garantir que AWS Lambda tenha a versão mais recente.
- identity_center_helper — Essa camada suporta chamadas para o IAM Identity Center.

O diretório lambda_src contém as seguintes funções do Lambda:

- AccountTagToSsmParameter— Essa função usa as tags anexadas à conta para criar parâmetros no Parameter Store. AWS Organizations Cada parâmetro começa com um `/account/tags/` prefixo.
- AttachPermissionSet— Essa função adiciona um conjunto de permissões a um grupo do IAM Identity Center.
- ADGroupSincronização do Azure — Essa função sincroniza o grupo de ID Microsoft Entra de destino com o IAM Identity Center.
- CheckForRunningProcesses— Essa função verifica se o `AWSAccelerator-Pipeline` pipeline está em execução no momento. Se o pipeline estiver em execução, a função atrasará o AWS Step Functions fluxo de trabalho.
- CreateAccount— Esta função usa AWS Service Catalog e AWS Control Tower para criar o novo Conta da AWS.
- CreateAdditionalResources— Essa função cria os AWS recursos que não são gerenciados pelo Landing Zone Accelerator ou AWS CloudFormation, como o alias e AWS Service Catalog as tags da conta.
- GetAccountStatus— Essa função verifica o produto provisionado AWS Service Catalog para determinar se o processo de criação da conta foi concluído.
- GetExecutionStatus— Essa função recupera o status de uma execução em AWS Step Functions execução ou concluída.
- NameAvailability— Esta função verifica se um Conta da AWS nome já existe em AWS Organizations.

- ReturnResponse— Se a criação da conta for bem-sucedida, essa função retornará o ID da nova conta. Se a criação da conta não for bem-sucedida, ela retornará uma mensagem de erro.
- RunStepFunction— Essa função executa o AWS Step Functions fluxo de trabalho que cria a conta.
- SendEmailWithSES — Essa função envia e-mails para os usuários que estão aguardando a conclusão da criação da conta.
- Validar o ADGroup SyncTo SSO — Essa função verifica se os grupos de ID Microsoft Entra especificados estão sincronizados com o IAM Identity Center.
- ValidateResources— Essa função valida que todas as AWS Control Tower personalizações foram executadas com êxito.

Práticas recomendadas

Recomendamos as seguintes convenções de nomenclatura para: AWS CDK

- Inicie todos os parâmetros com um `p` prefixo.
- Inicie todas as condições com um `c` prefixo.
- Inicie todos os recursos com um `r` prefixo.
- Inicie todas as saídas com um o prefixo.

Épicos

Implante as funções do IAM para validação e marcação

Tarefa	Descrição	Habilidades necessárias
Prepare o Landing Zone Accelerator AWS para personalização.	1. No Landing Zone Accelerator no repositório de AWS código, crie um arquivo chamado. `customizations-config.yaml` Você usa esse arquivo para definir personalizações para a solução principal. Para obter mais informações,	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	consulte Personalização da solução. 2. No `customizations-config.yaml` arquivo, crie uma seção chamada `cloudFormationStacks` .	

Tarefa	Descrição	Habilidades necessárias
Prepare-se para implantar a `lza-account-creation-validation` função.	Agora, você personaliza a solução para implantar a função `lza-account-creation-validation` do IAM em todas as contas, exceto na conta de gerenciamento. Essa função fornece à função `ValidateResources` Lambda acesso somente de leitura às novas contas. 1. Baixe o account-creation-validation-rolearquivo.yaml em. GitHub 2. Salve o arquivo no local indicado na seção de modelos do `customizations-config.yaml` arquivo. 3. Abra o arquivo `customizations-config.yaml` . 4. Na `cloudFormationStacks` seção, adicione o código a seguir. Atualize o alvo Região da AWS conforme necessário para sua landing zone: `- deploymentTargets: organizationalUnits: - Root`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>excludedAccounts:
	- Management
	
	description: IAM Role to allow Account Validation
	name: lza-account-creation-validation
	regions:
	- us-east-1
	template: cloudformation/account-creation-validation-role.yaml
	runOrder: 1
	terminationProtection: true
	parameters:
	- name: pManagementAccountId
	value: "{{ account Management }}"</pre> 5. Salve e feche o arquivo `customizations-config.yaml` .	

Tarefa	Descrição	Habilidades necessárias
Prepare-se para implantar a `account-tagging-to-ssm-parameter-role` função.	Agora, você personaliza a solução para implantar a função `account-tagging-to-ssm-parameter-role` do IAM em todas as contas, exceto na conta de gerenciamento. Essa função é usada para criar os parâmetros no AWS Systems Manager Parameter Store. 1. Baixe o arquivo account-tagging-to-ssm-parameter-role.yaml em. GitHub 2. Salve o arquivo no local indicado na seção de modelos do `customizations-config.yaml` arquivo. 3. Abra o arquivo `customizations-config.yaml` . 4. Na `cloudFormationStacks` seção, adicione o código a seguir. Atualize o alvo Região da AWS conforme necessário para sua landing zone: `- deploymentTargets: organizationalUnits: - Root excludedAccounts:`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>-
	Management
	descripti
	on: IAM Role to
	create SSM Parameter
	s based on Account
	Tagging
	name: lza-
	account-tagging-to-
	ssm-parameter
	regions:
	- us-
	east-1
	template:
	cloudformation/acc
	ount-tagging-to-ss
	m-parameter-role.y
	aml
	runOrder: 1
	terminati
	onProtection: true
	
	parameters:
	- name:
	pManagementAccount
	Id
	value:
	"{{ account Managemen
	t }}"</pre> 5. Salve e feche o arquivo `customizations-con fig.yaml` .	

Tarefa	Descrição	Habilidades necessárias
Prepare-se para implantar a `config-log-validation-role` função.	Agora, você personaliza a solução para implantar a função do `config-log-validation-role` IAM na conta de arquivamento de registros. Essa função permite que a função `ValidateResources` Lambda acesse o bucket do Amazon S3 para registrar e acessar regras. AWS Config 1. Baixe o config-log-validation-rolearquivo.yaml em. GitHub 2. Salve o arquivo no local indicado na seção de modelos do `customizations-config.yaml` arquivo. 3. Abra o arquivo `customizations-config.yaml` . 4. Na `cloudFormationStacks` seção, adicione o código a seguir. Atualize o alvo Região da AWS conforme necessário para sua landing zone: `- deploymentTargets: accounts: - LogArchive`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>descripti
	on: IAM Role to
	 validate Config and
	 Logs
	name:
	 lza-config-log-val
	idation-role
	regions:
	- us-
	east-1
	template:
	 cloudformation/con
	fig-log-validation-
	role.yaml
	runOrder: 1
	terminati
	onProtection: true
	
	parameters:
	- name:
	 pManagementAccount
	Id
	value:
	 "{{ account Managemen
	t }}"</pre> 5. Salve, feche e confirme as alterações feitas no `customizations-con fig.yaml` arquivo.	

(Opcional) Obtenha dados do Microsoft Entra ID

Tarefa	Descrição	Habilidades necessárias
Crie o aplicativo que permite que uma função Lambda se comunique com o Microsoft Entra ID.	1. No centro de administr ação do Microsoft Entra ID, registre o `create_aw s_account` aplicativ	Microsoft Entra ID

Tarefa	Descrição	Habilidades necessárias

	o. Para obter instruções, consulte Registrar um aplicativo na documentação da Microsoft.
	2. Siga as instruções em Atualizar as permissões solicitadas de um aplicativo na documentação da Microsoft para configurar as seguintes permissões do Microsoft Graph para o `create_aws_account` aplicativo:
	• Aplicativo.Read.All
	  • Tipo: Aplicação
	  • É necessário consentimento do administrador: Sim
	• AppRoleAssignment. ReadWrite.Tudo
	  • Tipo: Aplicação
	  • É necessário consentimento do administrador: Sim
	• Grupo. ReadWrite.Tudo
	  • Tipo: Aplicação
	  • É necessário consentimento do administrador: Sim
	• ServicePrincipalEndpoint.Ler. Tudo
	  • Tipo: Aplicação	

Tarefa	Descrição	Habilidades necessárias

	• É necessário consentimento do administrador: Sim
	• Sincronização. ReadWrite.Tudo
	  • Tipo: Aplicação
	  • É necessário consentimento do administrador: Sim
	• User.Read
	  • Tipo: Delegado
	  • É necessário consentimento do administrador: Não	

Tarefa	Descrição	Habilidades necessárias
Recupere valores para o `create_aws_account` aplicativo.	Agora, você recupera os valores necessários para o `create_aws_account` aplicativo. 1. No centro de administração do Microsoft Entra ID, navegue até Registros de aplicativos e escolha `create_aws_account` . 2. No painel esquerdo, escolha Visão geral. 3. Na página Visão geral, anote os seguintes valores: • ID do aplicativo (cliente) • ID do diretório (inquilino) 4. No painel esquerdo, em Gerenciar, escolha Certificados e segredos. 5. Na página Certificados e segredos, escolha a guia Segredos do cliente e anote os seguintes valores: • Valor secreto do cliente • ID secreta do cliente	Microsoft Entra ID
Crie o aplicativo que integra o Microsoft Entra ID com o IAM Identity Center.	No centro de administração do Microsoft Entra ID, registre o `LZA2` aplicativo. Para obter instruções, consulte Registrar um aplicativo na documentação da Microsoft.	Microsoft Entra ID

Tarefa	Descrição	Habilidades necessárias
Recupere valores para o LZA2 aplicativo.	Agora, você recupera os valores necessários para o LZA2 aplicativo. 1. No centro de administração do Microsoft Entra ID, navegue até Aplicativos corporativos e escolhaLZA2. 2. No painel esquerdo, escolha Visão geral. 3. Na página Visão geral, anote os seguintes valores: • Name • ID de objeto 4. No painel esquerdo, em Gerenciar, escolha Manifesto. 5. No arquivo JSON, na `appRoles` seção, localize a função do aplicativo chamada`User`. 6. Anote o `id` valor dessa função do aplicativo.	Microsoft Entra ID

Tarefa	Descrição	Habilidades necessárias

Criar um segredo.	1. No AWS CLI, insira o comando a seguir para criar as variáveis. Use os valores que você recuperou para os LZA2 aplicativos `create_aws_account` e:
	
	`# Variables for create_aws_account app`
	`TENANT_ID='<Directory ID>'`
	`CLIENT_ID='<Application ID>'`
	`SECRET_ID='<Client secret ID>'`
	`SECRET_VALUE='<Client secret value>'`
	
	`# Variables for LZA2 app`
	`OBJECT_ID='<Object ID>'`
	`APP_ROLE_ID='<App role ID>'`
	`ENTERPRISE_APP_NAME='<Name>'`
	
	2. Digite o comando a seguir para criar um segredo chamado `GraphApiSecret` em AWS Secrets Manager:
	
	`aws secretsmanager create-secret \`
	`--name GraphApiSecret \`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre> --secret-string
	 "{\"client_id\":
	 \"${CLIENT_ID}\",
	 \"tenant_id\":
	 \"${TENANT_ID}\",
	 \"object_id\":
	 \"${OBJECT_ID}\",
	 \"app_role_id\":
	 \"${APP_ROLE_ID}\"
	, \"secret_value\":
	 \"${SECRET_VALUE}\
	", \"secret_id\":
	 \"${SECRET_ID}\"}"</pre> Se precisar atualizar o segredo no futuro, você pode atualizar as variáveis e executar o seguinte comando: <pre>aws secretsmanager
	 update-secret \
	  --secret-id
	 GraphApiSecret \
	  --secret-string
	 "{\"client_id\":
	 \"${CLIENT_ID}\",
	 \"tenant_id\":
	 \"${TENANT_ID}\",
	 \"object_id\":
	 \"${OBJECT_ID}\",
	 \"app_role_id\":
	 \"${APP_ROLE_ID}\"
	, \"secret_value\":
	 \"${SECRET_VALUE}\
	", \"secret_id\":
	 \"${SECRET_ID}\"}"</pre>	

Implante a solução

Tarefa	Descrição	Habilidades necessárias

Clone o código-fonte.	1. Digite o seguinte comando para clonar o lza-account-creation-workflowrepositório:
	`git clone https://github.com/aws-samples/lza-account-creation-workflow`
	2. Digite o comando a seguir para navegar até o `config` diretório do repositório clonado:
	`cd lza-account-creation-workflow/config`
		DevOps engenheiro

Para atualizar o arquivo `deploy-config.yaml` .	1. Abra o arquivo `deploy-config.yaml` . 2. Revise o modelo e atualize os valores conforme necessário para implantação em seu AWS ambiente. Por exemplo, atualize valores para o seguinte: • `accountCreationFailure` • `accountCompletionFromEmail` • `ssoLoginUrl` • `rootEmailPrefix` • `rootEmailDomain`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	3. Se você estiver integrando com o Microsoft Entra ID, faça o seguinte: • Defina `enableAzureADIntegration` como `true`. • Para `graphApiSecretName` valor, insira o segredo que você criou anteriormente (`GraphApiSecret`). 4. Salve e feche o arquivo `deploy-config.yaml`.	

Tarefa	Descrição	Habilidades necessárias

Implante a solução em seu AWS ambiente.	1. Digite o comando:
	`cdk bootstrap <account-number>/<Region>`
	Para obter mais informações, consulte Bootstrapping na documentação. AWS CDK
	2. Insira o comando a seguir para sintetizar o CloudFormation modelo:
	`cdk synth`
	Para obter mais informações, consulte Configurar e realizar a síntese de AWS CDK pilha na AWS CDK documentação.
	3. Insira o comando a seguir para implantar a solução.
	`cdk deploy`
	Para obter mais informações, consulte Implantar AWS CDK aplicativos na AWS CDK documentação.
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Note Essa solução usa um bucket do Amazon S3 para armazenar o código-fonte dessa solução. Você pode usar o script upload_to_source_bucket.py para criar um arquivo do código-fonte e fazer upload de uma versão atualizada.	

Opção 1 — Crie uma conta usando Python

Tarefa	Descrição	Habilidades necessárias
Identifique quais argumentos usar.	Escolha quais argumentos usar ao executar o script Python que inicia o fluxo de trabalho Step Functions. Para obter uma lista completa dos argumentos, consulte a seção Informações adicionais desse padrão.	AWS DevOps, Python
Inicie o script Python.	1. Digite o seguinte comando para navegar até o repositório clonado: `cd lza-account-creation-workflow`	DevOps engenheiro, Python

Tarefa	Descrição	Habilidades necessárias
	2. Execute o script Python que inicia o fluxo de trabalho Step Functions. Veja a seguir um exemplo de comando que inclui exemplos de argumentos e valores: `python ./run-stepfunction.py \ --account-name "lza-test-01" \ --support-dl "johnsmith@example.com" \ --managed-org-unit "Workloads/Workload-1" \ --purpose "Testing new micro service" \ --force-update true \ --ad-integration "{\"CustomerAccountAdmin\": \"platform-admin\", \"CustomerAccountDev\": \"workload1-app1\"}" \ --bypass-creation true \ --tags APPLICATION=TestingMicroService` 3. Espere até receber uma notificação de que a conta foi criada com sucesso.	

Tarefa	Descrição	Habilidades necessárias
	Note Se o processo de criação da conta falhar, o Amazon SNS enviará uma notificação para os endereços de e-mail que você define `accountCreationFailure` no `deploy-config.yaml` arquivo. O solicitante da conta não é notificado.	

Opção 2 — Crie uma conta usando o API Gateway e o awscurl

Tarefa	Descrição	Habilidades necessárias
Configure as variáveis para awscurl.	1. Digite o comando a seguir para navegar até o diretório do código-fonte: `cd lza-account-creation-workflow` 2. Digite o comando a seguir para definir as variáveis da chave de AWS acesso. Você pode copiar as variáveis do portal de AWS acesso e depois colá-	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	las em um shell. Veja um exemplo a seguir:
	
	`export AWS_ACCESS_KEY_ID="<id>"`
	`export AWS_SECRET_ACCESS_KEY="<key>"`
	`export AWS_SESSION_TOKEN="<token>"`
	
	3. Insira o comando a seguir para definir o Região da AWS para chamadas de API:
	
	`export AWS_REGION=$(aws configure get region)`
	
	4. Insira o comando a seguir para recuperar o endpoint do API Gateway da `lza-account-creation-workflow-application` CloudFormation saída:
	
	`export API_GATEWAY_ENDPOINT=$(aws cloudformation describe-stacks --stack-name "lza-account-creation-workflow-application" --query 'Stacks[*].Outputs[?OutputKey==`oApiGatewayCreateAccountEndpoin`	

Tarefa	Descrição	Habilidades necessárias
	t`].OutputValue' --output text)	
Verifique a disponibilidade do nome.	Digite o comando a seguir para verificar se o nome está disponível para Conta da AWS o. <AWS_ACCOUNT_NAME> Substitua pelo nome da conta de destino: `awscurl --service execute-api \ --region ${AWS_REGION} \ --access_key ${AWS_ACCESS_KEY_ID} \ --secret_key ${AWS_SECRET_ACCESS_KEY} \ --security_token ${AWS_SESSION_TOKEN} \ -X POST ${API_GATEWAY_ENDPOINT}check_name?account_name=<AWS_ACCOUNT_NAME>`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Execute o fluxo de trabalho de criação da conta.	1. Na pasta raiz do repositório clonado, abra o `api_example.json` arquivo. 2. Atualize os parâmetros com seus valores de configuração: `{ "account_name": "lza-test-01", "account_email": "johnsmith+lzatest01@example.com", "support_dl": "johnsmith@example.com", "managed_org_unit": "Workloads/Workload-1", "ad_integration": [{ "PermissionSetName": "CustomerAccountAdmin", "ActiveDirectoryGroupName": "platform-admin" }, { "PermissionSetName": "CustomerAccountDev", "ActiveDirectoryGroupName": "workload1-app1" }`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>],
	    "force_update":
	 "true",
	    "bypass_c
	reation": "false",
	    "account_tags": [
	        {
	            "Key":
	 "Environment",
	            "Value":
	 "Dev"
	        }, {
	            "Key":
	 "DeploymentMethod",
	            "Value":
	 "ApiGateway"
	        }
	    ]
	}</pre> 3. Salve e feche o arquivo `api_example.json` .
	4. Insira o comando a seguir para iniciar o fluxo de trabalho do Step Functions:
	<pre>awscurl --service
	 execute-api \
	    --data @api-exam
	ple.json \
	    --region ${AWS_REG
	ION} \
	    --access_key
	 ${AWS_ACCESS_KEY_I
	D} \
	    --secret_key
	 ${AWS_SECRET_ACCES
	S_KEY} \
	    --security_token
	 ${AWS_SESSION_TOKE
	N} \</pre>	

Tarefa	Descrição	Habilidades necessárias

	<pre>-X POST ${API_GATEWAY_ENDPOINT}execute</pre>
	5. Na saída do comando anterior, anote a execução de Step Functions Amazon Resource Name (ARN).
	6. Se você quiser verificar o status do fluxo de trabalho do Step Functions, digite o comando a seguir. <STEP_FUNCTION_EXECUTION_NAME> Substitua pelo ARN ou nome de execução do Step Functions:
	<pre>awscurl --service execute-api \
	--region ${AWS_REGION} \
	--access_key ${AWS_ACCESS_KEY_ID} \
	--secret_key ${AWS_SECRET_ACCESS_KEY} \
	--security_token ${AWS_SESSION_TOKEN} \
	-X GET ${API_GATEWAY_ENDPOINT}get_execution_status?execution=<STEP_FUNCTION_EXECUTION_NAME></pre>	

Tarefa	Descrição	Habilidades necessárias
	7. Espere até receber uma notificação de que a conta foi criada com sucesso. **Note** Se o processo de criação da conta falhar, o Amazon SNS enviará uma notificação para os endereços de e-mail que você define `accountCreationFailure` no `deploy-config.yaml` arquivo. O solicitante da conta não é notificado.	

(Opcional) Limpe a solução

Tarefa	Descrição	Habilidades necessárias
Remova objetos dos buckets do Amazon S3.	Remova qualquer objeto nos seguintes buckets do Amazon S3: • `lza-account-creation-work-<CDK_UNIQUE_ID>` • `lza-account-creation-workflow-src-<A`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	WS_REGION>-<AWS_ACCOUNT> • lza-account-creation-workflow-<AWS_REGION>-<AWS_ACCOUNT>	

Exclua a CloudFormation pilha.	Digite o seguinte comando para excluir a CloudFormation pilha:
	`aws cloudformation delete-stack \ --stack-name lza-account-creation-workflow-application`
	`aws cloudformation wait stack-delete-complete \ --stack-name lza-account-creation-workflow-application`
		AWS DevOps

Exclua o pipeline.	Digite o seguinte comando para excluir o `lza-account-creation-workflow-pipeline` pipeline: `cdk destroy lza-account-creation-workflow-pipeline --force`	AWS DevOps

Recursos relacionados

- Landing Zone Accelerator ativado AWS (Biblioteca de AWS soluções)
- Solução de AWS CDK problemas comuns (AWS CDK documentação)

Mais informações

Diagrama do fluxo de trabalho do Step Functions

A imagem a seguir mostra os estados no fluxo de trabalho do Step Functions.

Arguments (Argumentos)

A seguir estão os argumentos que você pode usar ao executar o script Python que inicia o fluxo de trabalho Step Functions.

Os seguintes argumentos são necessários:

- `account-name (-a)`(string) — O nome do novo Conta da AWS.
- `support-dl (-s)`(string) — O endereço de e-mail que recebe a notificação quando o processo de criação da conta é concluído.
- `managed-org-unit (-m)`(string) — A unidade organizacional gerenciada (OU) que conterá a nova conta.

Os argumentos a seguir são opcionais:

- `ad-integration (-ad)`(dicionário de seqüências de caracteres) — O grupo Microsoft Entra ID e o conjunto de permissões atribuído. Veja a seguir um exemplo de como usar esse argumento:

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

- `account-email (-e)`(string) — O endereço de e-mail do usuário raiz do novo Conta da AWS.

> **Note**
>
> Se esse argumento não for usado, um endereço de e-mail será gerado usando os valores `rootEmailPrefix` e `rootEmailDomain` do `configs/deploy-config.yaml` arquivo. Se um endereço de e-mail não for fornecido, um endereço de e-mail é gerado usando o seguinte formato:`rootEmailPrefix+accountName@rootEmailDomain`.

- `region (-r)`(string) — Região da AWS Onde o fluxo de trabalho do Step Functions foi implantado. O valor padrão é `us-east-1`.

- `force-update (-f)`(string Boolean) — Insira `true` para forçar AWS Service Catalog a atualização do produto provisionado.
- `bypass-creation (-b)`(string Boolean) — Digite `true` para ignorar a adição da conta ao `accounts-config.yaml` arquivo e ignorar a execução do pipeline. `AWSAccelerator-Pipeline` Esse argumento geralmente é usado para testar o processo de fluxo de trabalho de criação da conta ou para executar o restante das etapas do Step Functions se ocorrer um erro no `Landing Zone Accelerator` pipeline.
- `tags (-t)`(string) — Tags adicionais que você deseja adicionar ao Conta da AWS. Por padrão, as seguintes tags são adicionadas: `account-name`, `support-dl`, `purpose` e. Veja a seguir um exemplo de como usar esse argumento:

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

Faça o inventário automático de AWS recursos em várias contas e regiões

Criado por Matej Macek (AWS)

Resumo

Esse padrão descreve uma abordagem automatizada para manter um inventário abrangente de AWS recursos em várias contas e. Regiões da AWS Ele foi projetado para ajudar os engenheiros de infraestrutura e segurança a melhorar suas práticas de gerenciamento de recursos. Ele usa AWS Config para monitorar alterações de recursos, o Amazon Athena para consultas e o Amazon QuickSight para painéis interativos. Você implementa essa solução implantando uma AWS CloudFormation pilha.

Essa solução é semelhante à apresentada em Visualização de AWS Config dados usando o Amazon Athena e a QuickSight AmazonAWS (postagem no blog). Esse padrão expande essa solução para atender aos seguintes requisitos comuns e fornecer os seguintes benefícios principais:

- Focada na conformidade — essa abordagem pode ajudá-lo a atender aos requisitos regulatórios, como PCI DSS, NIST SP 800-53, ISO/IEC 27001, HIPAA, GDPR e outros que exigem inventários precisos de ativos.
- Estrutura de personalização — Ela fornece uma base para a criação de QuickSight painéis para vários AWS recursos, para que você possa personalizar a solução de acordo com seus requisitos específicos.
- Aprimoramentos orientados ao usuário — Essa abordagem incorpora feedback de casos de uso do mundo real e atende às solicitações de uma solução mais abrangente.

As equipes de infraestrutura, segurança e finanças geralmente enfrentam desafios de visibilidade e colaboração em ambientes dinâmicos, com várias contas ou várias regiões. Essa solução foi projetada para enfrentar esses desafios e reduzir significativamente o tempo e o esforço necessários para criar e manter um inventário de recursos. O resultado é uma visão centralizada dos recursos que ajuda você a melhorar as decisões de alocação de recursos, identificar e mitigar riscos, otimizar custos e melhorar a visibilidade e a colaboração gerais. Essa abordagem preenche a lacuna entre as soluções conceituais e as necessidades reais de implementação para fins operacionais, de segurança e de conformidade.

Pré-requisitos e limitações

Pré-requisitos

- O seguinte ativo Contas da AWS:
  - Conta de gerenciamento - Uma conta centralizada para cobrança, criação de contas e controle de acesso em toda a organização
  - Conta de auditoria — um hub centralizado para monitoramento de segurança, verificações de conformidade e notificações de desvios
  - Conta de arquivamento de registros — Uma conta centralizada para armazenar e analisar os dados coletados
- Na conta de auditoria, um AWS Config agregador que coleta e agrega dados de configuração de suas contas e regiões de destino
- Na conta de arquivamento de registros, configure o seguinte:
  - Um bucket do Amazon Simple Storage Service (Amazon S3) onde você armazena os dados do agregador AWS Config
  - Uma QuickSight assinatura da Amazon
  - Uma conexão autorizada entre QuickSight e o Amazon Athena
  - Permissões para acessar o bucket do Amazon S3 por meio de uma consulta do Athena
- AWS Command Line Interface (AWS CLI), instalado e configurado
- Permissões para implantar uma CloudFormation pilha que provisiona os seguintes recursos:
  - Uma AWS Lambda função
  - Uma configuração de notificação do Amazon S3
  - Banco de dados, tabelas e visualizações do Athena
  - QuickSight conjuntos de dados e fontes de dados
- Permissões para executar automações em AWS Systems Manager
- Permissões para acessar QuickSight

Limitações

- A solução depende de. AWS Config AWS Config geralmente registra as alterações de configuração em seus recursos logo após a detecção de uma alteração ou na frequência especificada por você. No entanto, isso é feito com base no melhor esforço e às vezes pode levar mais tempo.

- Essa solução rastreia somente os tipos de recursos AWS Config compatíveis.
- A solução não rastreia o inventário de recursos em outros provedores de nuvem ou ambientes locais.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte a página de endpoints e cotas do serviço na AWS documentação e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra um processo simplificado para coletar, organizar, analisar e visualizar dados de configuração e conformidade em várias contas em uma AWS organização.

O diagrama mostra o seguinte fluxo de trabalho:

1. Em um cronograma periódico, o AWS Config agregador coleta dados de configuração e conformidade sobre os recursos nas contas e regiões de destino e, em seguida, entrega os dados ao bucket do Amazon S3 na conta de arquivamento de registros.
2. Adicionar novos AWS Config dados ao bucket do Amazon S3 invoca uma função. AWS Lambda
3. A função Lambda particiona os dados configurando chaves com valores que correspondem à região e à data de cada arquivo de snapshot. Isso ajuda a consultar e processar AWS Glue com eficiência os dados de configuração e conformidade.
4. O Amazon Athena usa um AWS Glue esquema para executar consultas SQL nos dados armazenados no bucket do Amazon S3. Ele utiliza os metadados do esquema AWS Glue para entender a estrutura dos dados.
5. As visualizações no Athena definem e extraem os conjuntos de dados de destino.
6. Os painéis na Amazon QuickSight ajudam você a visualizar e analisar os conjuntos de dados.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS

- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo. Um AWS Config agregador coleta dados AWS Config de configuração e conformidade de várias regiões Contas da AWS .
- AWS Glueé um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados. Esse padrão usa um registro AWS Gluede catálogo de dados e esquema.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala. AWS Systems Manager A automação simplifica as tarefas comuns de manutenção, implantação e remediação para muitos. Serviços da AWS

Repositório de código

O AWS CloudFormation modelo para esse padrão está disponível no GitHub repositório de AWS Config visualização. Este CloudFormation modelo implanta um runbook AWS Systems Manager de automação configurado AWS Config para uso com o Amazon Athena. Essa automação se prepara AWS Glue para se conectar ao bucket designado do Amazon S3, cria visualizações no Amazon Athena e configura a Amazon para visualização do painel. QuickSight

Práticas recomendadas

- Recomendamos que você siga as melhores práticas em Configurar e governar um AWS ambiente seguro com várias contas sem orientação AWS Control Tower AWS prescritiva.
- Recomendamos que você crie um AWS Config agregador que colete dados de configuração e conformidade de toda AWS a organização. Para obter mais informações, consulte Agregação de dados multirregionais de várias contas na documentação. AWS Config
- Antes de implantar essa solução, recomendamos que você revise as informações de preços atuais do Amazon S3 AWS Config, Athena e. QuickSight

Épicos

Implante a CloudFormation pilha

Tarefa	Descrição	Habilidades necessárias
Baixe o CloudFormation modelo.	Baixe o modelo Config-QuickSight CloudFormation -Visualization-ssm-automation.yaml.	Administrador da AWS, administrador de nuvem, DevOps engenheiro
Modifique o CloudFormation modelo.	Conclua esta etapa somente se você estiver usando AWS Control Towere AWS Config for gerenciado por AWS Control Tower. Você precisa modificar o CloudFormation modelo. 1. Faça login na conta de gerenciamento do . 2. Abra o console de AWS Organizations. 3. Navegue até a página Settings (Configurações). Essa página exibe detalhes	DevOps engenheiro, administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	sobre a organização, incluindo o ID da organização.
	4. Copie o ID da organização.
	5. No editor de texto de sua preferência, abra o arquivo Config- QuickSight -Visualization-ssm-automation.yaml.
	6. Encontre a seguinte linha:
	`return re.match( '^AWSLogs/(\d+)/Config/([\w-]+)/(\d+)/(\d+)/(\d+)/(\d+)/ConfigSnapshot/[^\\\]+$', object_key)`
	7. Substitua essa linha pela seguinte, onde <ORGANIZATION_ID> está a ID que você copiou anteriormente:
	`return re.match( '^<ORGANIZATION_ID>/AWSLogs/(\d+)/Config/([\w-]+)/(\d+)/(\d+)/(\d+)/(\d+)/ConfigSnapshot/[^\\\]+$', object_key)`
	8. Salve e feche o arquivo Config- QuickSight -Visualization-ssm-automation.yaml.	

Tarefa	Descrição	Habilidades necessárias
Crie uma CloudFormation pilha.	Siga as instruções em Criar uma pilha a partir do CloudFormation console. Observe o seguinte: 1. Escolha Carregar um arquivo de modelo e, em seguida, escolha o arquivo YAML que você baixou. 2. Para Stack name (Nome da pilha), insira `Config-QuickSight-Visualization-SSM-Automation` . 3. Selecione Enviar.	Administrador da AWS, administrador de nuvem, DevOps engenheiro

Execute a automação no Systems Manager

Tarefa	Descrição	Habilidades necessárias
Encontre seu nome QuickSight de usuário.	1. Abra o console de QuickSight . 2. Abra o menu do perfil. 3. Anote o nome do usuário. Você precisará desse valor posteriormente.	Administrador da AWS, administrador de nuvem, DevOps engenheiro
Encontre o nome do canal de entrega e o nome do bucket do Amazon S3.	1. No AWS CLI, digite o seguinte comando: `aws configservice describe-delivery-channels`	Administrador da AWS, administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	2. Anote o nome do bucket do Amazon S3 e o nome do seu canal de AWS Config entrega. Você precisará desses valores mais tarde.	

Tarefa	Descrição	Habilidades necessárias
Execute a automação no Systems Manager.	1. Abra o console de AWS Systems Manager. 2. No painel de navegação, escolha Documents. 3. Escolha Owned by me (De minha propriedade). 4. Escolha Config- -Visualiz ation. QuickSight 5. Escolha Execute automatio n. 6. Na seção Parâmetros de entrada, insira seus valores para os seguintes parâmetros: • `ConfigDeliveryChan nelName` — Insira o nome do seu canal AWS Config de entrega. Esse parâmetro é obrigatório. • `ConfigS3BucketLoca tion` — Insira o nome do bucket do Amazon S3 em que você armazena os dados de AWS Config configuração. Esse parâmetro é obrigatório. • `QuickSightUserName` — Insira um nome de usuário que tenha acesso administrativo QuickSigh t a. Esse parâmetro é obrigatório.	Administrador da AWS, administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• `AutomationAssumeRole` — O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Esse parâmetro é opcional. Deixe esse parâmetro em branco. • `DeleteConfigVisualization` — Escolha `false`. 7. Clique em Executar.	

Visualize dados na Amazon QuickSight

Tarefa	Descrição	Habilidades necessárias
Atualize os dados.	Para agendar atualizações do conjunto de dados de acordo com seus requisitos específicos, siga as instruções em Atualização de dados do SPICE.	Administrador da AWS, DevOps engenheiro, administrador de nuvem
Crie uma análise do .	Para criar um painel QuickSight que ajude você a visualizar os recursos, siga as instruções em Iniciando uma análise na Amazon QuickSight.	QuickSight administrador

Tarefa	Descrição	Habilidades necessárias
Crie um dashboard.	1. Depois de concluir a modificação da QuickSigh t análise, siga as instruçõe s em Publicação de painéis para criar um painel. Um painel é uma análise que você pode compartilhar com outros QuickSight usuários. 2. Siga as instruções em Conceder acesso a um painel para compartilhar o painel com seus QuickSight usuários-alvo.	QuickSight administrador

Limpar (opcional)

Tarefa	Descrição	Habilidades necessárias
Exclua os recursos criados pela automação do Systems Manager.	1. Abra o console de AWS Systems Manager. 2. No painel de navegação, escolha Documents. 3. Escolha Owned by me (De minha propriedade). 4. Escolha Config- -Visualiz ation. QuickSight 5. Escolha Execute automatio n. 6. Na seção Parâmetros de entrada, para o `DeleteCon figVisualization` parâmetro, insira`true`.	Administrador da AWS, administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	7. Clique em Executar.	
Exclua a CloudFormation pilha.	Para excluir os recursos na `Config-QuickSight-Visualization-SSM-Automation` pilha, siga as instruções em Excluir uma pilha do CloudFormation console.	Administrador da AWS, administrador de nuvem, DevOps engenheiro

Solução de problemas

Problema	Solução

QuickSight A Amazon está tentando se conectar ao `us-east-1` Região da AWS, mas a criação de recursos nessa região não é permitida.	Uma política de controle de serviços está restringindo sua assinatura da Amazon QuickSight nesta região. Na política de controle de serviço, especifique manualmente o alvo Região da AWS. `<REGION_ID>` Substitua pelo identificador de região apropriado:
	`https://<REGION_ID>.quicksight.aws.amazon.com/sn/start/dashboards`
	Veja um exemplo a seguir:
	`https://eu-central-1.quicksight.aws.amazon.com/sn/start/dashboards`

No Amazon Athena, você encontra a seguinte mensagem: `Before you run your first query, you need to set up a query result location in Amazon S3.`	Certifique-se de ter preparado um bucket do Amazon S3 onde você armazenará os resultados da consulta do Amazon Athena. Em seguida, siga as instruções em Especific

Problema	Solução
	ar um local do resultado da consulta usando o console do Amazon Athena.

Recursos relacionados

AWS documentação

- AWS Config documentação
- QuickSight Documentação da Amazon

AWS postagem no blog

- Automatize a visualização AWS Config de dados com AWS Systems Manager
- Como registrar alterações na configuração de recursos periodicamente com AWS Config

Outros recursos

- Centro de aprendizagem QuickSight comunitária da Amazon
- Galeria QuickSight da Comunidade Amazon

Configure os logs de fluxo da VPC para centralização em todas as contas da AWS

Criado por Benjamin Morris (AWS) e Aman Kaur Gandhi (AWS)

Resumo

Em uma nuvem privada virtual (VPC) da Amazon Web Services (AWS), o atributo VPC Flow Logs pode fornecer dados úteis para solução de problemas operacionais e de segurança. No entanto, há limitações no uso de logs de fluxo de VPC em um ambiente com várias contas. Especificamente, os registros de fluxo entre contas do Amazon CloudWatch Logs não são suportados. Em vez disso, centralize os logs configurando um bucket do Amazon Simple Storage Service (Amazon S3) com a política de bucket apropriada.

> **Note**
>
> Esse padrão discute os requisitos para enviar registros de fluxo para um local centralizado. No entanto, se você também quiser que os logs estejam disponíveis localmente nas contas dos membros, você pode criar vários logs de fluxo para cada VPC. Usuários sem acesso à conta do Log Archive podem ver os registros de tráfego para solucionar problemas. Como alternativa, você pode configurar um único registro de fluxo para cada VPC que envia registros para CloudWatch o Logs. Em seguida, você pode usar um filtro de assinatura do Amazon Data Firehose para encaminhar os registros para um bucket do S3. Para obter mais informações, consulte a seção Recursos relacionados.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma organização da AWS Organizations com uma conta usada para centralizar registros (por exemplo, Log Archive)

Limitações

Se você usar a chave gerenciada `aws/s3` do AWS Key Management Service (AWS KMS) para criptografar seu bucket central, ele não receberá logs de uma conta diferente. Em vez disso, você

verá um código de `Unsuccessful` erro 400 com uma mensagem como `"LogDestination: <bucketName> is undeliverable"` a sua`ResourceId`.

Isso ocorre porque as chaves gerenciadas pela AWS de uma conta não podem ser compartilhadas entre contas.

A solução é usar a criptografia gerenciada pelo Amazon S3 (SSE-S3) ou uma chave gerenciada pelo cliente do AWS KMS que você possa compartilhar com as contas dos membros.

Arquitetura

Pilha de tecnologias de destino

No diagrama a seguir, dois logs de fluxo são implantados para cada VPC. Um envia registros para um grupo local CloudWatch de registros. O outro envia logs para um bucket do S3 em uma conta de registro centralizada. A política de bucket permite que o serviço de entrega de logs grave registros no bucket.

> **Note**
>
> A partir de novembro de 2023, AWS agora oferece suporte à chave de condição aws: SourceOrg ID. Essa condição permite que você negue a gravação no bucket centralizado para contas fora da sua AWS Organizations organização.

Arquitetura de destino

Automação e escala

Cada VPC é configurada para enviar logs para o bucket do S3 na conta de registro central. Use uma das seguintes soluções de automação para ajudar a garantir que os logs de fluxo sejam configurados adequadamente:

- AWS CloudFormation StackSets
- AWS Control Tower Account Factory for Terraform (AFT)
- Uma regra do AWS Config com remediação

Ferramentas

Ferramentas

- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas, aplicativos e serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS. Este padrão usa o atributo VPC Flow Logs para capturar informações sobre o tráfego de IP de e para as interfaces de rede do em sua VPC.

Práticas recomendadas

Usar a infraestrutura como código (IaC) pode simplificar muito o processo de implantação do VPC Flow Logs. Abstrair suas definições de implantação de VPC para incluir uma construção de recurso de log de fluxo implantará VPCs sua com registros de fluxo automaticamente. Isso é demonstrado na próxima seção.

Logs de fluxo centralizados

Exemplo de sintaxe para adicionar registros de fluxo centralizados a um módulo VPC no Terraform HashiCorp

Esse código cria um registro de fluxo que envia logs de uma VPC para um bucket S3 centralizado. Observe que esse padrão não abrange a criação do bucket do S3.

Para obter declarações de política de bucket recomendadas, consulte a seção Informações adicionais.

```
variable "vpc_id" { type = string }
locals { custom_log_format_v5 = "$${version} $${account-id} $${interface-id} $
${srcaddr} $${dstaddr} $${srcport} $${dstport} $${protocol} $${packets} $${bytes}
 $${start} $${end} $${action} $${log-status} $${vpc-id} $${subnet-id} $${instance-
id} $${tcp-flags} $${type} $${pkt-srcaddr} $${pkt-dstaddr} $${region} $${az-id} $
```

```
${sublocation-type} $${sublocation-id} $${pkt-src-aws-service} $${pkt-dst-aws-service}
 $${flow-direction} $${traffic-path}" }
resource "aws_flow_log" "centralized_flow_log" {
  log_destination      = "arn:aws:s3:::centralized-vpc-flow-logs-
<log_archive_account_id>" # Optionally, a prefix can be added after the ARN.
  log_destination_type = "s3"
  traffic_type         = "ALL"
  vpc_id               = var.vpc_id
  log_format           = local.custom_log_format_v5 # If you want fields from VPC Flow
 Logs v3+, you will need to create a custom log format.
}
```

Para obter mais informações sobre o formato de log personalizado, consulte a documentação da AWS.

Registros de fluxo locais

Exemplo de sintaxe para adicionar logs de fluxo locais a um módulo VPC no Terraform com as permissões necessárias

Esse código cria um registro de fluxo que envia registros de uma VPC para um grupo local de CloudWatch registros.

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

```
  "Version": "2012-10-17",
  "Statement": [{
      "Action": ["logs:CreateLog*", "logs:PutLogEvents", "logs:DescribeLog*",
 "logs:DeleteLogDelivery"],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:${data.aws_region.current.name}:*:log-group:vpc-flow-
logs*"
  }]
}
EOF
}
resource "aws_cloudwatch_log_group" "local_flow_logs" {
  name              = "vpc-flow-logs/${var.vpc_id}"
  retention_in_days = 30
}
resource "aws_flow_log" "local_flow_log" {
  iam_role_arn    = aws_iam_role.local_flow_log_role.arn
  log_destination = aws_cloudwatch_log_group.local_flow_logs.arn
  traffic_type    = "ALL"
  vpc_id          = var.vpc_id
}
```

Épicos

Implemente a infraestrutura da VPC Flow Logs

Tarefa	Descrição	Habilidades necessárias
Determine a estratégia de criptografia e crie a política para o bucket central do S3.	O bucket central não é compatível com a chave `aws/s3` do AWS KMS, então você deve usar o SSE-S3 ou uma chave gerenciada pelo cliente do AWS KMS. Se você usar uma chave do AWS KMS, a política de chave deve permitir que as contas de membros usem a chave.	Compliance
Crie o bucket de log de fluxo central.	Crie o bucket central para o qual os logs de fluxo serão	AWS geral

Tarefa	Descrição	Habilidades necessárias
	enviados e aplique a estratégia de criptografia que você escolheu na etapa anterior. Isso deve estar em um arquivo de log ou em uma conta com finalidade semelhante. Obtenha a política do bucket na seção Informações adicionais e aplique-a ao seu bucket central depois de atualizar os espaços reservados com os valores específicos do seu ambiente.	
Configure os logs de fluxo da VPC para enviar logs para o bucket central de logs de fluxo.	Adicione logs de fluxo a cada VPC da qual você deseja coletar dados. A maneira mais escalável de fazer isso é usar ferramentas de IaC, como AFT ou AWS Cloud Development Kit (AWS CDK). Por exemplo, você pode criar um módulo do Terraform que implanta uma VPC junto com um log de fluxo. Se necessário, você adiciona os logs de fluxo manualmente.	Administrador de rede

Tarefa	Descrição	Habilidades necessárias
Configure os registros de fluxo da VPC para enviar aos registros locais CloudWatch .	(Opcional) Se você quiser que os registros de fluxo fiquem visíveis nas contas em que os registros estão sendo gerados, crie outro registro de fluxo para enviar dados para o CloudWatch Logs na conta local. Como alternativa, você pode enviar os dados para um bucket S3 específico da conta na conta local.	AWS geral

Recursos relacionados

- Como facilitar a análise de dados e atender aos requisitos de segurança usando dados de log de fluxo centralizados (publicação no blog)
- Como habilitar automaticamente os logs de fluxo da VPC usando as regras do AWS Config (publicação no blog)

Mais informações

Política de bucket

Esse exemplo de política de bucket pode ser aplicado ao bucket central do S3 para logs de fluxo, depois de adicionar valores para nomes de espaço reservado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
```

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

Marque anexo do gateway de trânsito automaticamente usando o AWS Organizations

Criado por Richard Milner-Watts (AWS), Haris Bin Ayub (AWS) e John Capps (AWS)

Resumo

Na Amazon Web Services (AWS), você pode usar AWS Resource Access Managerpara compartilhar Conta da AWS além AWS Transit Gatewaydos limites. No entanto, quando você cria anexo do gateway de trânsito além dos limites da conta, os anexos são criados sem uma tag de nome. Isso pode tornar a identificação de anexos demorada.

Essa solução fornece um mecanismo automatizado para coletar informações sobre cada anexo do Transit Gateway para contas em uma organização gerenciada pela AWS Organizations. O processo inclui pesquisar o intervalo Encaminhamento Entre Domínios Sem Classificação (CIDR) na tabela de rotas do Transit Gateway. Em seguida, a solução aplica uma tag de nome na forma de `<CIDR-range>-<AccountName>` ao anexo na conta que contém o Transit Gateway.

Essa solução pode ser usada junto com uma solução como o Serverless Transit Network Orchestrator da Solutions Library. AWS O Serverless Transit Network Orchestrator permite a criação automatizada de anexos do Transit Gateway Gateway em grande escala.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Uma AWS Organizations organização que contém todas as contas relacionadas
- Acesso à conta de gerenciamento da organização, sob a raiz da organização, para criar a função AWS Identity and Access Management (IAM) necessária
- Uma conta de membro da Rede Compartilhada contendo um ou mais gateways de trânsito que são compartilhados com a organização e têm anexos

Arquitetura

A captura de tela a seguir AWS Management Console mostra exemplos de anexos do Transit Gateway sem etiqueta de nome associada e dois anexos do Transit Gateway com etiquetas de nome geradas por essa solução. A estrutura da tag de nome gerada é `<CIDR-range>-<AccountName>`.

Essa solução é usada AWS CloudFormationpara implantar um AWS Step Functionsfluxo de trabalho que gerencia a criação de tags de nome do Transit Gateway em todas as configurações Regiões da AWS. O fluxo de trabalho invoca AWS Lambdafunções, que executam as tarefas subjacentes.

Depois que a solução obtém os nomes das contas AWS Organizations, a máquina de estado Step Functions obtém todos os anexos do Transit Gateway IDs. Eles são processados paralelamente por região. Esse processamento inclui a pesquisa do intervalo CIDR para cada anexo. O intervalo CIDR é obtido pesquisando nas tabelas de rotas do Transit Gateway na região por uma ID de anexo do gateway de trânsito correspondente. Se todas as informações necessárias estiverem disponíveis, a solução aplicará uma tag de nome ao anexo. A solução não substituirá nenhuma tag de nome existente.

A solução é executada em um cronograma controlado por um EventBridge evento da Amazon. O evento inicia a solução todos os dias às 06:00 UTC.

Pilha de tecnologias de destino

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

Arquitetura de destino

A arquitetura da solução e o fluxo de trabalho são mostrados no diagrama a seguir.

1. O evento agendado inicia a regra.
2. A EventBridge regra inicia a máquina de estado Step Functions.
3. A máquina de estado invoca a `tgw-tagger-organizations-account-query` função do Lambda.
4. A função do Lambda `tgw-tagger-organizations-account-query` assume a função na conta de gerenciamento da organização.

5. A função `tgw-tagger-organizations-account-query` Lambda chama a API Organizations para retornar Conta da AWS metadados.
6. A máquina de estado invoca a `tgw-tagger-attachment-query` função do Lambda.
7. Para cada região, paralelamente, a máquina de estado invoca a função do Lambda `tgw-tagger-rtb-query` para ler o intervalo CIDR de cada anexo.
8. Para cada região, paralelamente, a máquina de estado invoca a função do Lambda `tgw-tagger-attachment-tagger`.
9. As tags de nome são criadas para anexo do gateway de trânsito na conta da Rede Compartilhada.

Automação e escala

A solução processa cada região em paralelo para reduzir a duração total da execução.

Ferramentas

Serviços da AWS

- AWS CloudFormationfornece uma maneira de modelar uma coleção de recursos relacionados AWS e de terceiros, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida, tratando a infraestrutura como código.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos em que você executa AWS em tempo real.
- EventBridgeA Amazon é um serviço de barramento de eventos sem servidor que você pode usar para conectar seus aplicativos a dados de várias fontes. EventBridge recebe um evento, um indicador de uma mudança no ambiente, e aplica uma regra para rotear o evento até um alvo. As regras fazem a correspondência entre os eventos e os destinos com base na estrutura do evento, chamada padrão do evento ou em um schedule.
- AWS Lambdaé um serviço de computação que oferece suporte à execução de código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia a milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando seu código não estiver em execução.
- AWS Organizationsajuda você a gerenciar e governar centralmente seu ambiente à medida que você cresce e escala seus AWS recursos. Usando o Organizations, você pode criar recursos novos Contas da AWS e alocar programaticamente, agrupar contas para organizar seus fluxos de

trabalho, aplicar políticas a contas ou grupos para fins de governança e simplificar o faturamento usando um único método de pagamento para todas as suas contas.

- AWS Step Functionsé um serviço de fluxo de trabalho visual de baixo código usado para orquestrar Serviços da AWS, automatizar processos de negócios e criar aplicativos sem servidor. Os fluxos de trabalho gerenciam falhas, novas tentativas, paralelização, integrações de serviços e observabilidade para que os desenvolvedores possam se concentrar em uma lógica de negócios de maior valor.
- AWS Transit Gatewayconexões VPCs e redes locais por meio de um hub central. Isso simplifica sua rede e acaba com relacionamentos complexos de peering. Ele atua como um roteador na nuvem, de forma que cada nova conexão seja feita apenas uma vez.
- A Amazon Virtual Private Cloud (Amazon VPC) é um serviço para lançar AWS recursos em uma rede virtual logicamente isolada que você define.
- AWS X-Raycoleta dados sobre solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter insights sobre esses dados para identificar problemas e oportunidades de otimização.

Código

O código-fonte dessa solução está disponível no GitHub repositório Transit Gateway Attachment Tagger. O repositório inclui os seguintes arquivos:

- `tgw-attachment-tagger-main-stack.yaml` cria todos os recursos para oferecer suporte a essa solução na conta de rede compartilhada.
- `tgw-attachment-tagger-organizations-stack.yaml` cria uma função na conta de gerenciamento da organização.

Épicos

Implemente a pilha principal de soluções

Tarefa	Descrição	Habilidades necessárias
Reúna as informações necessárias sobre os pré-requisitos.	Para configurar o acesso entre contas da função Lambda AWS Organizations à API, você precisa do ID da	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	conta de gerenciamento da organização. **Note** A ordem na qual as duas AWS CloudFormation pilhas são criadas é importante. Primeiro, você deve implantar recursos na conta de rede compartilhada. A função na conta de rede compartilhada já deve existir antes de implantar recursos na conta de gerenciamento da organização. Para obter mais informações, consulte a documentação do AWS.	

Tarefa	Descrição	Habilidades necessárias
Inicie o AWS CloudFormation modelo para a pilha principal de soluções.	O modelo para a pilha principal de soluções implantará as funções do IAM, o fluxo de trabalho Step Functions, as funções Lambda e o evento da Amazon CloudWatch . Abra o AWS Management Console para a conta de Rede Compartilhada e, em seguida, abra o console: &CFN. Crie a pilha usando o modelo `tgw-attachment-tagger-main-stack.yaml` e especificando os seguintes valores: • Nome da pilha — tgw-attachment-tagger-main -stack • awsOrganizationsRootAccountId— ID da conta de gerenciamento da organização • TGWRegionsparâmetro — Regiões da AWS para a solução, inserido como uma string delimitada por vírgula • TGWListparâmetro — Gateway de trânsito IDs a ser excluído da solução, inserido em uma string delimitada por vírgula	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações sobre o lançamento de uma AWS CloudFormation pilha, consulte a AWS documentação.	
Verifique se a solução foi iniciada com sucesso.	Aguarde até que a CloudFormation pilha alcance o status CREATE_COMPLETE. Isso deve levar menos de um minuto. Abra o console Step Functions e verifique se uma nova máquina de estado foi criada com o nome tgw-attachment-tagger-state-machine.	DevOps engenheiro

Implante a pilha do AWS Organizations

Tarefa	Descrição	Habilidades necessárias
Reúna as informações necessárias sobre os pré-requisitos.	Para configurar o acesso entre contas da função do Lambda à API do AWS Organizations, você precisa do ID da conta da rede compartilhada.	DevOps engenheiro
Inicie o CloudFormation modelo para a pilha Organizations	O modelo da pilha do AWS Organizations implantará o perfil do IAM na conta de gerenciamento da organização. Acesse o console da AWS para a conta de gerenciam	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ento da organização e, em seguida, abra o CloudFormation console. Crie a pilha usando o modelo `tgw-attachment-tagger-organizations-stack.yaml` e especificando os seguintes valores: • Nome da pilha — tgw-attachment-tagger-organizations-stack • NetworkingAccountIdparâmetro — ID da conta da rede compartilhada Para as outras opções de criação de pilha, use os padrões.	
Verifique se a solução foi iniciada com sucesso.	Aguarde até que a AWS CloudFormation pilha alcance o status CREATE_COMPLETE. Isso deve levar menos de um minuto. Abra o console AWS Identity and Access Management (IAM) e verifique se uma nova função foi criada com o nome tgw-attachment-tagger-organization-query-role.	DevOps engenheiro

Verifique a solução

Tarefa	Descrição	Habilidades necessárias
Execute uma máquina de estado.	Abra o console Step Functions para a conta Shared Networking e escolha State machines no painel de navegação. Selecione a máquina de estado tgw-attachment-tag ger-state-máquina e escolha Iniciar execução. Como a entrada para essa máquina de estado não é usada pela solução, você pode usar o valor padrão. `{ "Comment": "Insert your JSON here" }` Escolha Start Execution.	DevOps engenheiro
Observe a máquina de estado até a conclusão.	Na nova página que se abre, você pode assistir à execução da máquina de estado. A duração dependerá do número de anexos do gateway de trânsito a serem processad os. Nesta página, você pode examinar cada etapa da máquina de estado. Você	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	pode visualizar as várias tarefas na máquina de estado e seguir os links para os CloudWatch registros das funções do Lambda. Para as tarefas que são executadas paralelamente no mapa, você pode usar a lista suspensa Índice para visualizar as implementações específicas para cada região.	
Verifique as etiquetas de anexo do gateway de trânsito.	Abra o console VPC da conta de rede compartilhada e escolha anexo do gateway de trânsito. No console, uma tag de nome é fornecida para anexos que atendem aos critérios (o anexo é propagado para uma tabela de rotas do Transit Gateway e o proprietá rio do recurso é membro da organização).	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Verifique o início CloudWatch do evento.	Aguarde o início do CloudWatch evento. Isso está programado para às 06:00 UTC. Em seguida, abra o console Step Functions para a conta Shared Networking e escolha State machines no painel de navegação. Selecione a máquina de estado tgw-attachment-tag ger-state-máquina. Verifique se a solução foi executada às 06:00 UTC.	DevOps engenheiro

Recursos relacionados

- AWS Organizations
- AWS Resource Access Manager
- Orquestrador de rede de trânsito com tecnologia sem servidor
- Criação de perfis do IAM
- Criando uma pilha no console AWS CloudFormation

Mais padrões

- Provisione AWS Service Catalog produtos com base em AWS CloudFormation modelos usando GitHub Ações
- Provisione funções do IAM com privilégios mínimos implantando uma solução de máquina de venda automática de funções

IA e aprendizado de máquina

Tópicos

- Dados agregados no Amazon DynamoDB para previsão de ML no Athena
- Associe um AWS CodeCommit repositório em um Conta da AWS com o Amazon SageMaker AI Studio Classic em outra conta
- Extraia automaticamente conteúdo de arquivos PDF usando o Amazon Textract
- Crie um modelo de previsão de inicialização a frio usando o DeepAR para séries temporais no SageMaker Amazon AI Studio Lab
- Crie um MLOps fluxo de trabalho usando o Amazon SageMaker AI e o Azure DevOps
- Configure o registro de invocação de modelo no Amazon Bedrock usando AWS CloudFormation
- Crie uma imagem de contêiner Docker personalizada SageMaker e use-a para treinamento de modelos no AWS Step Functions
- Use agentes do Amazon Bedrock para automatizar a criação de controles de entrada de acesso no Amazon EKS por meio de prompts baseados em texto
- Implemente um caso de uso do RAG AWS usando o Terraform e o Amazon Bedrock
- Implante a lógica de pré-processamento em um modelo de ML em um único endpoint usando um pipeline de inferência na Amazon SageMaker
- Desenvolva assistentes avançados baseados em bate-papo com IA generativa usando RAG e prompting ReAct
- Desenvolva um assistente baseado em bate-papo totalmente automatizado usando agentes e bases de conhecimento do Amazon Bedrock
- Documente o conhecimento institucional a partir de entradas de voz usando o Amazon Bedrock e o Amazon Transcribe
- Gere recomendações personalizadas e reclassificadas usando o Amazon Personalize
- Simplifique os fluxos de trabalho de aprendizado de máquina, do desenvolvimento local aos experimentos escaláveis, usando SageMaker IA e Hydra
- Treine e implante um modelo de ML personalizado compatível com GPU na Amazon SageMaker
- Traduza a linguagem natural em consultas DSL para consultas OpenSearch e Elasticsearch
- Use o Amazon Q Developer como assistente de codificação para aumentar sua produtividade
- Use o SageMaker processamento para engenharia de recursos distribuídos de conjuntos de dados de ML em escala de terabytes

- Visualize os resultados do modelo de IA/ML usando o Flask e o AWS Elastic Beanstalk
- Mais padrões

Dados agregados no Amazon DynamoDB para previsão de ML no Athena

Criado por Sachin Doshi (AWS) e Peter Molnar (AWS)

Resumo

Esse padrão mostra como criar agregações complexas de dados da Internet das Coisas (IoT) em uma tabela do Amazon DynamoDB usando o Amazon Athena. Você também aprende como enriquecer os dados com inferência de aprendizado de máquina (ML) usando a Amazon SageMaker AI e como consultar dados geoespaciais usando o Athena. Você poderá usar esse padrão como base para criar uma solução de previsão de ML que atenda aos requisitos da sua organização.

Para fins de demonstração, esse padrão usa um cenário de exemplo de uma empresa que opera um compartilhamento de scooters e deseja prever o número ideal de scooters que deverão ser implantados para clientes em diferentes bairros urbanos. A empresa usa um modelo de ML pré-treinado que prevê a demanda do cliente na próxima hora com base nas últimas quatro horas. O cenário usa um conjunto de dados público do Departamento de Inovação e Tecnologia Cívica da Prefeitura da região metropolitana de Louisville. Os recursos para esse cenário estão disponíveis em um GitHub repositório.

Pré-requisitos e limitações

- Um ativo Conta da AWS
- Permissões para criar uma AWS CloudFormation pilha com funções AWS Identity and Access Management (IAM) para o seguinte:
  - Bucket do Amazon Simple Storage Service (Amazon S3)
  - Athena
  - DynamoDB
  - SageMaker IA
  - AWS Lambda

Arquitetura

Pilha de tecnologia

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

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para criar agregações complexas de dados no DynamoDB usando os recursos de consulta do Athena, uma função Lambda, armazenamento Amazon S3, um endpoint de IA e um painel. SageMaker QuickSight

O diagrama mostra o seguinte fluxo de trabalho:

1. Uma tabela do DynamoDB ingere dados de IoT transmitidos de uma frota de patinetes.
2. Uma função do Lambda carrega a tabela do DynamoDB com os dados ingeridos.
3. Uma consulta do Athena cria uma nova tabela do DynamoDB para os dados geoespaciais que representam os bairros urbanos.
4. O local da consulta é salvo em um bucket do S3.
5. Uma função Athena consulta a inferência de ML do endpoint de SageMaker IA que hospeda o modelo de ML pré-treinado.
6. O Athena consulta dados diretamente das tabelas do DynamoDB e agrega os dados para análise.
7. Um usuário visualiza a saída dos dados analisados em um QuickSight painel.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.

- O Amazon SageMaker AI é um serviço gerenciado de ML que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Repositório de código

O código desse padrão está disponível no repositório GitHub Use ML predictions over Amazon DynamoDB with Amazon Athena ML. Você pode usar o CloudFormation modelo do repositório para criar os seguintes recursos usados no cenário de exemplo:

- Uma tabela do DynamoDB
- Uma função do Lambda para carregar a tabela com dados pertinentes
- Um endpoint de SageMaker IA para solicitações de inferência, com o XGBoost modelo pré-treinado que é armazenado no Amazon S3
- Um grupo de trabalho do Athena chamado `V2EngineWorkGroup`
- Consultas Athena nomeadas para pesquisar os shapefiles geoespaciais e prever a demanda de scooters
- Um conector pré-construído do Amazon Athena DynamoDB que permite que o Athena se comunique com o DynamoDB e AWS SAM usa () para criar o aplicativo em referência ao conector AWS Serverless Application Model do DynamoDB

Épicos

Obtenha o conjunto de dados de exemplo

Tarefa	Descrição	Habilidades necessárias
Baixe o conjunto de dados e os recursos.	1. Baixe um conjunto de dados públicos de aluguéis de veículos sem doca. Para fins de demonstração, esses dados são pré-preenchidos no DynamoDB como parte do caso de uso, mas em um ambiente de produção você envia esses dados para o DynamoDB por meio de vários mecanismos, como dispositivos IoT ou consumidores do Amazon Kinesis. Esses mecanismos usam o Lambda para inserir dados no DynamoDB. 2. Baixe os shapefiles GIS que representam os limites dos bairros históricos e culturais da cidade de Louisville, Kentucky (KY), EUA. O conjunto de dados público é fornecido pelo Consórcio de Informações de Louisville e Jefferson County, KY. Os shapefiles originais já foram convertidos em um arquivo de texto que você pode consultar com o Athena, mas você	Desenvolvedor de aplicativos, cientista de dados

Tarefa	Descrição	Habilidades necessárias
	pode encontrar o código Python para transformar os shapefiles no notebook Jupyter em Geo-Spatial processing of GIS shapefiles with Amazon Athena in. GitHub 3. Baixe o código Python pré-treinado que treina o modelo de ML para previsões de hora em hora usando SageMaker IA e Athena. 4. Obtenha a consulta SQL no Athena que reúne tudo para previsões em tempo real a partir dos dados armazenados no DynamoDB. 5. (Opcionalmente) Use QuickSight para visualizar dados geoespaciais em um mapa de Louisville, Kentucky.	

Use um CloudFormation modelo para implantar os recursos necessários

Tarefa	Descrição	Habilidades necessárias
Crie uma CloudFormation pilha.	1. Baixe o CloudFormation modelo do GitHub repositório.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	2. **Note** Faça login no e AWS Managemen t Console, em seguida, escolha `us-east-1` . : O modelo de ML é armazenado no Amazon Elastic Container Registry (Amazon ECR) para `us-east-1` Região da AWS o, mas o padrão é independente de região. Você pode replicar o padrão em qualquer região em que os Serviços da AWS usados nesse padrão sejam suportados. 3. Abra o CloudFormation console e escolha Pilhas no painel de navegação. 4. escolha Criar pilha e, em seguida, escolha Com recursos existentes (importar recursos). 5. Na página Identificar recursos, escolha Próximo.	

Tarefa	Descrição	Habilidades necessárias
	6. Na seção Especificar modelo, em Origem do modelo, selecione Carregar um arquivo de modelo. 7. Escolha Arquivo e, em seguida, escolha o CloudFormation modelo que você baixou anteriormente. 8. Escolha Avançar, aceite os valores padrão dos parâmetros e escolha Avançar para percorrer o restante do assistente de configuração. 9. Marque a caixa de seleção Eu reconheço que AWS CloudFormation pode criar recursos do IAM com nomes personalizados. 10. Selecione Criar pilha. **Note** A CloudFormation pilha pode levar de 15 a 20 minutos para criar esses recursos.	

Tarefa	Descrição	Habilidades necessárias
Verifique a CloudFormation implantação.	Para verificar se os dados de amostra do CloudFormation modelo estão carregados no DynamoDB, faça o seguinte: 1. Abra o Console do DynamoDB e depois escolha Tabelas no painel de navegação. 2. Na seção Tabelas, verifique a tabela `DynamoDBTableDocklessVehicles` . 3. Depois que a criação do recurso for concluída, abra o console do Athena e escolha Grupos de trabalho no painel de navegação. 4. Escolha o grupo `V2EngineWorkGroup` de trabalho e, em seguida, escolha Trocar grupo de trabalho. 5. Se você receber uma solicitação para salvar o local do resultado da consulta, escolha um local do Amazon S3 onde você tenha permissões de gravação. 6. Escolha Salvar. 7. No painel de navegação, escolha Query editor (Editor de consultas) e, depois, o	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	banco de dados `athena-ml-db-<your-AWS-account-number>` .	

Carregar arquivos de geolocalização no Athena

Tarefa	Descrição	Habilidades necessárias
Crie uma tabela do Athena com dados geoespaciais.	Para carregar os arquivos de geolocalização no Athena, faça o seguinte: 1. Abra o console do Athena e escolha o editor de consultas no painel de navegação. 2. Escolha a guia Consultas de exemplo. 3. Pesquise e selecione Q1: Bairros. 4. Para retornar ao editor de consultas, escolha a guia Editor. 5. Escolha Executar. Isso cria uma tabela nomeada `louisville_ky_neighborhoods` em seu banco de dados. Lembre-se de que a tabela é criada no banco de dados `athena-ml-db-<your-AWS-account-number>` .	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	A consulta cria uma nova tabela para os dados geoespaciais que representam os bairros urbanos. A tabela de dados é criada a partir de shapefiles GIS. A instrução `CREATE EXTERNAL TABLE` define o esquema da tabela e a localização e o formato do arquivo de dados subjacente. Para que o código Python processe arquivos de formato e produza essa tabela, consulte Processamento geoespacial de arquivos de formato GIS com o Amazon Athena em amostras. AWS Para obter um código SQL detalhado, consulte create_neighborhood_table.sql em GitHub.	

Prever a demanda por patinetes por bairro a partir dos dados agregados do DynamoDB

Tarefa	Descrição	Habilidades necessárias
Declare uma função no Athena para consultar a SageMaker IA.	1. Abra o console do Athena, escolha Editor de consultas no painel de navegação e, em seguida, escolha a guia Editor.	Cientista de dados, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	2. Copie e cole a seguinte instrução SQL no editor de consultas. `USING EXTERNAL FUNCTION predict_demand ( location_id BIGINT, hr BIGINT , dow BIGINT, n_pickup_1 BIGINT, n_pickup_2 BIGINT, n_pickup_3 BIGINT, n_pickup_4 BIGINT, n_dropoff_1 BIGINT, n_dropoff_2 BIGINT, n_dropoff_3 BIGINT, n_dropoff_4 BIGINT ) RETURNS DOUBLE SAGEMAKER '<Your SageMaker endpoint>'` A primeira parte da instrução SQL declara a função externa para consultar inferências de ML do endpoint de SageMaker IA que hospeda o modelo pré-treinado. 3. Defina a ordem e o tipo dos parâmetros de entrada e o dos valores retornados. 4. Escolha Executar.	

Tarefa	Descrição	Habilidades necessárias
Prever a demanda por patinetes por bairro a partir dos dados agregados do DynamoDB.	Agora você poderá usar o Athena para consultar dados transacionais diretamente do DynamoDB e, em seguida, agregar os dados para análise e previsão. Isso não é facilmente alcançado consultando diretamente um banco de dados NoSQL do DynamoDB. 1. Abra o console do Athena e escolha o Editor de consultas no painel de navegação. 2. Escolha a guia Consultas salvas. 3. Pesquise e selecione Q2: Dynamo Predict. DBAthena MLScooter 4. Para retornar ao editor de consultas, escolha a guia Editor. 5. Escolha Executar. A instrução SQL faz o seguinte: • Usa uma Consulta federada do Athena para consultar a tabela do DynamoDB com os dados brutos da viagem • Coloca coordenadas geográficas em bairros	Desenvolvedor de aplicativos, cientista de dados

Tarefa	Descrição	Habilidades necessárias
	usando as funções geoespaciais de Athena • Enriquece os dados com inferência de ML usando IA SageMaker Para obter informações sobre como usar o SQL para agregar dados do DynamoDB SageMaker e dados de inferência de IA no Athena, consulte athena_long.sql em. GitHub	
Verifique a saída.	A tabela de saída inclui o bairro, longitude e latitude do centroide do bairro. Também inclui o número de veículos previstos para a próxima hora. A consulta produz as previsões para um momento selecionado. Você poderá fazer previsões para qualquer outro momento alterando a expressão `TIMESTAMP '2019-09-07 15:00'` em todos os lugares da declaração. Se você tiver um feed de dados em tempo real na tabela do DynamoDB, altere o timestamp para `NOW()`.	Desenvolvedor de aplicativos, cientista de dados

Limpe o ambiente

Tarefa	Descrição	Habilidades necessárias
Excluir recursos.	1. Abra o console do Athena e esvazie o bucket que você criou como parte da CloudFormation pilha. 2. Abra o CloudFormation console e exclua a pilha chamada`abdb-1462-athena-dynamodb-ml-stack` . 3. Abra o CloudWatch console da Amazon e, em seguida, exclua o grupo de registros chamado`/aws/sagemaker/Endpoints/Sg-athena-ml-dynamodb-model-endpoint` .	Desenvolvedor de aplicativos, AWS DevOps

Recursos relacionados

- SDK da Federação de Consultas do Amazon Athena () GitHub
- Consultando dados geoespaciais (documentação)AWS
- Use previsões de ML sobre dados do Amazon DynamoDB com o Amazon Athena ML (Big Data Blog)AWS
- Amazon ElastiCache (Redis OSS) (AWS documentação)
- Amazon Neptune (documentação)AWS

Associe um AWS CodeCommit repositório em um Conta da AWS com o Amazon SageMaker AI Studio Classic em outra conta

Criado por Laurens van der Maas (AWS) e Aubrey Oosthuizen (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão fornece instruções e código sobre como associar um AWS CodeCommit repositório em um Conta da AWS (Conta A) com o Amazon SageMaker AI Studio Classic em outro Conta da AWS (Conta B). Para configurar a associação, você deve criar uma política e uma função AWS Identity and Access Management (IAM) na Conta A e uma política embutida do IAM na Conta B. Em seguida, você usa um script de shell para clonar o CodeCommit repositório da Conta A para o Amazon SageMaker AI Classic na Conta B.

Pré-requisitos e limitações

Pré-requisitos

- Dois Contas da AWS, um contendo o CodeCommit repositório e o outro contendo um domínio de SageMaker IA com um usuário
- Domínio e usuário de SageMaker IA provisionados, com acesso à Internet ou acesso a CodeCommit e AWS Security Token Service (AWS STS) por meio de endpoints de rede privada virtual (VPC)
- Conceitos básicos do IAM
- Uma compreensão básica do SageMaker AI Studio Classic
- Uma compreensão básica do Git e CodeCommit

Limitações

Esse padrão se aplica somente ao SageMaker AI Studio Classic, não ao RStudio Amazon SageMaker AI.

Arquitetura

Pilha de tecnologia

- SageMaker Inteligência Artificial da Amazon
- Amazon SageMaker AI Studio Clássico
- AWS CodeCommit
- AWS Identity and Access Management (IAM)
- Git

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura que associa um CodeCommit repositório da Conta A ao SageMaker AI Studio Classic na Conta B.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário assume a `MyCrossAccountRepositoryContributorRole` função na Conta A por meio da `sts:AssumeRole` função, enquanto usa a função de execução de SageMaker IA no SageMaker AI Studio Classic na Conta B. A função assumida inclui as CodeCommit permissões para clonar e interagir com o repositório especificado.
2. O usuário executa comandos Git a partir do terminal do sistema no SageMaker AI Studio Classic.

Automação e escala

Esse padrão consiste em etapas manuais que podem ser automatizadas usando o AWS Cloud Development Kit (AWS CDK), AWS CloudFormation, ou Terraform.

Ferramentas

Ferramentas da AWS

- O Amazon SageMaker AI é um serviço gerenciado de aprendizado de máquina (ML) que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção.
- O Amazon SageMaker AI Studio Classic é um ambiente de desenvolvimento integrado (IDE) baseado na web para aprendizado de máquina que permite criar, treinar, depurar, implantar e monitorar seus modelos de aprendizado de máquina.

- AWS CodeCommité um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.

  Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.

Outras ferramentas

- O Git é um sistema distribuído de controle de versões para rastrear alterações no código-fonte durante o desenvolvimento do software.

Épicos

Criar uma política do IAM e um perfil do IAM na conta A

Tarefa	Descrição	Habilidades necessárias
Criar uma política do IAM para acesso ao repositório na conta A.	1. Faça login no AWS Management Console e abra o console do IAM. 2. No painel de navegação, selecione Políticas e, em seguida, Criar política. 3. Selecione a guia JSON. 4. Copie a instrução da política de Exemplo de política do IAM na seção Informações adicionais desse padrão e cole-a no editor JSON. Certifiqu e-se de substituir todos os valores de espaço reservado na política.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	5. Selecione Próximo: Tags e, em seguida,Próximo: Análise. 6. Em Nome, insira um nome para a política. Observação: nesse padrão, a política do IAM é chamada de `CrossAccountAccessForMySharedDemoRepo` , mas você pode escolher o nome de política que preferir. 7. Selecione Criar política. **Tip** É uma prática recomendada restringir o escopo de suas políticas do IAM às permissões mínimas necessárias para seu caso de uso.	

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM para acesso ao repositório na conta A.	1. No painel de navegação do console do IAM, escolha Funções e, em seguida, Criar função. 2. Em Tipo de entidade confiável, selecione Conta da AWS. 3. Na seção Conta da AWS, selecione Outra conta da AWS. 4. Em ID da conta, insira o ID da conta para a conta B. 5. Na página Adicionar permissões, procure e escolha a política `CrossAccountAccessForMySharedDemoRepo` que você criou anteriormente. 6. Escolha Próximo. 7. Em Nome do perfil, insira um nome. Observação: nesse padrão, o perfil do IAM é chamado de `MyCrossAccountRepositoryContributorRole`, mas você pode escolher o nome de perfil que preferir. 8. Escolha Criar perfil e, em seguida, copie o nome do recurso da Amazon (ARN) do novo perfil.	AWS DevOps

Criar uma política em linha do IAM na Conta B

Tarefa	Descrição	Habilidades necessárias
Anexe uma política embutida à função de execução vinculada ao usuário do seu SageMaker domínio na Conta B.	1. No painel de navegação do console do IAM, escolha Perfis. 2. Pesquise e escolha a função de execução associada ao seu usuário do SageMaker AI Domain na Conta B. 3. Escolha Adicionar permissões e, em seguida, Criar política em linha. 4. Selecione a guia JSON. 5. Copie a seguinte declaração de política e, em seguida, cole-o no editor JSON. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>" } ] }`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	6. Substitua `<Account_A_ID>` pelo ID da conta A. Substitua `<Account_A_Role_Name>` pelo nome do perfil do IAM que você criou anteriormente. 7. Selecione Revisar política. 8. Em Nome, digite um nome para sua política em linha. 9. Selecione Criar política.	

Clone o repositório no SageMaker AI Studio Classic para a Conta B

Tarefa	Descrição	Habilidades necessárias
Crie o script de shell no SageMaker AI Studio Classic na Conta B.	1. No painel de navegação do SageMaker console, escolha Studio. 2. Selecione seu perfil de usuário e, em seguida, escolha Abrir Studio. 3. Na seção Início, escolha Abrir o assistente de execução. 4. Na seção Utilitários e arquivos, escolha Arquivo de texto. 5. Copie o script de Exemplo de script de SageMaker shell na seção Informações adicionais desse padrão e cole a instrução no novo arquivo. Certifique-se de	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	substituir todos os valores de espaço reservado na política. 6. Clique com o botão direito do mouse na guia untitled.txt do seu novo arquivo e escolha Renomear texto. Em Novo nome, digite cross_account_git_clone.sh e, em seguida, escolha Renomear.	
Invocar o script de shell a partir do terminal do sistema.	1. Na seção Início do SageMaker console, escolha Abrir o Launcher. 2. Na seção Utilitários e arquivos, escolha Terminal do sistema. 3. Na janela do terminal, execute o seguinte comando: `chmod u+x ./cross_account_git_clone.sh && ./cross_account_git_clone.sh` Você clonou seu CodeCommit repositório em uma conta cruzada do SageMaker AI Studio. Agora você pode executar todos os comandos do Git no terminal do sistema.	AWS DevOps

Mais informações

Exemplo de política do IAM

Para usar este exemplo, você precisa fazer o seguinte:

- <CodeCommit_Repository_Region>Substitua pelo Região da AWS para o repositório.
- Substitua <Account_A_ID> pelo ID da conta para a conta A.
- <CodeCommit_Repository_Name>Substitua pelo nome do seu CodeCommit repositório na Conta A.

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

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

Exemplo de script de shell de SageMaker IA

Para usar este exemplo, você precisa fazer o seguinte:

- Substitua <Account_A_ID> pelo ID da conta para conta A.
- Substitua <Account_A_Role_Name> pelo nome do perfil do IAM que você criou anteriormente.
- <CodeCommit_Repository_Region>Substitua pelo Região da AWS para o repositório.
- <CodeCommit_Repository_Name>Substitua pelo nome do seu CodeCommit repositório na Conta A.

```
#!/usr/bin/env bash
#Launch from system terminal
pip install --quiet git-remote-codecommit

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

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

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

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

Extraia automaticamente conteúdo de arquivos PDF usando o Amazon Textract

Criado por Tianxia Jia (AWS)

Resumo

Muitas organizações precisam extrair informações de arquivos PDF que são enviados para seus aplicativos de negócios. Por exemplo, uma organização pode precisar extrair com precisão as informações de arquivos PDF fiscais ou médicos para análise tributária ou processamento de reclamações médicas.

Na nuvem da Amazon Web Services (AWS), o Amazon Textract extrai automaticamente informações (por exemplo, texto impresso, formulários e tabelas) de arquivos PDF e produz um arquivo formatado em JSON que contém informações do arquivo PDF original. Você pode usar o Amazon Textract no Console de Gerenciamento da AWS ou implementando chamadas de API. Recomendamos que você use chamadas de API programáticas para escalar e processar automaticamente grandes quantidades de arquivos PDF.

Quando o Amazon Textract processa um arquivo, ele cria a seguinte lista de objetos `Block`: páginas, linhas e palavras de texto, formulários (pares de valores-chave), tabelas e células e elementos de seleção. Outras informações do objeto também estão incluídas, por exemplo, caixas delimitadoras IDs, intervalos de confiança e relacionamentos. O Amazon Textract extrai as informações do conteúdo como sequências de caracteres. Valores de dados identificados e transformados corretamente são necessários porque podem ser usados com mais facilidade por seus aplicativos downstream.

Esse padrão descreve um step-by-step fluxo de trabalho para usar o Amazon Textract para extrair automaticamente conteúdo de arquivos PDF e processá-lo em uma saída limpa. O padrão usa uma técnica de correspondência de modelos para identificar corretamente o campo obrigatório, o nome da chave e as tabelas e, em seguida, aplica correções de pós-processamento a cada tipo de dados. Você pode usar esse padrão para processar diferentes tipos de arquivos PDF e, em seguida, escalar e automatizar esse fluxo de trabalho para processar arquivos PDF que tenham um formato idêntico.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket existente do Amazon Simple Storage Service (Amazon S3) para armazenar os arquivos PDF após serem convertidos para o formato JPEG para processamento pelo Amazon Textract. Para obter mais informações sobre buckets do S3, consulte Visão geral dos buckets na documentação do Amazon S3.
- O caderno Jupyter `Textract_PostProcessing.ipynb` (anexado), instalado e configurado. Para obter mais informações sobre os cadernos Jupyter, consulte Criar um caderno Jupyter na documentação da Amazon. SageMaker
- Arquivos PDF existentes que têm um formato idêntico.
- Uma compreensão do Python.

Limitações

- Seus arquivos PDF devem ser de boa qualidade e claramente legíveis. Arquivos PDF nativos são recomendados, mas você pode usar documentos digitalizados que são convertidos em formato PDF se todas as palavras individuais estiverem claras. Para obter mais informações sobre isso, consulte Pré-processamento de documentos PDF com o Amazon Textract: detecção e remoção de imagens no blog do AWS Machine Learning.
- Para arquivos de várias páginas, você pode usar uma operação assíncrona ou dividir os arquivos PDF em uma única página e usar uma operação síncrona. Para obter mais informações sobre essas duas opções, consulte Detecção e análise de texto em documentos de várias páginas e Detecção e análise de texto em documentos de uma única página na documentação do Amazon Textract.

Arquitetura

O fluxo de trabalho desse padrão primeiro executa o Amazon Textract em um arquivo PDF de amostra (primeira execução) e depois o executa em arquivos PDF que têm um formato idêntico ao primeiro PDF (execução repetida). O diagrama a seguir mostra o fluxo de trabalho combinado de primeira execução e execução repetida que extrai automaticamente e repetidamente conteúdo de arquivos PDF com formatos idênticos.

O diagrama a seguir mostra o fluxo de trabalho desse padrão:

1. Converta um arquivo PDF em formato JPEG e armazene-o em um bucket do S3.

2. Chame a API Amazon Textract e analise o arquivo JSON de resposta do Amazon Textract.
3. Edite o arquivo JSON adicionando o par `KeyName:DataType` correto para cada campo obrigatório. Crie um arquivo `TemplateJSON` para o estágio de execução repetida.
4. Defina as funções de correção de pós-processamento para cada tipo de dados (por exemplo, flutuante, inteiro e data).
5. Prepare os arquivos PDF que tenham um formato idêntico ao seu primeiro arquivo PDF.
6. Chame a API Amazon Textract e analise o JSON de resposta do Amazon Textract.
7. Combine o arquivo JSON analisado com o arquivo `TemplateJSON`.
8. Implemente correções de pós-processamento.

O arquivo de saída JSON final tem o campo correto `KeyName` e `Value` para cada campo obrigatório.

Pilha de tecnologias de destino

- Amazon SageMaker
- Amazon S3
- Amazon Textract

Automação e escala

Você pode automatizar o fluxo de trabalho de repetição de execução usando uma função do Lambda da AWS que inicia o Amazon Textract quando um novo arquivo PDF é adicionado ao Amazon S3. Em seguida, o Amazon Textract executa os scripts de processamento e a saída final pode ser salva em um local de armazenamento. Para obter mais informações sobre isso, consulte Usar um acionador do Amazon S3 para invocar uma função do Lambda na documentação do Lambda.

Ferramentas

- SageMakerA Amazon é um serviço de ML totalmente gerenciado que ajuda você a criar e treinar modelos de ML de forma rápida e fácil e, em seguida, implantá-los diretamente em um ambiente hospedado pronto para produção.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Textract facilita a adição de detecção e análise de texto de documentos aos seus aplicativos.

Épicos

Primeira execução

Tarefa	Descrição	Habilidades necessárias
Converta o arquivo PDF.	Prepare o arquivo PDF para sua primeira execução dividindo-o em uma única página e convertendo-o em formato JPEG para a operação síncrona do Amazon Textract (`Syn API`). **Note** Você também pode usar a operação assíncrona do Amazon Textract (`Asyn API`) para arquivos PDF de várias páginas.	Cientista de dados, desenvolvedor
Analise a resposta JSON do Amazon Textract.	Abra o caderno Jupyter `Textract_PostProcessing.ipynb` (anexado) e chame a API Amazon Textract usando o seguinte código: `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename)`	Cientista de dados, desenvolvedor

Tarefa	Descrição	Habilidades necessárias

	`}`
	`},`
	`FeatureTypes=["TABLES", "FORMS"])`
	
	Analise a resposta JSON em um formulário e uma tabela usando o código a seguir:
	
	`parseformKV=form_kv_from_JSON(response)`
	`parseformTables=get_tables_fromJSON(response)`	

Edite o arquivo TemplateJSON.	Edite o JSON analisado para cada `KeyName` e `DataType` correspondentes (por exemplo, string, ponto flutuante, número inteiro ou data) e cabeçalhos de tabela (por exemplo, `ColumnNames` e `RowNames`). Esse modelo é usado para cada tipo de arquivo PDF individual, o que significa que o modelo pode ser reutilizado para arquivos PDF com formato idêntico.	Cientista de dados, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Defina as funções de correção de pós-processamento.	Os valores na resposta do Amazon Textract para o arquivo `TemplateJSON` são sequências de caracteres. Não há diferenciação para data, valor flutuante, número inteiro ou moeda. Esses valores devem ser convertidos no tipo de dados correto para seu caso de uso posterior. Corrija cada tipo de dados de acordo com o arquivo `TemplateJSON` usando o código a seguir: `finalJSON=postprocessingCorrection(parsedJSON,templateJSON)`	Cientista de dados, desenvolvedor

Repita a execução

Tarefa	Descrição	Habilidades necessárias
Prepare os arquivos PDF.	Prepare os arquivos PDF dividindo-os em uma única página e convertendo-os em formato JPEG para a operação síncrona do Amazon Textract (`Syn API`).	Cientista de dados, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Note Você também pode usar a operação assíncrona do Amazon Textract (`Asyn API`) para arquivos PDF de várias páginas.	
Chame a API do Amazon Textract.	Chame a API Amazon Textract usando o seguinte código: `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])`	Cientista de dados, desenvolvedor

Tarefa	Descrição	Habilidades necessárias

Analise a resposta JSON do Amazon Textract.	Analise a resposta JSON em um formulário e uma tabela usando o código a seguir:
	`parseformKV=form_kv_from_JSON(response)`
	`parseformTables=get_tables_fromJSON(response)`
		Cientista de dados, desenvolvedor

Carregue o arquivo TemplateJSON e combine-o com o JSON analisado.	Use o arquivo `TemplateJSON` para extrair os pares de valores-chave e a tabela corretos usando os seguintes comandos:
	`form_kv_corrected=form_kv_correction(parseformKV,templateJSON)`
	`form_table_corrected=form_Table_correction(parseformTables, templateJSON)`
	`form_kv_table_corrected_final={**form_kv_corrected , **form_table_corrected}`
		Cientista de dados, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Correções de pós-processamento.	Use `DataType` nos perfis de arquivo `TemplateJSON` e pós-processamento para corrigir dados usando o seguinte código: `finalJSON=postprocessingCorrection(form_kv_table_corrected_final,templateJSON)`	Cientista de dados, desenvolvedor

Recursos relacionados

- Extraia automaticamente texto e dados estruturados de documentos com o Amazon Textract
- Extraia texto e dados estruturados com o Amazon Textract
- Recursos do Amazon Textract

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie um modelo de previsão de inicialização a frio usando o DeepAR para séries temporais no SageMaker Amazon AI Studio Lab

Criado por Ivan Cui (AWS) e Eyal Shacham (AWS)

Resumo

Se você está alocando recursos de forma mais eficiente para o tráfego na web, prevendo a demanda de pacientes por necessidades de pessoal ou antecipando as vendas dos produtos de uma empresa, a previsão é uma ferramenta essencial. A previsão de partida a frio cria previsões para uma série temporal com poucos dados históricos, como um novo produto que acabou de entrar no mercado de varejo. Esse padrão usa o algoritmo de previsão Amazon SageMaker AI DeepAR para treinar um modelo de previsão de inicialização a frio e demonstra como realizar previsões em itens de inicialização a frio.

O DeepAR é um algoritmo de aprendizado supervisionado para prever séries temporais escalares (unidimensionais) usando redes neurais recorrentes (RNN). O DeepAR adota a abordagem de treinar um único modelo em conjunto em todas as séries temporais das séries temporais de produtos relacionados.

Os métodos tradicionais de previsão de séries temporais, como média móvel integrada autorregressiva (ARIMA) ou suavização exponencial (ETS), dependem muito das séries temporais históricas de cada produto individual. Portanto, esses métodos não são eficazes para a previsão de partida a frio. Quando seu conjunto de dados contém centenas de séries temporais relacionadas, o DeepAR supera os métodos padrão ARIMA e ETS. Você também pode usar o modelo treinado para gerar previsões para novas séries temporais semelhantes às séries temporais em que ele foi treinado.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Um domínio de SageMaker IA da Amazon.
- Um aplicativo do Amazon SageMaker AI Studio Lab ou do Jupiter Lab.

- Um bucket do Amazon Simple Storage Service (Amazon S3) com permissões de leitura e gravação.
- Conhecimento de programação em Python.
- Conhecimento do uso de um notebook Jupyter.

Limitações

- Invocar o modelo de previsão sem nenhum ponto de dados histórico retornará um erro. Invocar o modelo com o mínimo de pontos de dados históricos retornará previsões imprecisas com alta confiança. Esse padrão sugere uma abordagem para resolver essas limitações conhecidas da previsão de partida a frio.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte os serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- Python versão 3.10 ou posterior.
- O notebook do padrão foi testado no Amazon SageMaker AI Studio em uma instância ml.t3.medium com o kernel Python 3 (Data Science).

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

O fluxo de trabalho executa as seguintes tarefas:

1. Os arquivos de entrada de dados de treinamento e teste são sintetizados e, em seguida, enviados para um bucket do Amazon S3. Esses dados incluem várias séries temporais com características categóricas e dinâmicas, juntamente com valores-alvo (a serem previstos). O notebook Jupyter visualiza os dados para entender melhor os requisitos dos dados de treinamento e os valores previstos esperados.
2. Um trabalho de sintonizador de hiperparâmetros é criado para treinar o modelo e encontrar o melhor modelo com base em métricas predefinidas.

3. Os arquivos de entrada são baixados do bucket do Amazon S3 para cada instância dos trabalhos de ajuste de hiperparâmetros.
4. Depois que o trabalho do sintonizador seleciona o melhor modelo com base no limite predefinido do sintonizador, o modelo é implantado como um endpoint de IA. SageMaker
5. O modelo implantado está então pronto para ser invocado, onde suas previsões são validadas em relação aos dados de teste.

O notebook demonstra o quão bem o modelo prevê os valores-alvo quando um número adequado de pontos de dados históricos está disponível. No entanto, quando invocamos o modelo com menos pontos de dados históricos (que representam um produto frio), as previsões do modelo não coincidem com os dados de teste originais, mesmo dentro dos níveis de confiança do modelo. No padrão, um novo modelo é criado para produtos frios, onde seu comprimento inicial do contexto (pontos previstos) é definido como a quantidade de pontos históricos disponíveis, e um novo modelo é treinado iterativamente à medida que novos pontos de dados são adquiridos. O caderno mostra que o modelo terá previsões precisas, desde que a quantidade de pontos de dados históricos esteja próxima ao tamanho do contexto.

Ferramentas

Serviços da AWS

- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon SageMaker AI é um serviço gerenciado de aprendizado de máquina (ML) que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção.
- O Amazon SageMaker AI Studio é um ambiente de desenvolvimento integrado (IDE) baseado na web para ML que permite criar, treinar, depurar, implantar e monitorar seus modelos de ML.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub DeepAR- ColdProduct -Pattern.

Práticas recomendadas

- Treine seu modelo em um ambiente virtual e sempre use o controle de versão para obter o máximo esforço de reprodutibilidade.
- Inclua o máximo possível de recursos categóricos de alta qualidade para obter o melhor modelo preditivo.
- Certifique-se de que os metadados contenham itens categóricos semelhantes para que o modelo possa inferir adequadamente as previsões de produtos de inicialização a frio.
- Execute um trabalho de ajuste de hiperparâmetros para obter o melhor modelo preditivo.
- Nesse padrão, o modelo que você cria tem uma duração de contexto de 24 horas, o que significa que ele predirá as próximas 24 horas. Se você tentar prever as próximas 24 horas quando tiver menos de 24 horas de dados historicamente, a precisão da previsão do modelo se degradará linearmente com base na quantidade de pontos de dados históricos. Para mitigar esse problema, crie um novo modelo para cada conjunto de pontos de dados históricos até que esse número atinja o tamanho desejado da previsão (contexto). Por exemplo, comece com um modelo de duração de contexto de 2 horas e aumente o modelo progressivamente para 4 horas, 8 horas, 16 horas e 24 horas.

Épicos

Inicie seu aplicativo SageMaker AI Studio Classic

Tarefa	Descrição	Habilidades necessárias
Inicie seu ambiente de notebook.	1. Faça login no AWS Management Console e abra a página inicial do SageMaker AI Studio. Em seguida, escolha Open Studio. 2. No painel de navegação esquerdo, escolha o ícone	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	do Studio Classic em Aplicativos. Em seguida, escolha o botão Abrir na lista de aplicativos. Para obter mais informaçõ es, consulte Launch Amazon SageMaker AI Studio na documentação de SageMaker IA.	

Crie e ative o notebook

Tarefa	Descrição	Habilidades necessárias
Configure seu ambiente virtual para treinamento de modelos.	Para configurar seu ambiente virtual para treinamento de modelos, faça o seguinte: 1. Baixe o `deepar_synthetic.ipynb` notebook do GitHub repositório desse padrão para sua máquina local. 2. No Amazon SageMaker AI Studio Classic, escolha o ícone Carregar arquivos na barra de menu do Studio Classic e selecione o caderno baixado. 3. Escolha o notebook no Navegador de arquivos no painel de navegação esquerdo. Siga as instruçõe	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	s para configurar um ambiente de notebook. Selecione a imagem do Data Science 3.0 e o kernel do Python 3. Para obter mais informações, consulte Carregar arquivos para o SageMaker AI Studio Classic na documentação do SageMaker AI.	
Crie e valide um modelo de previsão.	• Siga as instruções no notebook para criar os dados de treinamento e teste, treinar o modelo e, em seguida, invocar o modelo. • Observe a precisão das previsões do modelo quando ele é fornecido com pontos de dados históricos adequados.	Cientista de dados

Recursos relacionados

- Hiperparâmetros DeepAR
- Previsão da demanda por lançamentos de novos produtos usando serviços de aprendizado AWS de máquina
- Inicie o Amazon SageMaker AI Studio Classic
- Use o algoritmo de SageMaker previsão AI DeepAR

Crie um MLOps fluxo de trabalho usando o Amazon SageMaker AI e o Azure DevOps

Criado por Deepika Kumar (AWS), Philips Kokoh Prasetyo (AWS) e Sara van de Moosdijk (AWS)

Resumo

As operações de aprendizado de máquina (MLOps) são um conjunto de práticas que automatizam e simplificam os fluxos de trabalho e as implantações de aprendizado de máquina (ML). MLOps se concentra em automatizar o ciclo de vida do ML. Isso ajuda a garantir que os modelos não sejam apenas desenvolvidos, mas também implantados, monitorados e retreinados de forma sistemática e repetida. Ele traz DevOps princípios para o ML. MLOps resulta em uma implantação mais rápida de modelos de ML, maior precisão ao longo do tempo e maior garantia de que eles fornecem valor comercial real.

As organizações geralmente têm DevOps ferramentas e soluções de armazenamento de dados existentes antes de iniciar sua MLOps jornada. Esse padrão mostra como aproveitar os pontos fortes do Microsoft Azure e. AWS Ele ajuda você a integrar o Azure DevOps com o Amazon SageMaker AI para criar um MLOps fluxo de trabalho.

A solução simplifica o trabalho entre o Azure e. AWS Você pode usar o Azure para desenvolvimento e AWS aprendizado de máquina. Ele promove um processo eficaz para criar modelos de aprendizado de máquina do início ao fim, incluindo tratamento de dados, treinamento e implantação AWS. Para maior eficiência, você gerencia esses processos por meio de DevOps pipelines do Azure. A solução é aplicável às operações do modelo básico (FMOps) e às operações do modelo de linguagem grande (LLMOps) na IA generativa, que inclui ajuste fino, bancos de dados vetoriais e gerenciamento imediato.

Pré-requisitos e limitações

Pré-requisitos

- Assinatura do Azure — Acesso aos serviços do Azure, como o Azure DevOps, para configurar os pipelines de integração contínua e implantação contínua (CI/CD).
- Conta ativa da AWS — Permissões para usar o Serviços da AWS usado nesse padrão.
- Dados — Acesso a dados históricos para treinar o modelo de aprendizado de máquina.
- Familiaridade com os conceitos de ML — compreensão do Python, do Jupyter Notebooks e do desenvolvimento de modelos de aprendizado de máquina.

- Configuração de segurança — Configuração adequada de funções, políticas e permissões no Azure e na AWS para garantir a transferência e o acesso seguros aos dados.
- (Opcional) Banco de dados vetorial — Se você estiver usando uma abordagem de geração aumentada de recuperação (RAG) e um serviço terceirizado para o banco de dados vetoriais, precisará acessar o banco de dados vetoriais externo.

Limitações

- Esta orientação não aborda transferências seguras de dados entre nuvens. Para obter mais informações sobre transferências de dados entre nuvens, consulte AWS Soluções para nuvem híbrida e multicloud.
- As soluções multicloud podem aumentar a latência para processamento de dados em tempo real e inferência de modelos.
- Essa orientação fornece um exemplo de MLOps arquitetura de várias contas. Os ajustes são necessários com base no aprendizado de máquina e na AWS estratégia.
- Esta orientação não descreve o uso de serviços de IA/ML que não sejam o Amazon SageMaker AI.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Arquitetura de destino

A arquitetura de destino integra o Azure DevOps com a Amazon SageMaker AI, criando um fluxo de trabalho de ML entre nuvens. Ele usa o Azure para CI/CD processes and SageMaker AI for ML model training and deployment. It outlines the process of obtaining data (from sources such as Amazon S3, Snowflake, and Azure Data Lake) through model building and deployment. Key components include CI/CD pipelines para criação e implantação de modelos, preparação de dados, gerenciamento de infraestrutura e Amazon SageMaker AI para treinamento, ajuste fino, avaliação e implantação de modelos de ML. Essa arquitetura foi projetada para fornecer fluxos de trabalho de ML eficientes, automatizados e escaláveis em todas as plataformas de nuvem.

A arquitetura consiste nos seguintes componentes:

1. Cientistas de dados realizam experimentos de ML na conta de desenvolvimento para explorar diferentes abordagens para casos de uso de ML usando várias fontes de dados. Cientistas de dados realizam testes e testes unitários e, para monitorar seus experimentos, podem usar o Amazon SageMaker AI com MLflow. No desenvolvimento de modelos generativos de IA, os cientistas de dados ajustam os modelos básicos do Amazon SageMaker AI JumpStart Model Hub. Após a avaliação do modelo, os cientistas de dados enviam e mesclam o código no repositório Model Build, que está hospedado no Azure. DevOps Esse repositório contém código para um pipeline de construção de modelos em várias etapas.
2. No Azure DevOps, o pipeline do Model Build, que fornece integração contínua (CI), pode ser ativado automática ou manualmente após a mesclagem do código com a ramificação principal. Na conta de automação, isso ativa o pipeline de SageMaker IA para pré-processamento de dados, treinamento e ajuste fino de modelos, avaliação de modelos e registro condicional de modelos com base na precisão.
3. A conta de automação é uma conta central em todas as plataformas de ML que hospeda ambientes de ML (Amazon ECR), modelos (Amazon S3), metadados do modelo (AI Model Registry), recursos SageMaker SageMaker (AI Feature Store), pipelines automatizados SageMaker (AI Pipelines) e insights de log de ML (). CloudWatch Para uma carga de trabalho generativa de IA, você pode precisar de avaliações adicionais para solicitações nos aplicativos posteriores. Um aplicativo de gerenciamento rápido ajuda a agilizar e automatizar o processo. Essa conta permite a reutilização dos ativos de ML e aplica as melhores práticas para acelerar a entrega de casos de uso de ML.
4. A versão mais recente do modelo foi adicionada ao SageMaker AI Model Registry para análise. Ele rastreia as versões do modelo e os respectivos artefatos (linhagem e metadados). Ele também gerencia o status do modelo (aprovado, rejeitado ou pendente) e gerencia a versão para implantação posterior.
5. Depois que um modelo treinado no Registro de Modelos for aprovado por meio da interface do estúdio ou de uma chamada de API, um evento poderá ser enviado para a Amazon. EventBridge EventBridge inicia o pipeline Model Deploy no Azure DevOps.
6. O pipeline do Model Deploy, que fornece implantação contínua (CD), verifica a fonte do repositório Model Deploy. A fonte contém o código, a configuração para a implantação do modelo e scripts de teste para benchmarks de qualidade. O pipeline do Model Deploy pode ser adaptado ao seu tipo de inferência.
7. Após as verificações de controle de qualidade, o pipeline do Model Deploy implanta o modelo na conta Staging. A conta Staging é uma cópia da conta de produção e é usada para testes e avaliações de integração. Para uma transformação em lote, o pipeline do Model Deploy pode

atualizar automaticamente o processo de inferência em lote para usar a versão mais recente do modelo aprovada. Para uma inferência em tempo real, sem servidor ou assíncrona, ele configura ou atualiza o respectivo endpoint do modelo.

8. Após o teste bem-sucedido na conta Staging, um modelo pode ser implantado na conta de produção por meio de aprovação manual por meio do pipeline Model Deploy. Esse pipeline provisiona um endpoint de produção na etapa Deploy to production, incluindo monitoramento de modelos e um mecanismo de feedback de dados.
9. Depois que o modelo estiver em produção, use ferramentas como o SageMaker AI Model Monitor e o SageMaker AI Clarify para identificar tendências, detectar desvios e monitorar continuamente o desempenho do modelo.

Automação e escala

Use a infraestrutura como código (IaC) para implantar automaticamente em várias contas e ambientes. Ao automatizar o processo de configuração de um MLOps fluxo de trabalho, é possível separar os ambientes usados pelas equipes de ML que trabalham em projetos diferentes. AWS CloudFormationajuda você a modelar, provisionar e gerenciar AWS recursos tratando a infraestrutura como código.

Ferramentas

Serviços da AWS

- O Amazon SageMaker AI é um serviço gerenciado de ML que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção.
- AWS Glueé um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados. Nesse padrão, o Amazon S3 é usado para armazenamento de dados e integrado à SageMaker IA para treinamento de modelos e objetos de modelo.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado. Nesse padrão, o Lambda é usado para tarefas de pré-processamento e pós-processamento de dados.

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável. Nesse padrão, ele armazena contêineres Docker que a SageMaker IA usa como ambientes de treinamento e implantação.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Nesse padrão, EventBridge orquestra fluxos de trabalho orientados por eventos ou baseados em tempo que iniciam o retreinamento ou a implantação automáticos do modelo.
- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala. Nesse padrão, ele é usado para criar um ponto de entrada único voltado para o exterior para SageMaker endpoints de IA.
- Para aplicativos RAG, você pode usar Serviços da AWS, como Amazon OpenSearch Service e Amazon RDS for PostgreSQL, para armazenar as incorporações vetoriais que fornecem ao LLM seus dados internos.

Outras ferramentas

- O Azure DevOps ajuda você a gerenciar pipelines de CI/CD e facilitar a criação, os testes e a implantação do código.
- O Azure Data Lake Storage ou o Snowflake são possíveis fontes terceirizadas de dados de treinamento para modelos de ML.
- Pinecone, Milvus ou ChromaDB são possíveis bancos de dados vetoriais de terceiros para armazenar incorporações vetoriais.

Práticas recomendadas

Antes de implementar qualquer componente desse MLOps fluxo de trabalho multicloud, conclua as seguintes atividades:

- Defina e compreenda o fluxo de trabalho do aprendizado de máquina e as ferramentas necessárias para apoiá-lo. Casos de uso diferentes exigem fluxos de trabalho e componentes diferentes. Por exemplo, um feature store pode ser necessário para reutilização de recursos e inferência de baixa latência em um caso de uso de personalização, mas pode não ser necessário para outros casos de uso. É necessário compreender o fluxo de trabalho desejado, os requisitos do caso de uso e os métodos de colaboração preferidos da equipe de ciência de dados para personalizar a arquitetura com sucesso.

- Crie uma separação clara de responsabilidade para cada componente da arquitetura. Distribuir o armazenamento de dados entre o Azure Data Lake Storage, o Snowflake e o Amazon S3 pode aumentar a complexidade e o custo. Se possível, escolha um mecanismo de armazenamento consistente. Da mesma forma, evite usar uma combinação de DevOps serviços do Azure e da AWS, ou uma combinação de serviços do Azure e do AWS ML.
- Escolha um ou mais modelos e conjuntos de dados existentes para realizar end-to-end testes do MLOps fluxo de trabalho. Os artefatos de teste devem refletir casos de uso reais que as equipes de ciência de dados desenvolvem quando a plataforma entra em produção.

Épicos

Projete sua MLOps arquitetura

Tarefa	Descrição	Habilidades necessárias
Identifique as fontes de dados.	Com base nos casos de uso atuais e futuros, nas fontes de dados disponíveis e nos tipos de dados (como dados confidenciais), documente as fontes de dados que precisam ser integradas à MLOps plataforma. Os dados podem ser armazenados no Amazon S3, no Azure Data Lake Storage, no Snowflake ou em outras fontes. Para cargas de trabalho generativas de IA, os dados também podem incluir uma base de conhecimento que fundamenta a resposta gerada. Esses dados são armazenados como incorpora ções vetoriais em bancos de dados vetoriais. Crie um plano para integrar essas fontes à	Engenheiro de dados, cientista de dados, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	sua plataforma e garantir o acesso aos recursos corretos.	
Escolha os serviços aplicáveis.	Personalize a arquitetura adicionando ou removendo serviços com base no fluxo de trabalho desejado da equipe de ciência de dados, nas fontes de dados aplicáveis e na arquitetura de nuvem existente. Por exemplo, engenheiros de dados e cientistas de dados podem realizar pré-processamento de dados e engenharia de recursos em SageMaker IA ou Amazon EMR. AWS GlueÉ improvável que todos os três serviços sejam necessários.	Administrador da AWS, engenheiro de dados, cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias
Analise os requisitos de segurança.	Reúna e documente os requisitos de segurança. Isso inclui determinar: • Quais equipes ou engenheiros podem acessar fontes de dados específicas • Quais equipes ou engenheiros podem acessar modelos de fundação pré-treinados • Se as equipes têm permissão para acessar o código e os modelos de outras equipes • Quais permissões (se houver) os membros da equipe devem ter para contas que não sejam de desenvolvimento • Quais medidas de segurança precisam ser implementadas para a transferência de dados entre nuvens Para obter mais informações sobre como proteger cargas de trabalho generativas de IA, consulte Protegendo a IA generativa: uma introdução à matriz de escopo de segurança de IA generativa (postagem no blog).AWS	Administrador da AWS, arquiteto de nuvem

Configurar AWS Organizations

Tarefa	Descrição	Habilidades necessárias
Configurar AWS Organizations.	Configure AWS Organizations na raiz Conta da AWS. Isso ajuda você a gerenciar as contas subsequentes que você cria como parte de uma MLOps estratégia de várias contas. Para obter mais informações, consulte a documentação do AWS Organizations.	Administrador da AWS

Configurar o ambiente de desenvolvimento e o controle de versão

Tarefa	Descrição	Habilidades necessárias
Crie uma conta AWS de desenvolvimento.	Crie um Conta da AWS local em que engenheiros e cientistas de dados tenham permissões para experimentar e criar modelos de ML. Para obter instruções, consulte Criação de uma conta de membro em sua organização na AWS Organizations documentação.	Administrador da AWS
Crie um repositório Model Build.	Crie um repositório Git no Azure onde os cientistas de dados possam enviar o código de criação e implantação do modelo após a conclusão da fase de experimentação. Para	DevOps engenheiro, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias
	obter instruções, consulte Configurar um repositório Git na documentação do Azure. DevOps	
Crie um repositório Model Deploy.	Crie um repositório Git no Azure que armazene modelos e códigos de implantação padrão. Ele deve incluir código para cada opção de implantação que a organização usa, conforme identificado na fase de design. Por exemplo, ele deve incluir endpoints em tempo real, endpoints assíncronos, inferência sem servidor ou transformações em lote. Para obter instruções, consulte Configurar um repositório Git na documentação do Azure. DevOps	DevOps engenheiro, engenheiro de ML
Crie um repositório do Amazon ECR.	Configure um repositório Amazon ECR que armazene os ambientes de ML aprovados como imagens do Docker. Permita que cientistas de dados e engenheiros de ML definam novos ambientes. Para obter instruções, consulte Criar um repositório privado na documentação do Amazon ECR.	Engenheiro de ML

Tarefa	Descrição	Habilidades necessárias
Configure o SageMaker AI Studio.	Configure o SageMaker AI Studio na conta de desenvolvimento de acordo com os requisitos de segurança previamente definidos, as ferramentas preferidas de ciência de dados (como MLflow) e o ambiente de desenvolvimento integrado (IDE) preferido. Use configurações de ciclo de vida para automatizar a instalação das principais funcionalidades e criar um ambiente de desenvolvimento uniforme para cientistas de dados. Para obter mais informações, consulte Amazon SageMaker AI Studio e servidor MLflow de rastreamento na documentação de SageMaker IA.	Cientista de dados, engenheiro de ML, engenheiro rápido

Integre pipelines de CI/CD

Tarefa	Descrição	Habilidades necessárias
Crie uma conta de automação.	Crie um Conta da AWS local onde os pipelines e trabalhos automatizados sejam executados. Você pode dar às equipes de ciência de dados acesso de leitura a essa conta. Para obter instruções, consulte Criação	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	de uma conta de membro em sua organização na AWS Organizations documentação.	
Configure um registro de modelo.	Configure o SageMaker AI Model Registry na conta de automação. Esse registro armazena os metadados dos modelos de ML e ajuda determinados cientistas de dados ou líderes de equipe a aprovar ou rejeitar modelos. Para obter mais informaçõ es, consulte Registrar e implantar modelos com o Model Registry na documenta ção de SageMaker IA.	Engenheiro de ML
Crie um pipeline de construçã o de modelos.	Crie um pipeline de CI/CD no Azure que inicie manual ou automaticamente quando o código é enviado para o repositório Model Build. O pipeline deve verificar o código-fonte e criar ou atualizar um pipeline de SageMaker IA na conta de automação. O pipeline deve adicionar um novo modelo ao registro do modelo. Para obter mais informações sobre a criação de um pipeline, consulte a documentação do Azure Pipelines.	DevOps engenheiro, engenheiro de ML

Crie a pilha de implantação

Tarefa	Descrição	Habilidades necessárias
Crie contas AWS de preparação e implantação.	Crie Contas da AWS para preparação e implantação de modelos de ML. Essas contas devem ser idênticas para permitir testes precisos dos modelos em preparação antes de passarem para a produção. Você pode dar às equipes de ciência de dados acesso de leitura à conta de teste. Para obter instruções, consulte Criação de uma conta de membro em sua organização na AWS Organizations documentação.	Administrador da AWS
Configure buckets S3 para monitoramento de modelos.	Conclua esta etapa se quiser ativar o monitoramento de modelos para os modelos implantados que são criados pelo pipeline Model Deploy. Crie buckets do Amazon S3 para armazenar os dados de entrada e saída. Para obter mais informações sobre a criação de buckets do S3, consulte Criação de um bucket na documentação do Amazon S3. Configure permissões entre contas para que os trabalhos automatizados de monitoramento de modelos sejam executado	Engenheiro de ML

Tarefa	Descrição	Habilidades necessárias
	s na conta de automação. Para obter mais informaçõ es, consulte Monitorar dados e qualidade do modelo na documentação de SageMaker IA.	
Crie um pipeline do Model Deploy.	Crie um pipeline de CI/CD no Azure que começa quando um modelo é aprovado no registro do modelo. O pipeline deve verificar o código-fo nte e o artefato do modelo, criar os modelos de infraestr utura para implantar o modelo nas contas de preparaçã o e produção, implantar o modelo na conta de preparaçã o, executar testes automatiz ados, aguardar a aprovação manual e implantar o modelo aprovado na conta de produção. Para obter mais informações sobre a criação de um pipeline, consulte a documentação do Azure Pipelines.	DevOps engenheiro, engenheiro de ML

(Opcional) Automatize a infraestrutura do ambiente de ML

Tarefa	Descrição	Habilidades necessárias
Crie AWS CDK nossos CloudFormation modelos.	Defina AWS Cloud Developme nt Kit (AWS CDK) nossos AWS CloudFormation	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	modelos para todos os ambientes que precisam ser implantados automatic amente. Isso pode incluir o ambiente de desenvolvimento, o ambiente de automação e os ambientes de preparaçã o e implantação. Para obter mais informações, consulte AWS CDKa CloudForm ationdocumentação e.	
Crie um pipeline de infraestr utura.	Crie um pipeline de CI/CD no Azure para implantação da infraestrutura. Um administr ador pode iniciar esse pipeline para criar novos ambientes Contas da AWS e configurar os que a equipe de ML exige.	DevOps engenheiro

Solução de problemas

Problema	Solução
Monitoramento insuficiente e detecção de desvios — O monitoramento inadequado pode levar à detecção perdida de problemas de desempenho do modelo ou desvio de dados.	Fortaleça as estruturas de monitoramento com ferramentas como Amazon CloudWatch, SageMaker AI Model Monitor e SageMaker AI Clarify. Configure alertas para ação imediata sobre problemas identificados.
Erros de gatilho do pipeline de CI — O pipeline de CI no Azure DevOps pode não ser acionado na mesclagem de código devido a uma configuração incorreta.	Verifique as configurações do DevOps projeto do Azure para garantir que os webhooks estejam configurados corretamente e

Problema	Solução
	apontando para os endpoints de SageMaker IA corretos.
Governança — a conta de automação central pode não aplicar as melhores práticas em todas as plataformas de ML, levando a fluxos de trabalho inconsistentes.	Audite as configurações da conta de automação, garantindo que todos os ambientes e modelos de ML estejam em conformidade com as melhores práticas e políticas predefini das.
Atrasos na aprovação do registro do modelo — Isso acontece quando há um atraso na verificação e aprovação do modelo, seja porque as pessoas demoram para revisá-lo ou devido a problemas técnicos.	Implemente um sistema de notificação para alertar as partes interessadas sobre modelos que estão pendentes de aprovação e agilizar o processo de revisão.
Falhas no evento de implantação do modelo — Os eventos enviados para iniciar os pipelines de implantação do modelo podem falhar, causando atrasos na implantação.	Confirme se a Amazon EventBridge tem as permissões e os padrões de eventos corretos para invocar os DevOps pipelines do Azure com sucesso.
Gargalos na implantação da produção — Os processos de aprovação manual podem criar gargalos, atrasando a implantação dos modelos na produção.	Otimize o fluxo de trabalho de aprovação dentro do pipeline de implantação do modelo, promovendo análises oportunas e canais de comunicação claros.

Recursos relacionados

AWS documentação

- Documentação da Amazon SageMaker AI
- Lente de Machine Learning (estrutura AWS bem arquitetada)
- Planejamento para o sucesso MLOps (AWS orientação prescritiva)

Outros AWS recursos

- MLOps roteiro básico para empresas com Amazon SageMaker AI (postagem AWS no blog)
- AWS Summit ANZ 2022 - End-to-end MLOps para arquitetos (YouTube vídeo)
- FMOps/LLMOps: Operacionalize a IA generativa e as diferenças com MLOps (AWS postagem do blog)
- Operacionalize a avaliação de LLM em grande escala usando o Amazon SageMaker AI Clarify e MLOps os serviços (AWS publicação no blog)
- O papel dos bancos de dados vetoriais em aplicativos generativos de IA (postagem AWS no blog)

Documentação do Azure

- DevOps Documentação do Azure
- Documentação do Azure Pipelines

Configure o registro de invocação de modelo no Amazon Bedrock usando AWS CloudFormation

Criado por Vikramaditya Bhatnagar (AWS)

Resumo

Você pode configurar o Amazon Bedrock para coletar registros de invocação, dados de entrada do modelo e dados de saída do modelo para todas as invocações do modelo em seu. Conta da AWS Essa é a melhor prática para criar aplicativos robustos de IA generativa com o Amazon Bedrock. Você pode armazenar registros de invocação de modelo em um grupo de CloudWatch logs do Amazon Logs, em um bucket do Amazon Simple Storage Service (Amazon S3) ou em ambos. Ter dados de registro no CloudWatch Logs ajuda você a criar filtros métricos, alarmes e painéis personalizados. O Amazon S3 é ideal para replicar dados em Regiões da AWS ou para armazenamento de longo prazo, conforme regido pelas políticas da sua organização.

Esse padrão fornece um AWS CloudFormation modelo de amostra que usa uma abordagem de infraestrutura como código (IaC) para configurar o registro de invocação de modelo para o Amazon Bedrock. O modelo configura o armazenamento de registros no CloudWatch Logs e no Amazon S3.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- As seguintes permissões:
  - Permissões para criar CloudFormation pilhas
  - Permissões para acessar o Amazon Bedrock
  - Permissões para criar e acessar buckets do Amazon S3
  - Permissões para criar e acessar grupos de CloudWatch registros do Logs
  - Permissões para criar e acessar AWS Lambda funções
  - Permissões para criar e acessar AWS Key Management Service (AWS KMS) chaves

Limitações

Esse padrão registra invocações do modelo no CloudWatch Logs e no Amazon S3. Ele não suporta a escolha de apenas um desses dois serviços.

Arquitetura

Arquitetura de destino

O CloudFormation modelo fornece os seguintes recursos em seu alvo Conta da AWS:

- Um grupo CloudWatch de registros de registros para armazenar registros de invocação de modelos
- Um bucket do Amazon S3 para armazenar registros de invocação do modelo e uma política de bucket correspondente
- Um bucket do Amazon S3 para armazenar registros de acesso do lado do servidor e uma política de bucket correspondente
- Uma AWS Lambda função que define as configurações de registro no Amazon Bedrock
- Um AWS KMS key e um alias de chave correspondente
- Uma função de serviço AWS Identity and Access Management (IAM) para o Amazon Bedrock

O diagrama a seguir mostra como os registros de invocação são armazenados após a implantação da CloudFormation pilha associada a esse padrão. O Amazon Bedrock publica dados de log quando o modelo básico fornece texto, uma imagem, um vídeo ou dados incorporados. Conforme mostrado no diagrama, os buckets do Amazon S3 e o grupo de CloudWatch logs Logs são criptografados com um. AWS KMS key

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário envia uma consulta para um modelo básico no Amazon Bedrock.
2. O Amazon Bedrock assume a função de serviço do IAM.
3. O Amazon Bedrock gera dados de log e os armazena em um grupo de CloudWatch registros de registros e em um bucket do Amazon S3.
4. Se um usuário ler, carregar ou excluir qualquer arquivo no bucket do Amazon S3 que contenha os registros de invocação do modelo, essas atividades serão registradas em outro bucket do Amazon S3 para registros de acesso do lado do servidor.

Automação e escala

Para escalar essa solução, você pode implantar o CloudFormation modelo como uma pilha definida para vários Regiões da AWS e. Contas da AWS Para obter mais informações, consulte Gerenciamento de pilhas entre contas e regiões StackSets na CloudFormation documentação.

Ferramentas

Serviços da AWS

- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais empresas de IA e da Amazon para seu uso por meio de uma API unificada.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas e aplicativos, Serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e desempenho líderes do setor.

Outras ferramentas

- O Git é um sistema de controle de versão distribuído e de código aberto.

Repositório de código

O código desse padrão está disponível no repositório GitHub enable-bedrock-logging-using-cloudformation.

Épicos

Crie a CloudFormation pilha

Tarefa	Descrição	Habilidades necessárias
Faça o download do CloudFormation modelo.	Baixe o CloudFormation modelo do GitHub repositório.	Arquiteto de nuvem
Implante o modelo.	Crie uma pilha na sua conta e região de destino. Na seção Parâmetros, especifique valores para os parâmetro s definidos no modelo. Para obter instruções, consulte Criação de uma pilha na CloudFormation documenta ção.	Arquiteto de nuvem

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Habilite o acesso ao modelo.	No Amazon Bedrock, adicione acesso ao modelo básico. Para obter instruções, consulte Adicionar ou remover o acesso aos modelos da Amazon Bedrock Foundation na documentação do Amazon Bedrock.	Arquiteto de nuvem
Execute um exemplo de prompt.	Nos playgrounds do Amazon Bedrock, execute um exemplo de prompt. Para obter instruções, consulte Gerar respostas no console usando	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	playgrounds na documentação do Amazon Bedrock.	
Revise a configuração de registro.	1. Faça login no console Amazon Bedrock. 2. Na barra de navegação, escolha Região da AWS onde você implantou a CloudFormation pilha. 3. No painel de navegação esquerdo, em Configura ções do Bedrock, escolha Configurações. 4. Confirme o seguinte: • O registro de invocação do modelo está ativado. • Todos os tipos de dados são selecionados. • Para destinos de registro, S3 e CloudWatch Logs são selecionados.	Arquiteto de nuvem
Analise o bucket do Amazon S3.	1. Na seção Configurações do S3, escolha Procurar no S3. Isso abre o bucket de destino no console do Amazon S3. 2. Confirme se os dados de registro estão presentes no exemplo de prompt que você executou anteriorm ente.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Analise o grupo de registros.	1. Navegue de volta para a página de configurações no console do Amazon Bedrock. 2. Na seção Configurações de CloudWatch registros, revise as configurações do grupo de CloudWatch registros de registros. Anote o nome do grupo de registros. 3. Abra o console de CloudWatch. 4. No painel de navegação, em Logs, escolha Grupos de logs. 5. Escolha o nome do grupo de registros em que o Amazon Bedrock publica os dados de registro. 6. Confirme se os dados de registro estão presentes no exemplo de prompt que você executou anteriormente.	Arquiteto de nuvem

Recursos relacionados

AWS documentação

- Acessando um bucket do Amazon S3 (documentação do Amazon S3)
- Criação e gerenciamento de pilhas (CloudFormation documentação)
- Monitore a invocação do modelo (documentação do Amazon Bedrock)

- Trabalhando com grupos de registros e fluxos de CloudWatch registros (documentação de registros)

AWS postagens no blog

- Monitoramento de aplicativos de IA generativa usando o Amazon Bedrock e a integração com a Amazon CloudWatch
- Melhores práticas para criar aplicativos robustos de IA generativa com Amazon Bedrock Agents — Parte 1
- Melhores práticas para criar aplicativos robustos de IA generativa com Amazon Bedrock Agents — Parte 2

Crie uma imagem de contêiner Docker personalizada SageMaker e use-a para treinamento de modelos no AWS Step Functions

Criado por Julia Bluszcz (AWS), Neha Sharma (AWS), Aubrey Oosthuizen (AWS), Mohan Gowda Purushothama (AWS) e Mateusz Zaremba (AWS)

Resumo

Esse padrão mostra como criar uma imagem de contêiner Docker para a Amazon SageMaker e usá-la para um modelo de treinamento no AWS Step Functions. Ao empacotar algoritmos personalizados em um contêiner, você pode executar praticamente qualquer código no SageMaker ambiente, independentemente da linguagem de programação, estrutura ou dependências.

No SageMaker notebook de exemplo fornecido, a imagem personalizada do contêiner Docker é armazenada no Amazon Elastic Container Registry (Amazon ECR). Em seguida, o Step Functions usa o contêiner armazenado no Amazon ECR para executar um script de processamento do Python para. SageMaker Em seguida, o contêiner exporta o modelo para o Amazon Simple Storage Service (Amazon S3).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma função do AWS Identity and Access Management (IAM) para SageMaker com permissões do Amazon S3
- Uma função do IAM para Step Functions
- Familiaridade com o Python
- Familiaridade com o Amazon SageMaker Python SDK
- Familiaridade com a AWS Command Line Interface (AWS CLI)
- Familiaridade com o AWS SDK para Python (Boto3)
- Familiaridade com o Amazon ECR
- Familiaridade com o Docker

Versões do produto

- SDK de ciência de dados do AWS Step Functions versão 2.3.0
- SDK do Amazon SageMaker Python versão 2.78.0

Arquitetura

O diagrama a seguir mostra um exemplo de fluxo de trabalho para criar uma imagem de contêiner do Docker e usá-la para um modelo de treinamento no Step Functions: SageMaker

O diagrama mostra o seguinte fluxo de trabalho:

1. Um cientista ou DevOps engenheiro de dados usa um SageMaker notebook da Amazon para criar uma imagem personalizada de contêiner Docker.
2. Um cientista ou DevOps engenheiro de dados armazena a imagem do contêiner Docker em um repositório privado do Amazon ECR que está em um registro privado.
3. Um cientista ou DevOps engenheiro de dados usa o contêiner Docker para executar uma tarefa de processamento do SageMaker Python em um fluxo de trabalho do Step Functions.

Automação e escala

O SageMaker notebook de exemplo nesse padrão usa um tipo de instância de `ml.m5.xlarge` notebook. É possível alterar o tipo de instância de acordo com seu caso de uso. Para obter mais informações sobre os tipos de instância de SageMaker notebook, consulte Amazon SageMaker Pricing.

Ferramentas

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- SageMakerA Amazon é um serviço gerenciado de aprendizado de máquina (ML) que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção.
- O Amazon SageMaker Python SDK é uma biblioteca de código aberto para treinar e implantar modelos de aprendizado de máquina em. SageMaker

- O AWS Step Functions é um serviço de orquestração com tecnologia sem servidor que permite combinar funções do AWS Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios.
- O AWS Step Functions Data Science Python SDK é uma biblioteca de código aberto que ajuda você a criar fluxos de trabalho do Step Functions que processam e publicam modelos de aprendizado de máquina.

Épicos

Crie uma imagem de contêiner do Docker personalizada e armazene-a no Amazon ECR

Tarefa	Descrição	Habilidades necessárias
Configure o Amazon ECR e crie um novo registro privado.	Se você ainda não o fez, configure o Amazon ECR seguindo as instruções em Configuração com o Amazon ECR no Guia do usuário do Amazon ECR. Cada conta da AWS é fornecida com um registro privado padrão do Amazon ECR.	DevOps engenheiro
Crie um repositório privado do Amazon ECR.	Siga as instruções em Criação de um repositório privado no Guia do usuário do Amazon ECR. **Note** O repositório que você cria é onde você armazenará suas imagens personalizadas de contêiner do Docker.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Crie um Dockerfile que inclua as especificações necessárias para executar seu trabalho de SageMaker processamento.	Crie um Dockerfile que inclua as especificações necessári as para executar seu trabalho de SageMaker processamento configurando um Dockerfil e. Para obter instruções, consulte Adaptar seu próprio contêiner de treinamento no Amazon SageMaker Developer Guide.
	
	Para obter mais informações sobre Dockerfiles, consulte a Referência do Dockerfile na documentação do Docker.
	
	Exemplo de células de código do caderno Jupyter para criar um Dockerfile
	
	Célula 1
	
	`# Make docker folder`
	`!mkdir -p docker`
	
	Célula 2
	
	`%%writefile docker/Do`
	`ckerfile`
	
	`FROM python:3.7-slim-bu`
	`ster`
	
	`RUN pip3 install`
	` pandas==0.25.3 scikit-`
	`learn==0.21.3`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ENV PYTHONUNBUFFERED=T RUE ENTRYPOINT ["python3"]	

Tarefa	Descrição	Habilidades necessárias
Crie a imagem do contêiner do Docker e envie-a para o Amazon ECR.	1. Crie a imagem do contêiner usando o Dockerfile que você criou executando o comando `docker build` na AWS CLI. 2. Envie a imagem do contêiner para o Amazon ECR executando o comando `docker push`. Para obter mais informações, consulte Criando e registrando o contêiner em Criando seu próprio contêiner de algoritmo em GitHub. Exemplo de células de código do caderno Jupyter para criar e registrar uma imagem do Docker **Important** Antes de executar as células a seguir, verifique se você criou um Dockerfile e o armazenou no diretório chamado. `docker` Além disso, certifique-se de ter criado um repositório Amazon ECR e de substituir o valor `ecr_repository`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	na primeira célula pelo nome do seu repositór io.
	
	Célula 1
	
	`import boto3`
	`tag = ':latest'`
	`account_id = boto3.cli`
	`ent('sts').get_cal`
	`ler_identity().get`
	`('Account')`
	`region = boto3.Ses`
	`sion().region_name`
	`ecr_repository = 'byoc'`
	
	`image_uri = '{}.dkr.e`
	`cr.{}.amazonaws.com/`
	`{}'.format(account_id,`
	` region, ecr_repository`
	` + tag)`
	
	Célula 2
	
	`# Build docker image`
	`!docker build -t`
	` $image_uri docker`
	
	Célula 3
	
	`# Authenticate to ECR`
	`!aws ecr get-login`
	`-password --region`
	` {region} | docker`
	` login --username`
	` AWS --password-stdin`	

Tarefa	Descrição	Habilidades necessárias

	`{account_id}.dkr.ecr.{region}.amazonaws.com`
	
	Célula 4
	
	`# Push docker image`
	`!docker push $image_uri`
	
	Note
	Você deve autenticar seu cliente Docker em seu registro privado para poder usar os comandos `docker push` e. `docker pull` Esses comandos enviam e extraem imagens de e para os repositórios em seu registro.	

Crie um fluxo de trabalho do Step Functions que use sua imagem personalizada de contêiner do Docker

Tarefa	Descrição	Habilidades necessárias
Crie um script Python que inclua sua lógica personalizada de processamento e treinamento de modelos.	Escreva uma lógica de processamento personalizada para ser executada em seu script de processamento de dados. Em seguida, salve-	Cientista de dados

Tarefa	Descrição	Habilidades necessárias

	o como um script Python chamado `training.py` .
	
	Para obter mais informações, consulte Traga seu próprio modelo com o Modo de SageMaker script ativado GitHub.
	
	Exemplo de script Python que inclui processamento personalizado e lógica de treinamento de modelos
	
	`%%writefile training.py`
	`from numpy import empty`
	`import pandas as pd`
	`import os`
	`from sklearn import datasets, svm`
	`from joblib import dump, load`
	
	`if __name__ == '__main__':`
	`digits = datasets.load_digits()`
	`#create classifier object`
	`clf = svm.SVC(gamma=0.001, C=100.)`
	
	`#fit the model`
	`clf.fit(digits.data[:-1], digits.target[:-1])`	

Tarefa	Descrição	Habilidades necessárias

	`#model output in binary format`
	`output_path = os.path.join('/opt/ml/processing/model', "model.joblib")`
	`dump(clf, output_path)`	

Tarefa	Descrição	Habilidades necessárias

Crie um fluxo de trabalho do Step Functions que inclua sua tarefa de SageMaker processamento como uma das etapas.	Instale e importe o AWS Step Functions Data Science SDK e faça o upload do arquivo training.py para o Amazon S3. Em seguida, use o Amazon SageMaker Python SDK para definir uma etapa de processamento em Step Functions.
	
	Important
	Certifique-se de ter criado uma função de execução do IAM para Step Functions em sua conta da AWS.
	
	Exemplo de configuração de ambiente e script de treinamento personalizado para upload para o Amazon S3
	
	`!pip install stepfunct ions`
	
	`import boto3`
	`import stepfunctions`
	`import sagemaker`
	`import datetime`
	
	`from stepfunctions`
	` import steps`
		Cientista de dados

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

Tarefa	Descrição	Habilidades necessárias
	`input_code = sagemaker_session.upload_data( "training.py", bucket=bucket, key_prefix="preprocessing.py", )` Exemplo SageMaker de definição de etapa de processamento que usa uma imagem personalizada do Amazon ECR e um script Python **Note** Certifique-se de usar o `execution_input` parâmetro para especificar o nome do trabalho. O valor do parâmetro deve ser exclusivo sempre que a tarefa for executada. Além disso, o código do arquivo training.py é passado como um parâmetro `input` para o `ProcessingStep` , o que significa que ele será copiado dentro do contêiner. O destino do código	

Tarefa	Descrição	Habilidades necessárias

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

Tarefa	Descrição	Habilidades necessárias

	<pre>],
	outputs=[
	Processin
	gOutput(
	source='/
	opt/ml/processing/
	model',
	destinati
	on="s3://{}/{}".fo
	rmat(bucket, prefix),
	output_na
	me='byoc-example')
	],
	container_entrypoi
	nt=["python3", "/opt/
	ml/processing/input/c
	ode/training.py"],
	)</pre>
	Exemplo de fluxo de trabalho do Step Functions que executa uma tarefa SageMaker de processamento
	
	Note
	Esse exemplo de fluxo de trabalho inclui somente a etapa do trabalho de SageMaker processamento, não um fluxo de trabalho completo do Step Functions. Para ver um exemplo completo de fluxo de trabalho, consulte Exemplos de	

Tarefa	Descrição	Habilidades necessárias

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

Recursos relacionados

- Processar dados (Amazon SageMaker Developer Guide)
- Adaptando seu próprio contêiner de treinamento (Amazon SageMaker Developer Guide)

Use agentes do Amazon Bedrock para automatizar a criação de controles de entrada de acesso no Amazon EKS por meio de prompts baseados em texto

Criado por Keshav Ganesh (AWS) e Sudhanshu Saurav (AWS)

Resumo

As organizações enfrentam desafios no gerenciamento de controles de acesso e provisionamento de recursos quando várias equipes precisam trabalhar com um cluster compartilhado do Amazon Elastic Kubernetes Service (Amazon EKS). Um serviço gerenciado do Kubernetes, como o Amazon EKS, simplificou as operações de cluster. No entanto, a sobrecarga administrativa de gerenciar o acesso da equipe e as permissões de recursos continua complexa e demorada.

Esse padrão mostra como os agentes do Amazon Bedrock podem ajudar você a automatizar o gerenciamento de acesso ao cluster do Amazon EKS. Essa automação permite que as equipes de desenvolvimento se concentrem no desenvolvimento de seus aplicativos principais, em vez de lidar com a configuração e o gerenciamento do controle de acesso. Você pode personalizar um agente do Amazon Bedrock para realizar ações em uma ampla variedade de tarefas por meio de instruções simples em linguagem natural.

Ao usar AWS Lambda funções como grupos de ação, um agente do Amazon Bedrock pode lidar com tarefas como criar entradas de acesso de usuários e gerenciar políticas de acesso. Além disso, um agente do Amazon Bedrock pode configurar associações de identidade de pod que permitem acesso a recursos AWS Identity and Access Management (IAM) para os pods em execução no cluster. Usando essa solução, as organizações podem simplificar a administração do cluster Amazon EKS com instruções simples baseadas em texto, reduzir a sobrecarga manual e melhorar a eficiência geral do desenvolvimento.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Funções e permissões do IAM estabelecidas para o processo de implantação. Isso inclui permissões para acessar os modelos da Amazon Bedrock Foundation (FM), criar funções Lambda e quaisquer outros recursos necessários em todo o destino. Contas da AWS

- Acesso ativado no ativo Conta da AWS a esses Amazon Bedrock FMs: Amazon Titan Text Embeddings V2 e Anthropic Claude 3 Haiku.
- AWS Command Line Interface (AWS CLI) versão 2.9.11 ou posterior, instalada e configurada.
- eksctl 0.194.0 ou posterior, instalado.

Limitações

- Treinamento e documentação podem ser necessários para ajudar a garantir a adoção tranquila e o uso eficaz dessas técnicas. Usar o Amazon Bedrock, o Amazon EKS, o Lambda, o OpenSearch Amazon Service e a OpenAPI envolve uma curva de aprendizado significativa para desenvolvedores e equipes. DevOps
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte os serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

Essa solução executa as seguintes etapas:

1. O usuário interage com o agente Amazon Bedrock enviando uma solicitação ou consulta que serve como entrada para o agente processar e agir.
2. Com base na solicitação, o agente Amazon Bedrock verifica o esquema da OpenAPI para identificar a API correta a ser segmentada. Se o agente do Amazon Bedrock encontrar a chamada de API correta, a solicitação vai para o grupo de ação associado à função Lambda que implementa essas ações.
3. Se uma API relevante não for encontrada, o agente Amazon Bedrock consulta a OpenSearch coleção. A OpenSearch coleção usa conteúdo indexado da base de conhecimento proveniente do bucket Amazon S3 que contém o Guia do usuário do Amazon EKS.
4. A OpenSearch coleção retorna informações contextuais relevantes para o agente Amazon Bedrock.
5. Para solicitações acionáveis (aquelas que correspondem a uma operação de API), o agente Amazon Bedrock é executado em uma nuvem privada virtual (VPC) e aciona a função Lambda.

6. A função Lambda executa uma ação baseada na entrada do usuário dentro do cluster Amazon EKS.
7. O bucket do Amazon S3 para o código Lambda armazena o artefato que tem o código e a lógica escritos para a função Lambda.

Ferramentas

Serviços da AWS

- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon OpenSearch Service é um serviço gerenciado que ajuda você a implantar, operar e escalar OpenSearch clusters no Nuvem AWS. Seu recurso de coleções ajuda você a organizar seus dados e criar bases de conhecimento abrangentes que assistentes de IA, como agentes do Amazon Bedrock, podem usar.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- O eksctl é utilitário de linha de comando para criar e gerenciar clusters do Kubernetes no Amazon EKS.

Repositório de código

O código desse padrão está disponível no repositório GitHub eks-access-controls-bedrock-agent.

Práticas recomendadas

- Mantenha a maior segurança possível ao implementar esse padrão. Certifique-se de que o cluster Amazon EKS seja privado, tenha permissões de acesso limitadas e que todos os recursos estejam dentro de uma nuvem privada virtual (VPC). Para obter informações adicionais, consulte Melhores práticas de segurança na documentação do Amazon EKS.
- Use chaves gerenciadas pelo AWS KMS cliente sempre que possível e conceda permissões de acesso limitadas a elas.
- Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositório desse padrão, execute o seguinte comando na sua estação de trabalho local: `git clone https://github.com/aws-samples/eks-access-controls-bedrock-agent.git`	AWS DevOps
Obtenha o Conta da AWS ID.	Para obter o Conta da AWS ID, use as seguintes etapas: 1. Abra um shell na pasta raiz do repositório clonado,.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`eks-access-controls-bedrock-agent`
	2. Para obter seu Conta da AWS ID, navegue até o diretório clonado e execute o seguinte comando:
	`AWS_ACCOUNT=$(aws sts get-caller-identity --query "Account" --output text)`
	Esse comando armazena seu Conta da AWS ID na `AWS_ACCOUNT` variável.	

Tarefa	Descrição	Habilidades necessárias

Crie o bucket S3 para o código Lambda.	Para implementar essa solução, você deve criar três buckets do Amazon S3 que atendam a propósitos diferentes, conforme mostrado no diagrama de arquitetura. Os buckets do S3 são para código Lambda, uma base de conhecimento e um esquema OpenAPI.
	
	Para criar o bucket de código Lambda, use as seguintes etapas:
	
	1. Para criar um bucket do S3 para código Lambda, execute o seguinte comando:
	
	`aws s3 mb s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} --region us-east-1`
	
	2. Para instalar a dependência do código Lambda, execute o seguinte comando:
	
	`cd eks-lambda`
	`npm install`
	`tsc`
	`cd .. && cd opensearch-lambda`
	`npm install`
	`tsc`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`cd ..`
	3. Para empacotar o código e carregá-lo no bucket do S3 para Lambda, execute o seguinte comando:
	`aws cloudformation package \ --template-file eks-access-controls.yaml \ --s3-bucket bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} \ --output-template-file eks-access-controls-template.yaml \ --region us-east-1`
	O comando package cria um novo CloudFormation modelo (`eks-access-controls-template.yaml`) que contém:
	• Referências ao código da função Lambda armazenado em seu bucket do S3.
	• Definições para toda a AWS infraestrutura necessária, incluindo VPC, sub-redes, agente Amazon Bedrock e coleção. OpenSearch Você pode usar esse modelo para implantar a	

Tarefa	Descrição	Habilidades necessárias
	solução completa usando CloudFormation.	

Tarefa	Descrição	Habilidades necessárias

Crie o bucket S3 para a base de conhecimento.	Para criar o bucket do Amazon S3 para a base de conhecimento, use as seguintes etapas:
	
	1. Para criar o bucket do Amazon S3 para a base de conhecimento, execute o seguinte comando:
	
	`aws s3 mb s3://eks-knowledge-base-${AWS_ACCOUNT} --region us-east-1`
	
	2. Para baixar o Guia do usuário do Amazon EKS e armazená-lo em um diretório, execute os seguintes comandos:
	
	`mkdir dataSource`
	`cd dataSource`
	`curl https://docs.aws.amazon.com/pdfs/eks/latest/userguide/eks-ug.pdf -o eks-user-guide.pdf`
	
	3. Para carregar o guia do usuário no bucket do S3 que você criou na etapa 1, execute o seguinte comando:
	
	`aws s3 cp eks-user-guide.pdf s3://eks-`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	knowledge-base-${AWS_ACCOUNT} \ --region us-east-1 \ 4. Para retornar ao diretório raiz, execute o seguinte comando: cd ..	
Crie o bucket do S3 para o esquema OpenAPI.	Para criar o bucket do Amazon S3 para o esquema OpenAPI, use as seguintes etapas: 1. Para criar o bucket do S3, execute o seguinte comando: aws s3 mb s3://eks-openapi-schema-${AWS_ACCOUNT} --region us-east-1 2. Para fazer o upload do esquema OpenAPI no bucket do S3, execute o seguinte comando: aws s3 cp openapi-schema.yaml s3://eks-openapi-schema-${AWS_ACCOUNT} --region us-east-1	AWS DevOps

Implante a CloudFormation pilha

Tarefa	Descrição	Habilidades necessárias
Implante a CloudFormation pilha.	Para implantar a CloudFormation pilha, use o arquivo CloudFormation de modelo `eks-access-controls-template.yaml` que você criou anteriormente. Para obter instruções mais detalhadas, consulte Criar uma pilha a partir do CloudFormation console na CloudFormation documentação. **Note** O provisionamento do OpenSearch índice com o CloudFormation modelo leva cerca de 10 minutos. Depois que a pilha for criada, anote o `VPC_ID` e `PRIVATE_SUBNET ID s`.	AWS DevOps
Crie o cluster do Amazon EKS.	Para criar o cluster Amazon EKS dentro da VPC, use as seguintes etapas: 1. Crie uma cópia do arquivo de `eks-config.yaml` configuração e nomeie a	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	cópia como`eks-deploy.yaml` .
	2. Abra `eks-deploy.yaml` em um editor de texto. Em seguida, substitua os seguintes valores de espaço reservado por valores da pilha implantada:`VPC_ID`,, e `PRIVATE_SUBNET1` `PRIVATE_SUBNET2`
	3. Para criar o cluster usando o utilitário eksctl, execute o seguinte comando:
	`eksctl create cluster -f eks-deploy.yaml`
	Note
	Esse processo de criação de cluster pode levar de 15 a 20 minutos para ser concluído.
	4. Para verificar se o cluster foi criado com êxito, execute os seguintes comandos:
	`aws eks describe-cluster --name --query "cluster.status"`	

Tarefa	Descrição	Habilidades necessárias
	`aws eks update-ku beconfig --name -- region kubectl get nodes` Os resultados esperados são os seguintes: • O status do cluster é`ACTIVE`. • O comando `kubectl get nodes` mostra que todos os nós estão no `Ready` estado.	

Conecte a função Lambda e o cluster Amazon EKS

Tarefa	Descrição	Habilidades necessárias
Crie uma conexão entre o cluster Amazon EKS e a função Lambda.	Para configurar permissões de rede e IAM para permitir que a função Lambda se comunique com o cluster Amazon EKS, use as seguintes etapas: 1. Para identificar a função do IAM que está associada à função Lambda, abra AWS Management Console e localize a função Lambda chamada. `bedrock-a gent-eks-access-co ntrol` Anote o Amazon Resource Name (ARN) da função do IAM.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	2. Para criar uma entrada de acesso no cluster Amazon EKS para a função IAM da função Lambda, execute o seguinte comando:
	
	`aws eks create-access-entry --cluster-name eks-testing-cluster --principal-arn <principal-Role-ARN>`
	
	3. Para atribuir `AmazonEKSClusterAdminPolicy` permissões a essa função, execute o seguinte comando:
	
	`aws eks associate-access-policy --cluster-name eks-testing-cluster --principal-arn <principal-Role-ARN> --policy-arn arn:aws:eks::aws:cluster-access-policy/AmazonEKSClusterAdminPolicy --access-scope type=cluster`
	
	Para obter mais informações, consulte Associar políticas de acesso a entradas de acesso e Amazon EKSCluster	

Tarefa	Descrição	Habilidades necessárias
	AdminPolicy na documentação do Amazon EKS. 4. Localize o grupo de segurança do cluster Amazon EKS. Adicione uma regra de entrada para permitir o tráfego de rede de entrada da função Lambda para o cluster Amazon EKS. Use os seguintes valores para a regra de entrada: • Tipo: HTTPS • Intervalo de portas: 443 • Fonte — Grupo de segurança Lambda Para obter mais informações, consulte Configurar regras de grupos de segurança na documentação da Amazon VPC.	

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Teste o agente Amazon Bedrock.	Antes de testar o agente Amazon Bedrock, certifique-se de fazer o seguinte:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• Teste primeiro com funções que não sejam de produção. • Documente todas as alterações feitas no acesso ao cluster. • Tenha um plano para reverter as alterações, se necessário. Para acessar o agente Amazon Bedrock, use as seguintes etapas: 1. Faça login na função AWS Management Console usando uma função do IAM com as permissões do Amazon Bedrock e abra o console do Amazon Bedrock em. https://console.aws.amazon.com/bedrock/ 2. No painel de navegação à esquerda, selecione Agentes. Em seguida, escolha seu agente configurado na seção Agentes. 3. Para testar o agente, experimente os seguintes exemplos de prompts, nos quais você `Principal-ARN-OF-ROLE` substitui	

Tarefa	Descrição	Habilidades necessárias
	por um ARN real da função do IAM: • Para criar uma entrada de acesso para qualquer função do IAM que você queira fornecer acesso ao cluster EKS, use o seguinte prompt: `Create an access entry in cluster eks-testing-new for a role whose principal arn is <Principal-ARN-OF-ROLE> with access policy as AmazonEKSAdminPolicy` Resultado esperado: • O agente deve confirmar a criação da entrada de acesso. • Para verificar, verifique usando AWS Management Console ou use a API Amazon EKS e execute o seguinte comando: `aws eks list-access-entries --cluster-name ekscluster` • Para descrever a entrada de acesso que você criou, use o seguinte prompt: `Describe an access`	

Tarefa	Descrição	Habilidades necessárias
	`entry in cluster eks-testing-new whose principal arn is <Principal-ARN-OF-ROLE>` Resultado esperado: • O agente deve devolver detalhes sobre a entrada de acesso. • Os detalhes devem corresponder ao que você configurou anteriormente para a entrada de acesso. • Para excluir a entrada de acesso que você criou, use o seguinte prompt: `Delete the access entry in cluster eks-testing-new whose principal arn is <Principal-ARN-OF-ROLE>` Resultado esperado: • O agente deve confirmar a exclusão da entrada de acesso. • Para verificar, verifique usando AWS Management Console ou use a API Amazon EKS e execute o seguinte comando: `aws eks list-access-`	

Tarefa	Descrição	Habilidades necessárias
	`entries --cluster -name ekscluster` Você também pode solicitar que o agente execute ações para associações do EKS Pod Identity. Para obter mais detalhes, consulte Saiba como o EKS Pod Identity concede acesso aos pods Serviços da AWS na documentação do Amazon EKS.	

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpar os recursos	Para limpar os recursos que esse padrão criou, use o procedimento a seguir. Aguarde a conclusão de cada etapa de exclusão antes de prosseguir para a próxima etapa. **Warning** Esse procedimento excluirá permanent emente todos os recursos criados por essas pilhas. Certifique-se de ter feito backup de todos	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	os dados importantes antes de continuar.
	
	1. Para excluir o cluster Amazon EKS, execute o seguinte comando:
	
	`eksctl delete cluster -f eks-deploy.yaml`
	
	Note
	Essa operação pode levar de 15 a 20 minutos para ser concluída.
	
	2. Para excluir os buckets do Amazon S3, execute os seguintes comandos:
	• Para esvaziar o balde Lambda:
	
	`aws s3 rm s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} --recursive`
	
	• Para esvaziar o bucket da base de conhecimento:
	
	`aws s3 rm s3://eks-knowledge-base-`	

Tarefa	Descrição	Habilidades necessárias

	`${AWS_ACCOUNT} –recursive`
	• Para esvaziar o bucket do esquema OpenAPI:
	`aws s3 rm s3://bedrock-agent-openapi-schema-${AWS_ACCOUNT} –recursive`
	• Para excluir os compartimentos vazios:
	`aws s3 rb s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT}`
	`aws s3 rb s3://eks-knowledge-base-${AWS_ACCOUNT}`
	`aws s3 rb s3://bedrock-agent-openapi-schema-${AWS_ACCOUNT}`
	3. Para excluir a CloudFormation pilha, execute o seguinte comando:
	`aws cloudformation delete-stack \ --stack-name`
	4. Para verificar a exclusão do cluster Amazon EKS, execute o seguinte comando:	

Tarefa	Descrição	Habilidades necessárias

	`eksctl get clusters`
	5. Para verificar a exclusão dos buckets do Amazon S3, execute os seguintes comandos:
	• Para verificar a exclusão do bucket Lambda:
	`aws s3 ls | grep "bedrock-agent-lambda-artifacts"`
	• Para verificar a exclusão do bucket da base de conhecimento:
	`aws s3 ls | grep "eks-knowledge-base"`
	• Para verificar a exclusão do bucket do esquema OpenAPI:
	`aws s3 ls | grep "bedrock-agent-openapi-schema"`
	6. Para verificar a exclusão da pilha, execute o seguinte comando:
	`aws cloudformation list-stacks \--query 'StackSummaries[?StackName==``]'`	

Tarefa	Descrição	Habilidades necessárias
	Se a pilha não for excluída, consulte Solução de problemas.	

Solução de problemas

Problema	Solução
Um código de erro diferente de zero é retornado durante a configuração do ambiente.	Verifique se você está usando a pasta correta ao executar qualquer comando para implantar essa solução. Para obter mais informações, consulte o arquivo FIRST_DEPLOY.md no repositório desse padrão.
A função Lambda não é capaz de realizar a tarefa.	Certifique-se de que a conectividade esteja configurada corretamente da função Lambda para o cluster Amazon EKS.
As solicitações do agente não reconhecem o. APIs	Reimplante a solução. Para obter mais informações, consulte o arquivo RE_DEPLOY .md no repositório desse padrão.
A pilha não é excluída.	Uma tentativa inicial de excluir a pilha pode falhar. Essa falha pode ocorrer devido a problemas de dependência com o recurso personalizado que foi criado para a OpenSearch coleção que faz a indexação da base de conhecimento. Para excluir a pilha, tente novamente a operação de exclusão mantendo o recurso personalizado.

Recursos relacionados

AWS Blog

- Uma análise aprofundada dos controles simplificados de gerenciamento de acesso do Amazon EKS

Documentação do Amazon Bedrock

- Automatize tarefas em seu aplicativo usando agentes de IA
- Como o Amazon Bedrock Agents funciona
- Teste e solucione problemas de comportamento do agente
- Use grupos de ação para definir ações para seu agente realizar

Documentação do Amazon EKS

- Saiba como o controle de acesso funciona no Amazon EKS

Implemente um caso de uso do RAG AWS usando o Terraform e o Amazon Bedrock

Criado por Martin Maritsch (AWS), Alice Morano (AWS), Julian Ferdinand Grueber (AWS), Nicolas Jacob Baer (AWS), Olivier Brique (AWS) e Nicola D Orazio (AWS)

Resumo

AWS fornece várias opções para criar seus casos de uso de IA generativa habilitados para Retrieval Augmented Generation (RAG). Esse padrão fornece uma solução para um aplicativo baseado em RAG baseado LangChain e compatível com o Amazon Aurora PostgreSQL como um armazenamento vetorial. Você pode implantar diretamente essa solução com o Terraform em seu Conta da AWS e implementar o seguinte caso de uso simples do RAG:

1. O usuário carrega manualmente um arquivo em um bucket do Amazon Simple Storage Service (Amazon S3), como um arquivo do Microsoft Excel ou um documento PDF. (Para obter mais informações sobre os tipos de arquivo compatíveis, consulte a documentação não estruturada.)
2. O conteúdo do arquivo é extraído e incorporado em um banco de dados de conhecimento baseado no Aurora PostgreSQL sem servidor, compatível com o Aurora, que suporta a ingestão quase em tempo real de documentos no armazenamento vetorial. Essa abordagem permite que o modelo RAG acesse e recupere informações relevantes para casos de uso em que baixas latências são importantes.
3. Quando o usuário se envolve com o modelo de geração de texto, ele aprimora a interação por meio do aumento da recuperação de conteúdo relevante dos arquivos enviados anteriormente.

O padrão usa Amazon Titan Text Embeddings v2 como modelo de incorporação e Anthropic Claude 3 Sonnet como modelo de geração de texto, ambos disponíveis no Amazon Bedrock.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Command Line Interface (AWS CLI) instalado e configurado com o seu Conta da AWS. Para obter instruções de instalação, consulte Instalar ou atualizar para a versão mais recente do AWS CLI na AWS CLI documentação. Para revisar suas AWS credenciais e seu acesso à sua conta, consulte Configuração e configurações do arquivo de credenciais na AWS CLI documentação.

- Acesso ao modelo que está habilitado para os modelos de linguagem grande necessários (LLMs) no console Amazon Bedrock do seu Conta da AWS. Esse padrão requer o seguinte LLMs:
  - `amazon.titan-embed-text-v2:0`
  - `anthropic.claude-3-sonnet-20240229-v1:0`

Limitações

- Essa arquitetura de exemplo não inclui uma interface para responder perguntas programáticas com o banco de dados vetoriais. Se seu caso de uso exigir uma API, considere adicionar o Amazon API Gateway com uma AWS Lambda função que executa tarefas de recuperação e resposta a perguntas.
- Esse exemplo de arquitetura não inclui recursos de monitoramento para a infraestrutura implantada. Se seu caso de uso exigir monitoramento, considere adicionar serviços AWS de monitoramento.
- Se você fizer upload de muitos documentos em um curto espaço de tempo para o bucket do Amazon S3, a função Lambda poderá encontrar limites de taxa. Como solução, você pode desacoplar a função Lambda com uma fila do Amazon Simple Queue Service (Amazon SQS), na qual você pode controlar a taxa de invocações do Lambda.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- AWS CLI versão 2 ou posterior
- Docker versão 26.0.0 ou posterior
- Poesia versão 1.7.1 ou posterior
- Python versão 3.10 ou posterior
- Terraform versão 1.8.4 ou posterior

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

Esse diagrama ilustra o seguinte:

1. Quando um objeto é criado no bucket do Amazon S3`bedrock-rag-template-<account_id>`, uma notificação do Amazon S3 invoca a função Lambda. `data-ingestion-processor`
2. A função Lambda `data-ingestion-processor` é baseada em uma imagem do Docker armazenada no repositório Amazon Elastic Container Registry (Amazon ECR). `bedrock-rag-template`

   A função usa o LangChain S3 FileLoader para ler o arquivo como um LangChain documento. Em seguida, LangChain RecursiveCharacterTextSplitterfragmente cada documento, dados a `CHUNK_SIZE` e a, dependendo do tamanho máximo do token do modelo de incorporação Amazon Titan Text Embedding V2. `CHUNK_OVERLAP` Em seguida, a função Lambda invoca o modelo de incorporação no Amazon Bedrock para incorporar os fragmentos em representações vetoriais numéricas. Por fim, esses vetores são armazenados no banco de dados Aurora PostgreSQL. Para acessar o banco de dados, a função Lambda primeiro recupera o nome de usuário e a senha de. AWS Secrets Manager
3. Na instância do notebook Amazon SageMaker AIaws-sample-bedrock-rag-template, o usuário pode escrever uma solicitação de pergunta. O código invoca Claude 3 no Amazon Bedrock e adiciona as informações da base de conhecimento ao contexto do prompt. Como resultado, a Cláusula 3 fornece respostas usando as informações nos documentos.

A abordagem desse padrão em relação à rede e à segurança é a seguinte:

- A função Lambda `data-ingestion-processor` está em uma sub-rede privada dentro da nuvem privada virtual (VPC). A função Lambda não tem permissão para enviar tráfego para a Internet pública por causa de seu grupo de segurança. Como resultado, o tráfego para o Amazon S3 e o Amazon Bedrock é roteado somente pelos endpoints da VPC. Consequentemente, o tráfego não atravessa a Internet pública, o que reduz a latência e adiciona uma camada adicional de segurança no nível da rede.
- Todos os recursos e dados são criptografados sempre que aplicável usando a chave AWS Key Management Service (AWS KMS) com o aliasaws-sample/bedrock-rag-template.

Automação e escala

Esse padrão usa o Terraform para implantar a infraestrutura do repositório de código em um. Conta da AWS

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e compatível com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL. Nesse padrão, o Aurora compatível com PostgreSQL usa o plug-in pgvector como banco de dados vetoriais.
- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável. Nesse padrão, o Amazon ECR hospeda a imagem do Docker para a função Lambda`data-ingestion-processor`.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado. Nesse padrão, o Lambda ingere dados no armazenamento vetorial.
- O Amazon SageMaker AI é um serviço gerenciado de aprendizado de máquina (ML) que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção.
- O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria

no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS. A VPC inclui sub-redes e tabelas de roteamento para controlar o fluxo de tráfego.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.
- Poetry é uma ferramenta para gerenciamento e empacotamento de dependências em Python.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub terraform-rag-template-using-amazon-bedrock.

Práticas recomendadas

- Embora esse exemplo de código possa ser implantado em qualquer um Região da AWS, recomendamos que você use o Leste dos EUA (Norte da Virgínia) — `us-east-1` ou Oeste dos EUA (Norte da Califórnia) —`us-west-1`. Essa recomendação é baseada na disponibilidade de modelos básicos e de incorporação no Amazon Bedrock no momento da publicação desse padrão. Para obter uma up-to-date lista do suporte ao modelo da Amazon Bedrock Foundation em Regiões da AWS, consulte Model support by Região da AWS na documentação do Amazon Bedrock. Para obter informações sobre como implantar esse exemplo de código em outras regiões, consulte Informações adicionais.
- Esse padrão fornece somente uma demonstração proof-of-concept (PoC) ou piloto. Se você quiser levar o código para produção, certifique-se de usar as seguintes práticas recomendadas:
  - Ative o registro de acesso ao servidor para o Amazon S3.
  - Configure o monitoramento e o alerta para a função Lambda.
  - Se seu caso de uso exigir uma API, considere adicionar o Amazon API Gateway com uma função Lambda que executa tarefas de recuperação e resposta a perguntas.

- Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Implemente a solução em um Conta da AWS

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o GitHub repositório fornecido com esse padrão, use o seguinte comando: `git clone https://github.com/aws-samples/terraform-rag-template-using-amazon-bedrock`	AWS DevOps
Configure as variáveis.	Para configurar os parâmetros desse padrão, faça o seguinte: 1. No seu computador, no GitHub repositório, use o seguinte comando para abrir a `terraform` pasta: `cd terraform` 2. Abra o `commons.tfvars` arquivo e personalize os parâmetros de acordo com suas necessidades.	AWS DevOps
Implante a solução.	Para implantar a solução, faça o seguinte:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	1. Na `terraform` pasta, use o comando a seguir para executar o Terraform e passar as variáveis que você personalizou:
	`terraform init`
	`terraform apply -var-file=commons.tfvars`
	2. Confirme se os recursos mostrados no diagrama de arquitetura foram implantados com êxito.
	
	A implantação da infraestrutura provisiona uma instância de SageMaker IA dentro da VPC e com as permissões para acessar o banco de dados Aurora PostgreSQL.	

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Execute a demonstração.	Depois que a implantação anterior da infraestrutura for bem-sucedida, use as etapas a seguir para executar a demonstração em um notebook Jupyter:	AWS geral

Tarefa	Descrição	Habilidades necessárias
	1. Faça login no AWS Management Console Conta da AWS local onde a infraestrutura está implantada. 2. Abra a instância do notebook SageMaker AIaws-sample-bedrock-rag-template . 3. Mova o notebook rag_demo.ipynb Jupyter para a instância do notebook SageMaker AI usando o recurso de arrastar e soltar. 4. Abra a instância do notebook rag_demo.ipynb na SageMaker IA e escolha o conda_python3 kernel. 5. Para executar a demonstração, execute as células do notebook. O notebook Jupyter orienta você pelo seguinte processo: • Requisitos de instalação • Definição de incorporação • Conexão de banco de dados • Ingestão de dados	

Tarefa	Descrição	Habilidades necessárias
	• Recuperação de geração de texto aumentada • Consultas de documentos relevantes	

Limpe a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Limpe a infraestrutura.	Para remover todos os recursos que você criou quando eles não são mais necessários, use o seguinte comando: `terraform destroy -var-file=commons.tfvars`	AWS DevOps

Recursos relacionados

AWS recursos

- Criar funções do Lambda com Python
- Parâmetros de inferência para modelos de fundação
- Acesso aos modelos da Amazon Bedrock Foundation
- O papel dos bancos de dados vetoriais em aplicativos generativos de IA (AWS Database Blog)
- Trabalho com Amazon Aurora PostgreSQL

Outros recursos

- documentação pgvector

Mais informações

Implementar um banco de dados vetorial

Esse padrão usa o Aurora compatível com PostgreSQL para implementar um banco de dados vetoriais para RAG. Como alternativa ao Aurora PostgreSQL, AWS fornece outros recursos e serviços para o RAG, como o Amazon Bedrock Knowledge Bases e o Amazon Service. OpenSearch Você pode escolher a solução que melhor atenda às suas necessidades específicas:

- O Amazon OpenSearch Service fornece mecanismos distribuídos de pesquisa e análise que você pode usar para armazenar e consultar grandes volumes de dados.
- O Amazon Bedrock Knowledge Bases foi projetado para criar e implantar bases de conhecimento como uma abstração adicional para simplificar o processo de ingestão e recuperação de RAG. As bases de conhecimento Amazon Bedrock podem funcionar tanto com o Aurora OpenSearch PostgreSQL quanto com o Amazon Service.

Implantação em outros Regiões da AWS

Conforme descrito em Arquitetura, recomendamos que você use a Região Leste dos EUA (Norte da Virgínia) `us-east-1` ou Oeste dos EUA (Norte da Califórnia) `us-west-1` para implantar esse exemplo de código. No entanto, há duas maneiras possíveis de implantar esse exemplo de código em regiões diferentes de `us-east-1` `us-west-1` e. Você pode configurar a região de implantação no `commons.tfvars` arquivo. Para acessar o modelo básico entre regiões, considere as seguintes opções:

- Atravessando a Internet pública — Se o tráfego puder atravessar a Internet pública, adicione gateways de Internet à VPC. Em seguida, ajuste o grupo de segurança atribuído à função Lambda `data-ingestion-processor` e à instância do notebook SageMaker AI para permitir o tráfego de saída para a Internet pública.
- Não atravessar a Internet pública — Para implantar essa amostra em qualquer região que não seja `us-east-1` ou`us-west-1`, faça o seguinte:

1. Na `us-west-1` região `us-east-1` ou, crie uma VPC adicional, incluindo um VPC endpoint para. `bedrock-runtime`
2. Crie uma conexão de emparelhamento usando o emparelhamento de VPC ou um gateway de trânsito para a VPC do aplicativo.

3. Ao configurar o cliente `bedrock-runtime` boto3 em qualquer função Lambda fora de `us-east-1` ou`us-west-1`, passe o nome DNS privado do VPC endpoint para `bedrock-runtime` in `us-east-1` ou us-west-1 como o para o cliente boto3. `endpoint_url`

Implante a lógica de pré-processamento em um modelo de ML em um único endpoint usando um pipeline de inferência na Amazon SageMaker

Criado por Mohan Gowda Purushothama (AWS), Gabriel Rodriguez Garcia (AWS) e Mateusz Zaremba (AWS)

Resumo

Esse padrão explica como implantar vários objetos de modelo de pipeline em um único endpoint usando um pipeline de inferência na Amazon. SageMaker O objeto do modelo de pipeline representa diferentes estágios do fluxo de trabalho de machine learning (ML), como pré-processamento, inferência de modelos e pós-processamento. Para ilustrar a implantação de objetos de modelo de pipeline conectados em série, esse padrão mostra como implantar um contêiner Scikit-learn de pré-processamento e um modelo de regressão baseado no algoritmo linear do aluno incorporado. SageMaker A implantação é hospedada por trás de um único endpoint em SageMaker.

> **Note**
>
> A implantação nesse padrão usa o tipo de instância ml.m4.2xlarge. Recomendamos usar um tipo de instância que se alinhe aos seus requisitos de tamanho de dados e à complexidade do seu fluxo de trabalho. Para obter mais informações, consulte Amazon SageMaker Pricing. Esse padrão usa imagens do Docker pré-construídas para o Scikit-learn, mas você pode usar seus próprios contêineres do Docker e integrá-los ao seu fluxo de trabalho.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Python 3.9
- SDK para Amazon SageMaker Python e biblioteca Boto3
- Função do AWS Identity and Access Management (AWS IAM) com permissões básicas e SageMaker permissões do Amazon Simple Storage Service (Amazon S3)

Versões do produto

- SDK 2.49.2 para Amazon SageMaker Python

Arquitetura

Pilha de tecnologias de destino

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon SageMaker
- SageMaker Estúdio Amazon
- Amazon Simple Storage Service (Amazon S3)
- Endpoint de inferência em tempo real para a Amazon SageMaker

Arquitetura de destino

O diagrama a seguir mostra a arquitetura para a implantação de um objeto de modelo de SageMaker pipeline da Amazon.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um SageMaker notebook implanta um modelo de pipeline.
2. Um bucket do S3 armazena os artefatos do modelo.
3. O Amazon ECR obtém as imagens do contêiner de origem do bucket do S3.

Ferramentas

Ferramentas da AWS

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- SageMakerA Amazon é um serviço gerenciado de ML que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção.
- O Amazon SageMaker Studio é um ambiente de desenvolvimento integrado (IDE) baseado na web para ML que permite criar, treinar, depurar, implantar e monitorar seus modelos de ML.

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Código

O código desse padrão está disponível no GitHub Inference Pipeline com o repositório Scikit-learn e Linear Learner.

Épicos

Prepare o conjunto de dados

Tarefa	Descrição	Habilidades necessárias

Prepare o conjunto de dados para sua tarefa de regressão.	Abra um caderno no Amazon SageMaker Studio.
	
	Para importar todas as bibliotecas necessárias e inicializar seu ambiente de trabalho, use o código de exemplo a seguir em seu notebook:
	
	`import sagemaker`
	`from sagemaker import get_execution_role`
	
	`sagemaker_session = sagemaker.Session()`
	
	`# Get a SageMaker-compatible role used by this Notebook Instance.`
	`role = get_execution_role()`
	
	`# S3 prefix`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias

	`bucket = sagemaker_session.default_bucket()`
	`prefix = "Scikit-LinearLearner-pipeline-abalone-example"`
	
	Para baixar um conjunto de dados de exemplo, adicione o seguinte código ao seu caderno:
	
	`! mkdir abalone_data`
	`! aws s3 cp s3://sagemaker-sample-files/datasets/tabular/uci_abalone/abalone.csv ./abalone_data`
	
	Note
	O exemplo desse padrão usa o Conjunto de Dados Abalone do UCI Machine Learning Repository.	

Tarefa	Descrição	Habilidades necessárias

Faça upload do conjunto de dados em um bucket do S3.	No caderno em que você preparou seu conjunto de dados anteriormente, adicione o código a seguir para carregar seus dados de amostra em um bucket do S3:
	`WORK_DIRECTORY = "abalone_data"`
	
	`train_input = sagemaker_session.upload_data( path="{}/{}".format(WORK_DIRECTORY, "abalone.csv"), bucket=bucket, key_prefix="{}/{}".format(prefix, "train"), )`
		Cientista de dados

Crie o pré-processador de dados usando SKLearn

Tarefa	Descrição	Habilidades necessárias
Prepare o script preprocessor.py.	1. Copie a lógica de pré-processamento do arquivo Python GitHub no repositório sklearn_abalone_featurizer.py e cole o código em um arquivo Python separado chamado. `sklearn_abalone_featurizer.py` Você pode modificar o código para se adequar ao seu	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	conjunto de dados personalizado e fluxo de trabalho personalizado. 2. Salve o `sklearn_abalone_featurizer.py` arquivo no diretório raiz do seu projeto (ou seja, no mesmo local em que você executa o SageMaker notebook).	

Tarefa	Descrição	Habilidades necessárias

Crie o objeto do SKLearn pré-processador.	Para criar um objeto SKLearn pré-processador (chamado SKLearn Estimator) que você possa incorporar ao seu pipeline de inferência final, execute o seguinte código em seu notebook: SageMaker
	
	`from sagemaker.sklearn.estimator import SKLearn`
	
	`FRAMEWORK_VERSION = "0.23-1"`
	`script_path = "sklearn_abalone_featurizer.py"`
	
	`sklearn_preprocessor = SKLearn(`
	`entry_point=script_path,`
	`role=role,`
	`framework_version=FRAMEWORK_VERSION,`
	`instance_type="ml.c4.xlarge",`
	`sagemaker_session=sagemaker_session,`
	`)`
	`sklearn_preprocessor.fit({"train": train_input})`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias

Teste a inferência do pré-processador.	Para confirmar se seu pré-processador está definido corretamente, inicie um trabalho de transformação em lote inserindo o seguinte código em seu SageMaker notebook:
	
	`# Define a SKLearn Transformer from the trained SKLearn Estimator`
	`transformer = sklearn_preprocessor.transformer(`
	`instance_count=1, instance_type="ml.m5.xlarge", assemble_with="Line", accept="text/csv"`
	`)`
	
	`# Preprocess training input`
	`transformer.transform(train_input, content_type="text/csv")`
	`print("Waiting for transform job: " + transformer.latest_transform_job.job_name)`
	`transformer.wait()`
	`preprocessed_train = transformer.output_path`	

Criar um modelo de machine learning

Tarefa	Descrição	Habilidades necessárias

Criar um objeto modelo.	Para criar um objeto de modelo com base no algoritmo linear do aluno, insira o seguinte código em seu SageMaker caderno:
	
	`import boto3 from sagemaker .image_uris import retrieve`
	
	`ll_image = retrieve( "linear-learner", boto3.Session().region_name) s3_ll_output_key_prefix = "ll_training_output" s3_ll_output_location = "s3://{}/{}/{}/{}" .format( bucket, prefix, s3_ll_output_key_prefix, "ll_model" )`
	
	`ll_estimator = sagemaker.estimator.Estimator( ll_image, role, instance_count=1, instance_type="ml.m4.2xlarge", volume_size=20, max_run=3600, input_mode="File",`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias

	<pre> output_path=s3_ll_
	output_location,
	    sagemaker_session=
	sagemaker_session,
	)
	
	ll_estimator.s
	et_hyperparameters
	(feature_dim=10,
	 predictor_type="re
	gressor", mini_batc
	h_size=32)
	
	ll_train_data =
	 sagemaker.inputs.T
	rainingInput(
	    preprocessed_train
	,
	    distribution="Full
	yReplicated",
	    content_type="text
	/csv",
	    s3_data_type="S3Pr
	efix",
	)
	
	data_channels =
	 {"train": ll_train_
	data}
	ll_estimator.fit(inpu
	ts=data_channels,
	 logs=True)</pre>	

	O código anterior recupera a imagem do Docker do Amazon ECR do Registro público do Amazon ECR para o modelo, cria um objeto estimador e, em seguida, usa	

Tarefa	Descrição	Habilidades necessárias
	esse objeto para treinar o modelo de regressão.	

Implanta o pipeline final

Tarefa	Descrição	Habilidades necessárias

Implantar o modelo de pipeline.	Para criar um objeto de modelo de pipeline (ou seja, um objeto de pré-processador) e implantar o objeto, insira o seguinte código em seu SageMaker notebook:
	`from sagemaker.model import Model`
	`from sagemaker.pipeline import PipelineModel`
	`import boto3`
	`from time import gmtime, strftime`
	
	`timestamp_prefix = strftime("%Y-%m-%d-%H-%M-%S", gmtime())`
	
	`scikit_learn_inferencee_model = sklearn_preprocessor.create_model()`
	`linear_learner_model = ll_estimator.create_model()`
	
	`model_name = "inference-pipeline-" + timestamp_prefix`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	``` endpoint_name = "inference-pipeline- ep-" + timestamp_prefix sm_model = PipelineM odel(name=model_name, role=role, models= [scikit_learn_infe rencee_model, linear_learner_model]) sm_model.deploy(init ial_instance_count =1, instance_type="ml. c4.xlarge", endpoint_ name=endpoint_name) ``` **Note** Você pode ajustar o tipo de instância usado no objeto de modelo para atender às suas necessidades.	

Tarefa	Descrição	Habilidades necessárias

Teste a inferência	Para confirmar se o endpoint está funcionando corretamente, execute o seguinte exemplo de código de inferência em seu SageMaker notebook:
	
	`from sagemaker.predictor import Predictor`
	`from sagemaker.serializers import CSVSerializer`
	
	`payload = "M, 0.44, 0.365, 0.125, 0.516, 0.2155, 0.114, 0.155"`
	`actual_rings = 10`
	`predictor = Predictor(`
	`endpoint_name=endpoint_name, sagemaker_session=sagemaker_session, serializer=CSVSerializer()`
	`)`
	
	`print(predictor.predict(payload))`
		Cientista de dados

Recursos relacionados

- Pré-processe os dados de entrada antes de fazer previsões usando os pipelines de SageMaker inferência da Amazon e o Scikit-learn (blog do AWS Machine Learning)
- Machine Learning de ponta a ponta com a Amazon SageMaker (GitHub)

Desenvolva assistentes avançados baseados em bate-papo com IA generativa usando RAG e prompting ReAct

Criado por Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS) e Shuai Cao (AWS)

Resumo

Uma empresa típica tem 70% de seus dados presos em sistemas isolados. Você pode usar assistentes generativos baseados em bate-papo com inteligência artificial para descobrir insights e relacionamentos entre esses silos de dados por meio de interações em linguagem natural. Para tirar o máximo proveito da IA generativa, os resultados devem ser confiáveis, precisos e incluir os dados corporativos disponíveis. Assistentes bem-sucedidos baseados em bate-papo dependem do seguinte:

- Modelos generativos de IA (como Anthropic Claude 2)
- Vetorização da fonte de dados
- Técnicas avançadas de raciocínio, como a ReAct estrutura, para estimular o modelo

Esse padrão fornece abordagens de recuperação de dados de fontes de dados como buckets do Amazon Simple Storage Service (Amazon S3), AWS Glue e Amazon Relational Database Service (Amazon RDS). O valor é obtido a partir desses dados intercalando a Geração Aumentada de Recuperação (RAG) com métodos. chain-of-thought Os resultados apoiam conversas complexas com assistentes baseadas em bate-papo que se baseiam na totalidade dos dados armazenados de sua empresa.

Esse padrão usa SageMaker manuais e tabelas de dados de preços da Amazon como exemplo para explorar os recursos de um assistente generativo baseado em bate-papo com IA. Você criará um assistente baseado em bate-papo que ajudará os clientes a avaliar o SageMaker serviço respondendo a perguntas sobre preços e recursos do serviço. A solução usa uma biblioteca Streamlit para criar o aplicativo de front-end e a LangChain estrutura para desenvolver o back-end do aplicativo alimentado por um modelo de linguagem grande (LLM).

As consultas ao assistente baseado em bate-papo são atendidas com uma classificação inicial de intenção para encaminhamento para um dos três fluxos de trabalho possíveis. O fluxo de trabalho mais sofisticado combina orientação consultiva geral com análises complexas de preços. Você pode adaptar o padrão para se adequar aos casos de uso corporativo, corporativo e industrial.

Pré-requisitos e limitações

Pré-requisitos

- AWS Command Line Interface (AWS CLI) instalada e configurada
- Kit de ferramentas do AWS Cloud Development Kit (AWS CDK) 2.114.1 ou posterior instalado e configurado
- Familiaridade básica com Python e AWS CDK
- Git instalado
- Docker instalado
- Python 3.11 ou posterior instalado e configurado (para obter mais informações, consulte a seção Ferramentas)
- Uma conta ativa da AWS inicializada usando o AWS CDK
- Acesso aos modelos Amazon Titan e Anthropic Claude ativado no serviço Amazon Bedrock
- Credenciais de segurança da AWS, inclusive `AWS_ACCESS_KEY_ID`, configuradas corretamente em seu ambiente de terminal

Limitações

- LangChain não suporta todos os LLM para streaming. Os modelos Anthropic Claude são suportados, mas os modelos do AI21 Labs não.
- Essa solução é implantada em uma única conta da AWS.
- Essa solução pode ser implantada somente nas regiões da AWS onde o Amazon Bedrock e o Amazon Kendra estão disponíveis. Para obter informações sobre disponibilidade, consulte a documentação do Amazon Bedrock e do Amazon Kendra.

Versões do produto

- Python versão 3.11 ou posterior
- Streamlit versão 1.30.0 ou posterior
- Streamlit-chat versão 0.1.1 ou posterior
- LangChain versão 0.1.12 ou posterior
- AWS CDK versão 2.132.1 ou posterior

Arquitetura

Pilha de tecnologias de destino

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

Arquitetura de destino

O código do AWS CDK implantará todos os recursos necessários para configurar o aplicativo assistente baseado em chat em uma conta da AWS. O aplicativo assistente baseado em bate-papo mostrado no diagrama a seguir foi projetado para responder às consultas SageMaker relacionadas dos usuários. Os usuários se conectam por meio de um Application Load Balancer a uma VPC que contém um cluster do Amazon ECS que hospeda o aplicativo Streamlit. Uma função Lambda de orquestração se conecta ao aplicativo. As fontes de dados do bucket do S3 fornecem dados para a função Lambda por meio do Amazon Kendra e do AWS Glue. A função Lambda se conecta ao Amazon Bedrock para responder consultas (perguntas) de usuários assistentes baseados em bate-papo.

1. A função Lambda de orquestração envia a solicitação de prompt do LLM para o modelo Amazon Bedrock (Claude 2).
2. O Amazon Bedrock envia a resposta do LLM de volta para a função Lambda de orquestração.

Fluxo lógico dentro da função Lambda de orquestração

Quando os usuários fazem uma pergunta por meio do aplicativo Streamlit, ele invoca diretamente a função Lambda de orquestração. O diagrama a seguir mostra o fluxo lógico quando a função Lambda é invocada.

- Etapa 1 — A entrada `query` (pergunta) é classificada em uma das três intenções:
  - Perguntas gerais de SageMaker orientação
  - Perguntas gerais SageMaker sobre preços (treinamento/inferência)
  - Perguntas complexas relacionadas SageMaker a preços
- Etapa 2 — A entrada `query` inicia um dos três serviços:
  - `RAG Retrieval service`, que recupera o contexto relevante do banco de dados vetoriais Amazon Kendra e chama o LLM por meio do Amazon Bedrock para resumir o contexto recuperado como resposta.
  - `Database Query service`, que usa o LLM, os metadados do banco de dados e as linhas de amostra das tabelas relevantes para converter a `query` entrada em uma consulta SQL. O serviço Database Query executa a consulta SQL no banco de dados de SageMaker preços por meio do Amazon Athena e resume os resultados da consulta como resposta.
  - `In-context ReACT Agent service`, que divide a entrada `query` em várias etapas antes de fornecer uma resposta. O agente usa `RAG Retrieval service` e `Database Query service` como ferramentas para recuperar informações relevantes durante o processo de raciocínio. Depois que os processos de raciocínio e ações são concluídos, o agente gera a resposta final como resposta.
- Etapa 3 — A resposta da função Lambda de orquestração é enviada ao aplicativo Streamlit como saída.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que permite analisar dados diretamente no Amazon Simple Storage Service (Amazon S3) usando SQL padrão.
- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados. Esse padrão usa um crawler do AWS Glue e uma tabela do Catálogo de Dados do AWS Glue.
- O Amazon Kendra é um serviço de pesquisa inteligente que usa processamento de linguagem natural e algoritmos avançados de aprendizado de máquina para retornar respostas específicas às perguntas de pesquisa de seus dados.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade.

Repositório de código

O código desse padrão está disponível no GitHub genai-bedrock-chatbotrepositório.

O repositório de código contém os seguintes arquivos e pastas:

- `assets`pasta — Os ativos estáticos, o diagrama de arquitetura e o conjunto de dados público
- `code/lambda-container`pasta — O código Python que é executado na função Lambda
- `code/streamlit-app`pasta — O código Python que é executado como imagem de contêiner no Amazon ECS
- `tests`pasta — Os arquivos Python que são executados para testar a unidade das construções do AWS CDK
- `code/code_stack.py`— O AWS CDK constrói arquivos Python usados para criar recursos da AWS

- `app.py`— O AWS CDK empilha arquivos Python usados para implantar recursos da AWS na conta de destino da AWS
- `requirements.txt`— A lista de todas as dependências do Python que devem ser instaladas para o AWS CDK
- `requirements-dev.txt`— A lista de todas as dependências do Python que devem ser instaladas para que o AWS CDK execute o pacote de testes unitários
- `cdk.json`: o arquivo de entrada para fornecer os valores necessários para gerar recursos

> **Note**
>
> O código do AWS CDK usa construções L3 (camada 3) e políticas do AWS Identity and Access Management (IAM) gerenciadas pela AWS para implantar a solução.

Práticas recomendadas

- O exemplo de código fornecido aqui é somente para uma demonstração proof-of-concept (PoC) ou piloto. Se você quiser levar o código para a produção, certifique-se de usar as seguintes práticas recomendadas:
  - O registro de acesso ao Amazon S3 está ativado.
  - Os registros de fluxo de VPC estão habilitados.
  - O índice Amazon Kendra Enterprise Edition está ativado.
- Configure o monitoramento e o alerta para a função do Lambda. Para obter mais informações, consulte Monitorar e solucionar problemas de funções do Lambda. Para obter as melhores práticas gerais ao trabalhar com funções do Lambda, consulte a documentação da AWS.

Épicos

Configurar credenciais da AWS na sua máquina local

Tarefa	Descrição	Habilidades necessárias

Exporte variáveis para a conta e a região da AWS em que a pilha será implantada.	Para fornecer credencia is da AWS para o AWS CDK usando variáveis de ambiente, execute os seguintes comandos.
	`export CDK_DEFAU LT_ACCOUNT=<12 Digit AWS Account Number>`
	`export CDK_DEFAU LT_REGION=<region>`
		DevOps engenheiro, AWS DevOps

Configurar o perfil da AWS CLI.	Para configurar o perfil da AWS CLI para a conta, siga as instruções na documentação da AWS.	DevOps engenheiro, AWS DevOps

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clone o repositório na sua máquina local.	Para clonar o repositório, execute o comando a seguir no seu terminal. `git clone https://g ithub.com/awslabs/ genai-bedrock-chat bot.git`	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Configurar o ambiente virtual Python e instalar as dependências necessárias.	Para ativar o ambiente virtual do Python, execute os comandos a seguir.
	`cd genai-bedrock-chatbot`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Para configurar as dependências necessárias, execute o comando a seguir.
	`pip3 install -r requirements.txt`
		DevOps engenheiro, AWS DevOps

Configure o ambiente do AWS CDK e sintetize o código do AWS CDK.	1. Para configurar o ambiente do AWS CDK em sua conta da AWS, execute o comando a seguir. `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` 2. Para converter o código em uma configuração de CloudFormation pilha da AWS, execute o comando`cdk synth`.	DevOps engenheiro, AWS DevOps

Configure e implante o aplicativo de assistente baseado em bate-papo

Tarefa	Descrição	Habilidades necessárias
Provisione o acesso ao modelo Claude.	Para habilitar o acesso ao modelo Anthropic Claude para sua conta da AWS, siga as instruções na documentação do Amazon Bedrock.	AWS DevOps
Implante recursos na conta.	Para implantar recursos na conta da AWS usando o AWS CDK, faça o seguinte: 1. Na raiz do repositório clonado, no `cdk.json` arquivo, forneça entradas para os parâmetros. `logging` Os valores de exemplo são `INFO` `DEBUGWARN`,, `ERROR` e. Esses valores definem mensagens em nível de log para a função Lambda e o aplicativo Streamlit. 2. O `app.py` arquivo na raiz do repositório clonado contém o nome da CloudFormation pilha da AWS usado para implantaç ão. O nome padrão da pilha é `chatbot-stack` . 3. Para implantar recursos, execute o comando `cdk deploy`.	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	O `cdk deploy` comando usa construções L3 para criar várias funções do Lambda para copiar documentos e arquivos de conjuntos de dados CSV para buckets do S3. 4. Depois que o comando for concluído, faça login no AWS Management Console, abra o CloudFormation console e verifique se a pilha foi implantada com sucesso. Após a implantação bem-sucedida, você pode acessar o aplicativo assistente baseado em bate-papo usando a URL fornecida na seção CloudFormation Saídas.	

Tarefa	Descrição	Habilidades necessárias
Execute o AWS Glue Crawler e crie a tabela do Data Catalog.	Um AWS Glue Crawler é usado para manter o esquema de dados dinâmico. A solução cria e atualiza partições na tabela do AWS Glue Data Catalog executando o rastreador sob demanda. Depois que os arquivos do conjunto de dados CSV forem copiados para o bucket do S3, execute o crawler AWS Glue e crie o esquema da tabela do catálogo de dados para teste: 1. Navegue até o console do AWS Glue. 2. No painel de navegação , em Catálogo de dados, escolha Crawlers. 3. Selecione o rastreador com sufixo. `sagemaker-pricing-crawler` 4. Execute o crawler. 5. Depois que o crawler é executado com êxito, ele cria definições de tabela no Catálogo de Dados do AWS Glue. **Note** O código do AWS CDK configura o crawler AWS Glue	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	para ser executado sob demanda, mas você também pode programá-lo para ser executado periodica mente.	

Tarefa	Descrição	Habilidades necessárias
Inicie a indexação de documentos.	Depois que os arquivos forem copiados no bucket do S3, use o Amazon Kendra para rastreá-los e indexá-los: 1. Navegue até o console do Amazon Kendra. 2. Selecione o índice com o sufixo`chatbot-index` . 3. No painel de navegação, escolha Fontes de dados e selecione o conector da fonte de dados com o sufixo`chatbot-index` . 4. Escolha Sincronizar agora para iniciar o processo de indexação. **Note** O código do AWS CDK configura a sincronização do índice Amazon Kendra para ser executada sob demanda, mas você também pode executá-la periodicamente usando o parâmetro Schedule.	AWS DevOps, DevOps engenheiro

Limpe todos os recursos da AWS na solução

Tarefa	Descrição	Habilidades necessárias
Remova os recursos da AWS.	Depois de testar a solução, limpe os recursos: 1. Para remover os recursos da AWS implantados pela solução, execute o comando `cdk destroy`. 2. Exclua todos os objetos dos dois buckets do S3 e, em seguida, remova os buckets. Para obter mais informaçõ es, consulte Excluir um bucket.	DevOps engenheiro, AWS DevOps

Solução de problemas

Problema	Solução
O AWS CDK retorna erros.	Para obter ajuda com problemas do AWS CDK, consulte Solução de problemas comuns do AWS CDK.

Recursos relacionados

- Amazon Bedrock:
  - Acesso ao modelo
  - Parâmetros de inferência para modelos de fundação
- Criar funções do Lambda com Python
- Comece a usar o AWS CDK

- Trabalhando com o AWS CDK em Python
- Criador de aplicativos de IA generativa na AWS
- LangChain documentação
- Simplifique a documentação

Mais informações

Comandos do AWS CDK

Ao trabalhar com o AWS CDK, lembre-se dos seguintes comandos úteis:

- Lista todas as pilhas no aplicativo

```
cdk ls
```

- Emite o modelo sintetizado da AWS CloudFormation

```
cdk synth
```

- Implanta a pilha na sua conta e região padrão da AWS

```
cdk deploy
```

- Compara a pilha implantada com o estado atual

```
cdk diff
```

- Abre a documentação do AWS CDK

```
cdk docs
```

- Exclui a CloudFormation pilha e remove os recursos implantados da AWS

```
cdk destroy
```

Desenvolva um assistente baseado em bate-papo totalmente automatizado usando agentes e bases de conhecimento do Amazon Bedrock

Criado por Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS), Praveen Kumar Jeyarajan (AWS) e Shuai Cao (AWS)

Resumo

Muitas organizações enfrentam desafios ao criar um assistente baseado em bate-papo capaz de orquestrar diversas fontes de dados para oferecer respostas abrangentes. Esse padrão apresenta uma solução para o desenvolvimento de um assistente baseado em bate-papo capaz de responder consultas de documentação e bancos de dados, com uma implantação simples.

Começando com o Amazon Bedrock, esse serviço de inteligência artificial generativa (IA) totalmente gerenciado fornece uma ampla variedade de modelos básicos avançados (FMs). Isso facilita a criação eficiente de aplicativos generativos de IA com um forte foco em privacidade e segurança. No contexto da recuperação de documentação, a Geração Aumentada de Recuperação (RAG) é um recurso fundamental. Ele usa bases de conhecimento para aumentar as solicitações de FM com informações contextualmente relevantes de fontes externas. Um índice Amazon OpenSearch Serverless serve como banco de dados vetorial por trás das bases de conhecimento do Amazon Bedrock. Essa integração é aprimorada por meio de uma engenharia rápida e cuidadosa para minimizar imprecisões e garantir que as respostas estejam ancoradas na documentação factual. Para consultas de banco FMs de dados, o Amazon Bedrock transforma consultas textuais em consultas SQL estruturadas, incorporando parâmetros específicos. Isso permite a recuperação precisa de dados de bancos de dados gerenciados pelos bancos de dados AWS Glue. O Amazon Athena é usado para essas consultas.

Para lidar com consultas mais complexas, obter respostas abrangentes exige informações provenientes de documentação e bancos de dados. Agents for Amazon Bedrock é um recurso generativo de IA que ajuda você a criar agentes autônomos capazes de entender tarefas complexas e dividi-las em tarefas mais simples para orquestração. A combinação de insights recuperados das tarefas simplificadas, facilitada pelos agentes autônomos do Amazon Bedrock, aprimora a síntese das informações, levando a respostas mais completas e exaustivas. Esse padrão demonstra como criar um assistente baseado em bate-papo usando o Amazon Bedrock e os serviços e recursos de IA generativa relacionados em uma solução automatizada.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Docker, instalado
- Kit de Desenvolvimento da Nuvem AWS (AWS CDK), instalado e inicializado nas regiões da AWS `us-east-1` `us-west-2`
- AWS CDK Toolkit versão 2.114.1 ou posterior, instalado
- AWS Command Line Interface (AWS CLI), instalada e configurada
- Python versão 3.11 ou posterior, instalado
- No Amazon Bedrock, habilite o acesso a Claude 2, Claude 2.1, Claude Instant e Titan Embeddings G1 — Text

Limitações

- Essa solução é implantada em uma única conta da AWS.
- Essa solução pode ser implantada somente nas regiões da AWS nas quais o Amazon Bedrock e o Amazon OpenSearch Serverless são compatíveis. Para obter mais informações, consulte a documentação do Amazon Bedrock e do Amazon OpenSearch Serverless.

Versões do produto

- Índice LLAMA versão 0.10.6 ou posterior
- Sqlalchemy versão 2.0.23 ou posterior
- OpenSearch-py versão 2.4.2 ou posterior
- requests_aws4auth versão 1.2.3 ou posterior
- SDK da AWS para Python (Boto3) versão 1.34.57 ou posterior

Arquitetura

Pilha de tecnologias de destino

O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software de código aberto para definir a infraestrutura de nuvem em código e provisioná-la por meio da AWS.

CloudFormation A pilha de CDK da AWS usada nesse padrão implanta os seguintes recursos da AWS:

- AWS Key Management Service (AWS KMS)
- Amazon Simple Storage Service (Amazon S3)
- Catálogo de dados do AWS Glue, para o componente de banco de dados do AWS Glue
- AWS Lambda
- AWS Identity and Access Management (IAM)
- Amazon sem OpenSearch servidor
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- AWS Fargate
- Amazon Virtual Private Cloud (Amazon VPC)
- Application Load Balancer

Arquitetura de destino

O diagrama mostra uma configuração abrangente nativa da nuvem da AWS em uma única região da AWS, usando vários serviços da AWS. A interface principal do assistente baseado em bate-papo é um aplicativo Streamlit hospedado em um cluster Amazon ECS. Um Application Load Balancer gerencia a acessibilidade. As consultas feitas por meio dessa interface ativam a função `Invocation` Lambda, que então interage com os agentes do Amazon Bedrock. Esse agente responde às perguntas dos usuários consultando as bases de conhecimento do Amazon Bedrock ou invocando uma `Agent executor` função Lambda. Essa função aciona um conjunto de ações associadas ao agente, seguindo um esquema de API predefinido. As bases de conhecimento do Amazon Bedrock usam um índice OpenSearch Serverless como base de banco de dados vetorial. Além disso, a `Agent executor` função gera consultas SQL que são executadas no banco de dados AWS Glue por meio do Amazon Athena.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que permite analisar dados diretamente no Amazon Simple Storage Service (Amazon S3) usando SQL padrão.

- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir com os serviços da AWS por meio de comandos em seu shell de linha de comando.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade.
- O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados. Esse padrão usa um crawler do AWS Glue e uma tabela do Catálogo de Dados do AWS Glue.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon OpenSearch Serverless é uma configuração sem servidor sob demanda para o Amazon Service. OpenSearch Nesse padrão, um índice OpenSearch sem servidor serve como um banco de dados vetorial para as bases de conhecimento do Amazon Bedrock.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- Streamlit é uma estrutura Python de código aberto para criar aplicativos de dados.

Repositório de código

O código desse padrão está disponível no GitHub genai-bedrock-agent-chatbotrepositório. O repositório de código contém os seguintes arquivos e pastas:

- `assets`pasta — Os ativos estáticos, como o diagrama de arquitetura e o conjunto de dados público.
- `code/lambdas/action-lambda`pasta — O código Python para a função Lambda que atua como uma ação para o agente Amazon Bedrock.
- `code/lambdas/create-index-lambda`pasta — O código Python para a função Lambda que cria o índice Serverless. OpenSearch
- `code/lambdas/invoke-lambda`pasta — O código Python para a função Lambda que invoca o agente Amazon Bedrock, que é chamado diretamente do aplicativo Streamlit.
- `code/lambdas/update-lambda`pasta — O código Python para a função Lambda que atualiza ou exclui recursos depois que os recursos da AWS são implantados por meio do AWS CDK.
- `code/layers/boto3_layer`pasta — A pilha de CDK da AWS que cria uma camada de Boto3 que é compartilhada entre todas as funções do Lambda.
- `code/layers/opensearch_layer`pasta — A pilha de CDK da AWS que cria uma camada OpenSearch sem servidor que instala todas as dependências para criar o índice.
- `code/streamlit-app`pasta — O código Python que é executado como imagem de contêiner no Amazon ECS
- `code/code_stack.py`— O AWS CDK constrói arquivos Python que criam recursos da AWS.
- `app.py`— O AWS CDK empilha arquivos Python que implantam recursos da AWS na conta de destino da AWS.
- `requirements.txt`— A lista de todas as dependências do Python que devem ser instaladas para o AWS CDK.
- `cdk.json`— O arquivo de entrada para fornecer os valores necessários para criar recursos. Além disso, nos `context/config` campos, você pode personalizar a solução adequadamente. Para obter mais informações sobre personalização, consulte a seção Informações adicionais.

Práticas recomendadas

- O exemplo de código fornecido aqui é apenas para fins proof-of-concept (PoC) ou piloto. Se você quiser levar o código para produção, certifique-se de usar as seguintes práticas recomendadas:
  - Ativar o registro de acesso ao Amazon S3

  - Habilitar registros de fluxo de VPC
- Configure o monitoramento e os alertas para as funções do Lambda. Para obter mais informações, consulte Monitorar e solucionar problemas de funções do Lambda. Para obter as melhores práticas, consulte as melhores práticas para trabalhar com as funções do AWS Lambda.

Épicos

Configure as credenciais da AWS em sua estação de trabalho local

Tarefa	Descrição	Habilidades necessárias
Exporte variáveis para a conta e a região.	Para fornecer credencia is da AWS para o AWS CDK usando variáveis de ambiente, execute os seguintes comandos. `export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number> export CDK_DEFAU LT_REGION=<Region>`	AWS DevOps, DevOps engenheiro
Configure o perfil nomeado da AWS CLI.	Para configurar o perfil nomeado da AWS CLI para a conta, siga as instruções em Configuração e configurações do arquivo de credenciais.	AWS DevOps, DevOps engenheiro

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clone o repositório em sua estação de trabalho local.	Para clonar o repositório, execute o comando a seguir no seu terminal.	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/awslabs/genai-bedrock-agent-chatbot.git`	

Configure o ambiente virtual Python.	Para ativar o ambiente virtual do Python, execute os comandos a seguir.
	`cd genai-bedrock-agent-chatbot`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Para configurar as dependências necessárias, execute o comando a seguir.
	`pip3 install -r requirements.txt`
		DevOps engenheiro, AWS DevOps

Configure o ambiente do AWS CDK.	Para converter o código em um CloudFormation modelo da AWS, execute o comando`cdk synth`.	AWS DevOps, DevOps engenheiro

Configurar e implantar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Implante recursos na conta.	Para implantar recursos na conta da AWS usando o AWS CDK, faça o seguinte:	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	1. Na raiz do repositório clonado, no `cdk.json` arquivo, forneça entradas para os parâmetros de registro. Os valores de exemplo são `INFO` `DEBUGWARN`,, `ERROR` e. Esses valores definem mensagens em nível de log para as funções Lambda e o aplicativo Streamlit. 2. O `cdk.json` arquivo na raiz do repositório clonado contém o nome da CloudFormation pilha da AWS usado para implantação. O nome padrão da pilha é`chatbot-stack` . O nome padrão do agente Amazon Bedrock é`ChatbotBedrockAgent` , e o alias padrão do agente Amazon Bedrock é. `Chatbot_Agent` 3. Para implantar recursos, execute o comando `cdk deploy`. O `cdk deploy` comando usa construções de camada 3 para criar várias funções do Lambda para copiar documentos e arquivos de conjuntos de dados	

Tarefa	Descrição	Habilidades necessárias
	CSV para buckets do S3. Ele também implanta o agente Amazon Bedrock, as bases de conhecimento e a função `Action group` Lambda para o agente Amazon Bedrock. 4. Faça login no AWS Management Console e, em seguida, abra o CloudFormation console em https://console.aws.amazon.com/cloudformation/. 5. Confirme se a pilha foi implantada com sucesso. Para obter instruções, consulte Como revisar sua pilha no console da AWS CloudFormation . Após a implantação bem-sucedida, você pode acessar o aplicativo assistente baseado em bate-papo usando a URL fornecida na guia Saídas no console. CloudFormation	

Limpe todos os recursos da AWS na solução

Tarefa	Descrição	Habilidades necessárias
Remova os recursos da AWS.	Depois de testar a solução, para limpar os recursos, execute o comando`cdk destroy`.	AWS DevOps, DevOps engenheiro

Recursos relacionados

Documentação da AWS

- Recursos do Amazon Bedrock:
  - Acesso ao modelo
  - Parâmetros de inferência para modelos de fundação
  - Agentes do Amazon Bedrock
  - Bases de conhecimento do Amazon Bedrock
- Criar funções do Lambda com Python
- Recursos do AWS CDK:
  - Comece a usar o AWS CDK
  - Solução de problemas comuns do AWS CDK
  - Trabalhando com o AWS CDK em Python
- Criador de aplicativos de IA generativa na AWS

Outros recursos da AWS

- Mecanismo vetorial para Amazon OpenSearch Serverless

Outros recursos

- LlamaIndex documentação
- Simplifique a documentação

Mais informações

Personalize o assistente baseado em bate-papo com seus próprios dados

Para integrar seus dados personalizados para implantar a solução, siga estas diretrizes estruturadas. Essas etapas foram projetadas para garantir um processo de integração contínuo e eficiente, permitindo que você implante a solução de forma eficaz com seus dados personalizados.

Para integração de dados da base de conhecimento

Preparação de dados

1. Localize o `assets/knowledgebase_data_source/` diretório.
2. Coloque seu conjunto de dados nessa pasta.

Ajustes de configuração

1. Abra o arquivo `cdk.json`.
2. Navegue até o `context/configure/paths/knowledgebase_file_name` campo e, em seguida, atualize-o adequadamente.
3. Navegue até o `bedrock_instructions/knowledgebase_instruction` campo e atualize-o para refletir com precisão as nuances e o contexto do seu novo conjunto de dados.

Para integração de dados estruturais

Organização de dados

1. Dentro do `assets/data_query_data_source/` diretório, crie um subdiretório, como`tabular_data`.
2. Coloque seu conjunto de dados estruturado (formatos aceitáveis incluem CSV, JSON, ORC e Parquet) nessa subpasta recém-criada.
3. Se você estiver se conectando a um banco de dados existente, atualize a função `create_sql_engine()` `code/lambda/action-lambda/build_query_engine.py` para se conectar ao seu banco de dados.

Atualizações de configuração e código

1. No `cdk.json` arquivo, atualize o `context/configure/paths/athena_table_data_prefix` campo para alinhar com o novo caminho de dados.
2. Revise `code/lambda/action-lambda/dynamic_examples.csv` incorporando novos text-to-SQL exemplos que correspondam ao seu conjunto de dados.
3. Revise `code/lambda/action-lambda/prompt_templates.py` para espelhar os atributos do seu conjunto de dados estruturado.
4. No `cdk.json` arquivo, atualize o `context/configure/bedrock_instructions/action_group_description` campo para explicar a finalidade e a funcionalidade da função `Action group` Lambda.
5. No `assets/agent_api_schema/artifacts_schema.json` arquivo, explique as novas funcionalidades `Action group` da sua função Lambda.

Atualização geral

No `cdk.json` arquivo, na `context/configure/bedrock_instructions/agent_instruction` seção, forneça uma descrição abrangente da funcionalidade pretendida e da finalidade do design do agente Amazon Bedrock, levando em consideração os dados recém-integrados.

Documente o conhecimento institucional a partir de entradas de voz usando o Amazon Bedrock e o Amazon Transcribe

Criado por Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Megan Wu (AWS) e Rajiv Upadhyay (AWS)

Resumo

Capturar o conhecimento institucional é fundamental para garantir o sucesso e a resiliência organizacional. O conhecimento institucional representa a sabedoria coletiva, os insights e as experiências acumuladas pelos funcionários ao longo do tempo, geralmente de natureza tácita e transmitidos informalmente. Essa riqueza de informações engloba abordagens exclusivas, melhores práticas e soluções para problemas complexos que talvez não estejam documentados em outro lugar. Ao formalizar e documentar esse conhecimento, as empresas podem preservar a memória institucional, promover a inovação, aprimorar os processos de tomada de decisão e acelerar as curvas de aprendizado para novos funcionários. Além disso, promove a colaboração, capacita indivíduos e cultiva uma cultura de melhoria contínua. Em última análise, aproveitar o conhecimento institucional ajuda as empresas a usar seu ativo mais valioso — a inteligência coletiva de sua força de trabalho — para enfrentar desafios, impulsionar o crescimento e manter a vantagem competitiva em ambientes de negócios dinâmicos.

Esse padrão explica como capturar conhecimento institucional por meio de gravações de voz de funcionários seniores. Ele usa o Amazon Transcribe e o Amazon Bedrock para documentação e verificação sistemáticas. Ao documentar esse conhecimento informal, você pode preservá-lo e compartilhá-lo com grupos subsequentes de funcionários. Esse esforço apóia a excelência operacional e melhora a eficácia dos programas de treinamento por meio da incorporação de conhecimentos práticos adquiridos por meio da experiência direta.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Docker, instalado
- AWS Cloud Development Kit (AWS CDK) versão 2.114.1 ou posterior, instalado e inicializado nas regiões da AWS `us-east-1` `us-west-2`
- AWS CDK Toolkit versão 2.114.1 ou posterior, instalado

- AWS Command Line Interface (AWS CLI), instalada e configurada
- Python versão 3.12 ou posterior, instalado
- Permissões para criar recursos do Amazon Transcribe, Amazon Bedrock, Amazon Simple Storage Service (Amazon S3) e AWS Lambda

Limitações

- Essa solução é implantada em uma única conta da AWS.
- Essa solução pode ser implantada somente nas regiões da AWS onde o Amazon Bedrock e o Amazon Transcribe estão disponíveis. Para obter informações sobre disponibilidade, consulte a documentação do Amazon Bedrock e do Amazon Transcribe.
- Os arquivos de áudio devem estar em um formato compatível com o Amazon Transcribe. Para obter uma lista dos formatos compatíveis, consulte Formatos de mídia na documentação Transcreve.

Versões do produto

- SDK da AWS para Python (Boto3) versão 1.34.57 ou posterior
- LangChain versão 0.1.12 ou posterior

Arquitetura

A arquitetura representa um fluxo de trabalho sem servidor na AWS. O AWS Step Functions orquestra funções Lambda para processamento de áudio, análise de texto e geração de documentos. O diagrama a seguir mostra o fluxo de trabalho do Step Functions, também conhecido como máquina de estado.

Cada etapa na máquina de estado é gerenciada por uma função Lambda distinta. A seguir estão as etapas do processo de geração de documentos:

1. A função `preprocess` Lambda valida a entrada passada para o Step Functions e lista todos os arquivos de áudio presentes no caminho da pasta URI fornecida pelo Amazon S3. As funções downstream do Lambda no fluxo de trabalho usam a lista de arquivos para validar, resumir e gerar o documento.

2. A função `transcribe` Lambda usa o Amazon Transcribe para converter arquivos de áudio em transcrições de texto. Essa função Lambda é responsável por iniciar o processo de transcrição e transformar com precisão a fala em texto, que é então armazenado para processamento posterior.
3. A função `validate` Lambda analisa as transcrições do texto, determinando a relevância das respostas às perguntas iniciais. Ao usar um modelo de linguagem grande (LLM) por meio do Amazon Bedrock, ele identifica e separa as respostas sobre o tópico das respostas fora do tópico.
4. A função `summarize` Lambda usa o Amazon Bedrock para gerar um resumo coerente e conciso das respostas sobre o tópico.
5. A função `generate` Lambda reúne os resumos em um documento bem estruturado. Ele pode formatar o documento de acordo com modelos predefinidos e incluir qualquer conteúdo ou dados adicionais necessários.
6. Se alguma das funções do Lambda falhar, você receberá uma notificação por e-mail por meio do Amazon Simple Notification Service (Amazon SNS).

Durante todo esse processo, o AWS Step Functions garante que cada função Lambda seja iniciada na sequência correta. Essa máquina de estado tem a capacidade de processamento paralelo para aumentar a eficiência. Um bucket do Amazon S3 atua como o repositório de armazenamento central, dando suporte ao fluxo de trabalho gerenciando os vários formatos de mídia e documentos envolvidos.

Ferramentas

Serviços da AWS

- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

- O AWS Step Functions é um serviço de orquestração com tecnologia sem servidor que permite combinar funções do AWS Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios.
- O Amazon Transcribe é um serviço automático de reconhecimento de fala que usa modelos de aprendizado de máquina para converter áudio em texto.

Outras ferramentas

- LangChainé uma estrutura para o desenvolvimento de aplicativos que são alimentados por grandes modelos de linguagem (LLMs).

Repositório de código

O código desse padrão está disponível no GitHub genai-knowledge-capturerepositório.

O repositório de código contém os seguintes arquivos e pastas:

- `assets`pasta — Os ativos estáticos da solução, como o diagrama de arquitetura e o conjunto de dados público
- `code/lambdas`folder — O código Python para todas as funções do Lambda
  - `code/lambdas/generate`pasta - O código Python que gera um documento a partir dos dados resumidos no bucket do S3
  - `code/lambdas/preprocess`folder - O código Python que processa as entradas para a máquina de estado Step Functions
  - `code/lambdas/summarize`pasta - O código Python que resume os dados transcritos usando o serviço Amazon Bedrock
  - `code/lambdas/transcribe`pasta - O código Python que converte dados de fala (arquivo de áudio) em texto usando o Amazon Transcribe
  - `code/lambdas/validate`folder - O código Python que valida se todas as respostas pertencem ao mesmo tópico
- `code/code_stack.py`— O AWS CDK constrói um arquivo Python que é usado para criar recursos da AWS
- `app.py`— O arquivo Python do aplicativo AWS CDK usado para implantar recursos da AWS na conta de destino da AWS

- `requirements.txt`— A lista de todas as dependências do Python que devem ser instaladas para o AWS CDK
- `cdk.json`— O arquivo de entrada para fornecer os valores necessários para criar recursos

Práticas recomendadas

O exemplo de código fornecido é apenas para fins proof-of-concept (PoC) ou piloto. Se você quiser levar a solução para a produção, use as seguintes práticas recomendadas:

- Ativar o registro de acesso ao Amazon S3
- Habilitar registros de fluxo de VPC

Épicos

Configure as credenciais da AWS em sua estação de trabalho local

Tarefa	Descrição	Habilidades necessárias

Exporte variáveis para a conta e a região da AWS.	Para fornecer credencia is da AWS para o AWS CDK usando variáveis de ambiente, execute os seguintes comandos.
	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAU LT_REGION=<Region>`
		AWS DevOps, DevOps engenheiro

Configure o perfil nomeado da AWS CLI.	Para configurar o perfil nomeado da AWS CLI para a conta, siga as instruções em Configuração e configurações do arquivo de credenciais.	AWS DevOps, DevOps engenheiro

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clone o repositório em sua estação de trabalho local.	Para clonar o genai-knowledge-capturerepositório, execute o comando a seguir no seu terminal. `git clone https://github.com/aws-samples/genai-knowledge-capture`	AWS DevOps, DevOps engenheiro
(Opcional) Substitua os arquivos de áudio.	Para personalizar o aplicativo de amostra para incorporar seus próprios dados, faça o seguinte: 1. Navegue até a `assets/audio_samples` pasta no repositório clonado. 2. Exclua as pastas que contêm os arquivos de áudio de amostra. 3. Crie uma pasta para cada tópico que você deseja analisar. 4. Transfira seus arquivos de áudio para suas respectivas pastas.	AWS DevOps, DevOps engenheiro
Configure o ambiente virtual Python.	Para ativar o ambiente virtual do Python, execute os comandos a seguir.	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

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

Sintetize o código do AWS CDK.	Para converter o código em uma configuração de CloudFormation pilha da AWS, execute o comando a seguir. `cdk synth`	AWS DevOps, DevOps engenheiro

Configurar e implantar a solução

Tarefa	Descrição	Habilidades necessárias
Provisione o acesso ao modelo básico.	Habilite o acesso ao modelo Anthropic Claude 3 Sonnet para sua conta da AWS. Para obter instruções, consulte Adicionar acesso ao modelo na documentação do Bedrock.	AWS DevOps
Implante recursos na conta.	Para implantar recursos na conta da AWS usando o AWS CDK, faça o seguinte: 1. (Opcional) Na raiz do repositório clonado, no `app.py` arquivo, atualize o nome da CloudFormation	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	pilha da AWS. O nome padrão da pilha é `genai-knowledge-capture-stack` . 2. Para implantar recursos, execute o comando `cdk deploy`. O `cdk deploy` comando usa construções de camada 3 para criar um conjunto de funções Lambda, um bucket do S3, um tópico do Amazon SNS e uma máquina de estado Step Functions. Os arquivos de áudio na `assets/audio_samples` pasta são copiados para o bucket do S3 durante a implantação. 3. Faça login no AWS Management Console e, em seguida, abra o CloudFormation console em https://console.aws.amazon.com/cloudformation/. 4. Confirme se a pilha foi implantada com sucesso. Para obter instruções, consulte Como revisar sua pilha no console da AWS CloudFormation .	

Tarefa	Descrição	Habilidades necessárias
Assine o tópico do Amazon SNS.	Para assinar o tópico do Amazon SNS para receber notificações, faça o seguinte: 1. No CloudFormation console, no painel de navegação, escolha Pilhas. 2. Escolha a `genai-knowledge-capture-stack` pilha. 3. Escolha a guia Outputs. 4. Encontre o nome do tópico do Amazon SNS com a chave. `SNSTopicName` 5. Configure um endereço de e-mail para receber notificações seguindo as instruções em Inscrever um endereço de e-mail em um tópico do Amazon SNS.	AWS geral

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Execute uma máquina de estado.	1. Abra o console do Step Functions. 2. Na página State machines, escolha genai-knowledge-capture-stack-state-machine. 3. Selecione Iniciar execução.	Desenvolvedor de aplicativos, AWS geral

Tarefa	Descrição	Habilidades necessárias
	4. (Opcional) Na caixa Nome, insira um nome para a execução. 5. Na área Entrada, insira o seguinte objeto JSON substituindo o texto do espaço reservado, onde: • `<Name>` é o nome que você deseja dar ao documento. • `<S3 bucket name>` é o nome do bucket do Amazon S3 que contém os arquivos de áudio. • `<Folder path>` é o diretório que contém os arquivos de áudio. `{ "documentName": "<Name>", "audioFileFolderUri": "s3://<S3 bucket name>/<Folder path>" }` 6. Escolha Start Execution. 7. Na página de detalhes da execução, revise os resultados e aguarde a conclusão da execução.	

Limpe todos os recursos da AWS na solução

Tarefa	Descrição	Habilidades necessárias
Remova os recursos da AWS.	Depois de testar a solução, limpe os recursos: 1. Exclua todos os objetos do bucket do S3 e, em seguida, exclua o bucket. Para obter mais informaçõ es, consulte Excluir um bucket. 2. No repositório clonado, execute o comando. `cdk destroy`	AWS DevOps, DevOps engenheiro

Recursos relacionados

Documentação da AWS

- Recursos do Amazon Bedrock:
  - Acesso ao modelo
  - Parâmetros de inferência para modelos de fundação
- Recursos do AWS CDK:
  - Comece a usar o AWS CDK
  - Trabalhando com o AWS CDK em Python
  - Solução de problemas comuns do AWS CDK
  - Comandos do kit de ferramentas
- Recursos do AWS Step Functions:
  - Comece a usar o AWS Step Functions
  - Solução de problemas
- Criar funções do Lambda com Python
- Criador de aplicativos de IA generativa na AWS

Outros recursos

- LangChain documentação

Gere recomendações personalizadas e reclassificadas usando o Amazon Personalize

Criado por Mason Cahill (AWS), Matthew Chasse (AWS) e Tayo Olajide (AWS)

Resumo

Esse padrão mostra como usar o Amazon Personalize para gerar recomendações personalizadas para seus usuários, incluindo recomendações reclassificadas, com base na ingestão de dados de interação do usuário em tempo real desses usuários. O cenário de exemplo usado nesse padrão é baseado em um site de adoção de animais de estimação que gera recomendações para seus usuários com base em suas interações (por exemplo, quais animais de estimação visitados pelo usuário). Seguindo o cenário de exemplo, você aprende a usar o Amazon Kinesis Data Streams para ingerir dados de interação, o AWS Lambda para gerar recomendações e reclassificar as recomendações e o Amazon Data Firehose para armazenar os dados em um bucket do Amazon Simple Storage Service (Amazon S3). Você também aprende a usar o AWS Step Functions para criar uma máquina de estado que gerencia a versão da solução (ou seja, um modelo treinado) que gera suas recomendações.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa com um AWS Cloud Development Kit (AWS CDK) integrado
- AWS Command Line Interface (AWS CLI) com credenciais configuradas
- Python 3.9

Versões do produto

- Python 3.9
- CDK da AWS: 2.23.0 ou superior
- CLI da AWS: 2.7.27 ou superior

Arquitetura

Pilha de tecnologia

- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Personalize
- Amazon Simple Storage Service (Amazon S3)
- AWS Cloud Development Kit (AWS CDK)
- AWS Command Line Interface (AWS CLI)
- AWS Lambda
- AWS Step Functions

Arquitetura de destino

O diagrama a seguir ilustra um pipeline para a ingestão de dados em tempo real no Amazon Personalize. O pipeline então usa esses dados para gerar recomendações personalizadas e reclassificadas para os usuários.

O diagrama mostra o seguinte fluxo de trabalho:

1. O Kinesis Data Streams ingere dados do usuário em tempo real (por exemplo, eventos como animais de estimação visitados) para processamento pelo Lambda e pelo Firehose.
2. Uma função do Lambda processa os registros do Kinesis Data Streams e faz uma chamada de API para adicionar a interação do usuário no registro a um rastreador de eventos no Amazon Personalize.
3. Uma regra baseada em tempo invoca uma máquina de estado do Step Functions e gera novas versões da solução para os modelos de recomendação e reclassificação usando os eventos do rastreador de eventos no Amazon Personalize.
4. As campanhas do Amazon Personalize são atualizadas pela máquina de estado para usar a nova versão da solução.
5. O Lambda reclassifica a lista de itens recomendados chamando a campanha de reclassificação do Amazon Personalize.
6. O Lambda recupera a lista de itens recomendados chamando a campanha de recomendações do Amazon Personalize.
7. O Firehose salva os eventos em um bucket do S3, onde eles podem ser acessados como dados históricos.

Ferramentas

Ferramentas da AWS

- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O Amazon Data Firehose ajuda você a entregar dados de streaming em tempo real para outros serviços da AWS, endpoints HTTP personalizados e endpoints HTTP de propriedade de provedores de serviços terceirizados compatíveis.
- O Amazon Kinesis Data Streams ajuda a coletar e processar grandes fluxos de registros de dados em tempo real.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Personalize é um serviço de machine learning (ML) totalmente gerenciado que ajuda você a gerar recomendações de itens para seus usuários com base em seus dados.
- O AWS Step Functions é um serviço de orquestração sem servidor que permite combinar funções do Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios.

Outras ferramentas

- pytest é uma estrutura Python para escrever testes pequenos e legíveis.
- Python é uma linguagem de programação de computador de uso geral.

Código

O código desse padrão está disponível no repositório GitHub Animal Recommender. Você pode usar o CloudFormation modelo da AWS desse repositório para implantar os recursos para a solução de exemplo.

> **Note**
>
> As versões da solução Amazon Personalize, o rastreador de eventos e as campanhas são apoiadas por recursos personalizados (dentro da infraestrutura) que expandem os recursos nativos. CloudFormation

Épicos

Criar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Crie um ambiente Python isolado.	Configuração Mac/Linux 1. Para criar manualmente um ambiente virtual, execute o `$ python3 -m venv .venv` comando no seu terminal. 2. Depois que o processo de inicialização for concluído, execute o comando `$ source .venv/bin/activate` para ativar o ambiente virtual. Configuração do Windows Para criar manualmente um ambiente virtual, execute o `% .venv\Scripts\activate.bat` comando no seu terminal.	DevOps engenheiro
Sintetize o modelo. CloudFormation	1. Execute o comando `$ pip install -r requireme`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`nts.txt` do terminal para instalar as dependências necessárias. 2. No CLI da AWS, defina as seguintes variáveis de ambiente: • `export ACCOUNT_ID=123456789` • `export CDK_DEPLOY_REGION=us-east-1` • `export CDK_ENVIRONMENT=dev` 3. No arquivo `config/{env}.yml`, atualize `vpcId` para corresponder ao ID da nuvem privada virtual (VPC). 4. Para sintetizar o CloudFormation modelo para esse código, execute o `$ cdk synth` comando. **Note** Na etapa 2, `CDK_ENVIRONMENT` refere-se ao `config/{env}.yml` arquivo.	

Tarefa	Descrição	Habilidades necessárias
Implante recursos e crie infraestrutura.	Para implantar os recursos da solução, execute o comando `./deploy.sh` no seu terminal. Esse comando instala as dependências necessári as do Python. Um script do Python cria um bucket do S3 e uma chave do AWS Key Management Service (AWS KMS) e, em seguida, adiciona os dados iniciais para as criações iniciais do modelo. Por fim, o script `cdk deploy` é executado para criar a infraestrutura restante. **Note** O treinamento inicial do modelo acontece durante a criação da pilha. Poderá levar até duas horas para a pilha terminar de ser criada.	DevOps engenheiro

Recursos relacionados

- Recomendador de animais () GitHub
- Documentação de referência do CDK da AWS
- Documentação do Boto3

- Otimize recomendações personalizadas para uma métrica de negócios de sua escolha com o Amazon Personalize (AWS Machine Learning Blog)

Mais informações

Exemplos de cargas e respostas

Função do Lambda de recomendação

Para recuperar recomendações, envie uma solicitação para a função do Lambda de recomendação com uma carga no seguinte formato:

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

O exemplo de resposta a seguir contém uma lista de grupos de animais:

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

Se você omitir o campo `userId`, a função retornará recomendações gerais.

Reclassificar a função do Lambda

Para usar a reclassificação, envie uma solicitação para a função do Lambda de reclassificação. A carga contém todos os itens a IDs serem reclassificados e seus metadados. `userId` Os dados de exemplo a seguir usam as classes Oxford Pets para `animal_species_id` (1=gato, 2=cachorro) e números inteiros de 1 a 5 para `animal_age_id` e `animal_size_id`:

```
{
   "userId":"12345",
   "itemMetadataList":[
      {
         "itemId":"1",
```

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

A função Lambda reclassifica esses itens e, em seguida, retorna uma lista ordenada que inclui o item IDs e a resposta direta do Amazon Personalize. Esta é uma lista classificada dos grupos de animais em que os itens estão e sua pontuação. O Amazon Personalize usa receitas de Personalização do usuário e Classificação personalizada para incluir uma pontuação para cada item nas recomendações. Essas pontuações representam a certeza relativa que o Amazon Personalize tem em relação ao item que o usuário selecionará em seguida. As pontuações mais altas representam maior certeza.

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

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

Carga útil do Amazon Kinesis

A carga a ser enviada ao Amazon Kinesis tem o seguinte formato:

```
{
    "Partitionkey": "randomstring",
    "Data": {
        "userId": "12345",
        "sessionId": "sessionId4545454",
        "eventType": "DetailView",
        "animalMetadata": {
            "animal_species_id": "1",
            "animal_primary_breed_id": "Russian_Blue",
            "animal_size_id": "1",
            "animal_age_id": "2"
        },
        "animal_id": "98765"
```

```
    }
}
```

> **Note**
>
> O `userId` campo é removido para um usuário não autenticado.

Simplifique os fluxos de trabalho de aprendizado de máquina, do desenvolvimento local aos experimentos escaláveis, usando SageMaker IA e Hydra

Criado por David Sauerwein (AWS), Julian Ferdinand Grueber (AWS) e Marco Geiger (AWS)

Resumo

Esse padrão fornece uma abordagem unificada para configurar e executar algoritmos de aprendizado de máquina (ML), desde o teste local até a produção na Amazon SageMaker AI. Os algoritmos de ML são o foco desse padrão, mas sua abordagem se estende à engenharia de recursos, inferência e pipelines completos de ML. Esse padrão demonstra a transição do desenvolvimento de scripts locais para trabalhos de treinamento de SageMaker IA por meio de um exemplo de caso de uso.

Um fluxo de trabalho típico de ML é desenvolver e testar soluções em uma máquina local, executar experimentos em grande escala (por exemplo, com parâmetros diferentes) na nuvem e implantar a solução aprovada na nuvem. Em seguida, a solução implantada deve ser monitorada e mantida. Sem uma abordagem unificada para esse fluxo de trabalho, os desenvolvedores geralmente precisam refatorar seu código em cada estágio. Se a solução depender de um grande número de parâmetros que podem mudar em qualquer estágio desse fluxo de trabalho, pode se tornar cada vez mais difícil permanecer organizado e consistente.

Esse padrão aborda esses desafios. Primeiro, ele elimina a necessidade de refatoração de código entre ambientes, fornecendo um fluxo de trabalho unificado que permanece consistente, seja em execução em máquinas locais, em contêineres ou em IA. SageMaker Em segundo lugar, ele simplifica o gerenciamento de parâmetros por meio do sistema de configuração da Hydra, onde os parâmetros são definidos em arquivos de configuração separados que podem ser facilmente modificados e combinados, com registro automático da configuração de cada execução. Para obter mais detalhes sobre como esse padrão aborda esses desafios, consulte Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Uma função de usuário AWS Identity and Access Management (IAM) para implantar e iniciar os trabalhos de treinamento de SageMaker IA

- AWS Command Line Interface (AWS CLI) versão 2.0 ou posterior instalada e configurada
- Poesia versão 1.8 ou posterior, mas anterior à 2.0, instalada
- Docker instalado
- Python versão 3.10.x

Limitações

- Atualmente, o código visa apenas trabalhos de treinamento de SageMaker IA. Estendê-lo para trabalhos de processamento e pipelines completos de SageMaker IA é simples.
- Para uma configuração de SageMaker IA totalmente produtiva, detalhes adicionais precisam estar em vigor. Os exemplos podem ser chaves personalizadas AWS Key Management Service (AWS KMS) para computação e armazenamento ou configurações de rede. Você também pode configurar essas opções adicionais usando o Hydra em uma subpasta dedicada da `config` pasta.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra a arquitetura da solução.

O diagrama mostra o seguinte fluxo de trabalho:

1. O cientista de dados pode iterar o algoritmo em pequena escala em um ambiente local, ajustar parâmetros e testar o script de treinamento rapidamente sem a necessidade de Docker ou SageMaker IA. (Para obter mais detalhes, consulte a tarefa “Executar localmente para testes rápidos” no Epics.)
2. Quando estiver satisfeito com o algoritmo, o cientista de dados cria e envia a imagem do Docker para o repositório Amazon Elastic Container Registry (Amazon ECR) chamado. `hydra-sm-artifact` (Para obter mais detalhes, consulte “Executar fluxos de trabalho em SageMaker IA” em Epics.)
3. O cientista de dados inicia trabalhos de treinamento de SageMaker IA ou de otimização de hiperparâmetros (HPO) usando scripts Python. Para trabalhos de treinamento regulares, a configuração ajustada é gravada no bucket do Amazon Simple Storage Service (Amazon S3)

chamado. `hydra-sample-config` Para trabalhos de HPO, o conjunto de configurações padrão localizado na `config` pasta é aplicado.

4. O trabalho de treinamento de SageMaker IA extrai a imagem do Docker, lê os dados de entrada do `hydra-sample-data` bucket do Amazon S3 e busca a configuração do bucket do Amazon S3 ou usa a configuração padrãohydra-sample-config. Após o treinamento, o trabalho salva os dados de saída no bucket do Amazon S3. `hydra-sample-data`

Automação e escala

- Para treinamento, reciclagem ou inferência automatizados, você pode integrar o AWS CLI código a serviços como AWS LambdaAWS CodePipeline, ou Amazon. EventBridge
- O escalonamento pode ser obtido alterando as configurações para os tamanhos das instâncias ou adicionando configurações para treinamento distribuído.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando. Para esse padrão, o AWS CLI é útil tanto para configuração inicial de recursos quanto para testes.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon SageMaker AI é um serviço gerenciado de aprendizado de máquina (ML) que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção. SageMaker O treinamento de IA é um serviço de ML totalmente gerenciado dentro da SageMaker IA que permite o treinamento de modelos de ML em grande escala. A ferramenta pode lidar com as demandas computacionais de modelos de treinamento de forma eficiente, fazendo uso da escalabilidade integrada e da integração com outros. Serviços da AWS SageMaker O treinamento de IA também oferece suporte a algoritmos e contêineres personalizados, tornando-o flexível para uma ampla variedade de fluxos de trabalho de ML.

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres. Ele foi usado nesse padrão para garantir ambientes consistentes em vários estágios, do desenvolvimento à implantação, e para empacotar dependências e códigos de forma confiável. A conteinerização do Docker permitiu fácil escalabilidade e controle de versão em todo o fluxo de trabalho.
- O Hydra é uma ferramenta de gerenciamento de configuração que oferece flexibilidade para lidar com várias configurações e gerenciamento dinâmico de recursos. É fundamental para gerenciar as configurações do ambiente, permitindo uma implantação perfeita em diferentes ambientes. Para obter mais detalhes sobre Hydra, consulte Informações adicionais.
- Python é uma linguagem de programação de computador de uso geral. O Python foi usado para escrever o código ML e o fluxo de trabalho de implantação.
- Poetry é uma ferramenta para gerenciamento e empacotamento de dependências em Python.

Repositório de código

O código desse padrão está disponível no repositório GitHub configuring-sagemaker-training-jobs-with-hydra.

Práticas recomendadas

- Escolha uma função do IAM para implantar e iniciar os trabalhos de treinamento de SageMaker IA que siga o princípio do menor privilégio e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e nas melhores práticas de segurança na documentação do IAM.
- Use credenciais temporárias para acessar a função do IAM no terminal.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias

Crie e ative o ambiente virtual.	Para criar e ativar o ambiente virtual, execute os seguintes comandos na raiz do repositór io:
	`poetry install`
	`poetry shell`
		AWS geral

Implantar a infraestrutura.	Para implantar a infraestr utura usando CloudFormation, execute o seguinte comando: `aws cloudformation deploy --template-file infra/hydra-sagemaker-setup.yaml --stack-name hydra-sagemaker-setup --capabilities CAPABILITY_NAMED_IAM`	AWS geral, DevOps engenheir o
Baixe os dados da amostra.	Para baixar os dados de entrada do openml para sua máquina local, execute o seguinte comando: `python scripts/download_data.py`	AWS geral
Execute localmente para testes rápidos.	Para executar o código de treinamento localmente para	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	testes, execute o seguinte comando: `python mypackage/train.py data.train_data_path=data/train.csv evaluation.base_dir_path=data` Os registros de todas as execuções são armazenados por tempo de execução em uma pasta chamada`outputs`. Para obter mais informações, consulte a seção “Saída” no GitHub repositório. Você também pode realizar vários treinamentos em paralelo, com parâmetros diferentes, usando a `--multirun` funcionalidade. Para obter mais detalhes, consulte a documentação do Hydra.	

Execute fluxos de trabalho em IA SageMaker

Tarefa	Descrição	Habilidades necessárias
Defina as variáveis de ambiente.	Para executar seu trabalho na SageMaker IA, defina as seguintes variáveis de ambiente, fornecendo sua	AWS geral

Tarefa	Descrição	Habilidades necessárias

	Região da AWS e sua Conta da AWS ID:
	
	`export ECR_REPO_NAME=hydra-sm-artifact`
	`export image_tag=latest`
	`export AWS_REGION="<your_aws_region>" # for instance, us-east-1`
	`export ACCOUNT_ID="<your_account_id>"`
	`export BUCKET_NAME_DATA=hydra-sample-data-$ACCOUNT_ID`
	`export BUCKET_NAME_CONFIG=hydra-sample-config-$ACCOUNT_ID`
	`export AWS_DEFAULT_REGION=$AWS_REGION`
	`export ROLE_ARN=arn:aws:iam::${ACCOUNT_ID}:role/hydra-sample-sagemaker`
	`export INPUT_DATA_S3_PATH=s3://$BUCKET_NAME_DATA/hydra-on-sm/input/`
	`export OUTPUT_DATA_S3_PATH=s3://$BUCKET_NAME_DATA/hydra-on-sm/output/`	

Tarefa	Descrição	Habilidades necessárias

Crie e envie uma imagem do Docker.	Para criar a imagem do Docker e enviá-la para o repositório Amazon ECR, execute o seguinte comando:
	`chmod +x scripts/create_and_push_image.sh`
	`scripts/create_and_push_image.sh $ECR_REPO_NAME $image_tag $AWS_REGION $ACCOUNT_ID`
	Essa tarefa pressupõe que você tenha credenciais válidas em seu ambiente. A imagem do Docker é enviada para o repositório Amazon ECR especificado na variável de ambiente na tarefa anterior e é usada para ativar o contêiner de SageMaker IA no qual o trabalho de treinamento será executado.
		Engenheiro de ML, General AWS

Tarefa	Descrição	Habilidades necessárias
Copie os dados de entrada para o Amazon S3.	O trabalho de treinamento de SageMaker IA precisa coletar os dados de entrada. Para copiar os dados de entrada para o bucket do Amazon S3 para obter dados, execute o seguinte comando: `aws s3 cp data/train.csv "${INPUT_DATA_S3_PATH}train.csv"`	Engenheiro de dados, General AWS

Tarefa	Descrição	Habilidades necessárias
Envie vagas de treinamento em SageMaker IA.	Para simplificar a execução de seus scripts, especifique os parâmetros de configuração padrão no `default.yaml` arquivo. Além de garantir a consistência em todas as execuções, essa abordagem também oferece a flexibili dade de substituir facilment e as configurações padrão conforme necessário. Veja o exemplo a seguir: `python scripts/s tart_sagemaker_tra ining_job.py sagemaker .role_arn=$ROLE_AR N sagemaker.config_s 3_bucket=$BUCKET_N AME_CONFIG sagemaker .input_data_s3_path= $INPUT_DATA_S3_PATH sagemaker.output_d ata_s3_path=$OUTPU T_DATA_S3_PATH`	AWS geral, engenheiro de ML, cientista de dados

Tarefa	Descrição	Habilidades necessárias
Execute o ajuste de hiperparâ metros de SageMaker IA.	Executar o ajuste de hiperparâ metros de SageMaker IA é semelhante ao envio de um trabalho de treinamento de SageMaker AII. No entanto, o script de execução difere de algumas maneiras important es, como você pode ver no arquivo start_sagemaker_hp o_job.py. Os hiperparâmetros a serem ajustados devem ser passados pela carga útil do boto3, não por um canal para o trabalho de treinamento. Para iniciar o trabalho de otimização de hiperparâ metros (HPO), execute os seguintes comandos: `python scripts/s tart_sagemaker_hpo _job.py sagemaker .role_arn=$ROLE_AR N sagemaker.config_s 3_bucket=$BUCKET_N AME_CONFIG sagemaker .input_data_s3_path= $INPUT_DATA_S3_PATH sagemaker.output_d ata_s3_path=$OUTPU T_DATA_S3_PATH`	Cientista de dados

Solução de problemas

Problema	Solução
Token expirado	Exporte novas AWS credenciais.
Falta de permissões do IAM	Certifique-se de exportar as credenciais de uma função do IAM que tenha todas as permissões necessárias do IAM para implantar o CloudFormation modelo e iniciar os trabalhos de treinamento de SageMaker IA.

Recursos relacionados

- Treine um modelo com a Amazon SageMaker AI (AWS documentação)
- O que é ajuste de hiperparâmetros?

Mais informações

Esse padrão aborda os seguintes desafios:

Consistência do desenvolvimento local à implantação em grande escala — Com esse padrão, os desenvolvedores podem usar o mesmo fluxo de trabalho, independentemente de estarem usando scripts Python locais, executando contêineres Docker locais, conduzindo grandes experimentos SageMaker em IA ou implantando em produção em IA. SageMaker Essa consistência é importante pelos seguintes motivos:

- Iteração mais rápida — Permite uma experimentação local rápida sem a necessidade de grandes ajustes ao aumentar a escala.
- Sem refatoração — A transição para experimentos maiores em SageMaker IA é perfeita, não exigindo nenhuma revisão da configuração existente.
- Melhoria contínua — Desenvolver novos recursos e melhorar continuamente o algoritmo é simples porque o código permanece o mesmo em todos os ambientes.

Gerenciamento de configuração — Esse padrão usa o Hydra, uma ferramenta de gerenciamento de configuração, para fornecer os seguintes benefícios:

- Os parâmetros são definidos nos arquivos de configuração, separados do código.
- Diferentes conjuntos de parâmetros podem ser trocados ou combinados facilmente.
- O rastreamento de experimentos é simplificado porque a configuração de cada execução é registrada automaticamente.
- Os experimentos na nuvem podem usar a mesma estrutura de configuração das execuções locais, garantindo a consistência.

Com o Hydra, você pode gerenciar a configuração de forma eficaz, habilitando os seguintes recursos:

- Divida as configurações — divida as configurações do seu projeto em partes menores e gerenciáveis que podem ser modificadas de forma independente. Essa abordagem facilita o gerenciamento de projetos complexos.
- Ajuste os padrões com facilidade — altere suas configurações básicas rapidamente, facilitando o teste de novas ideias.
- Alinhe as entradas CLI e os arquivos de configuração — Combine as entradas da linha de comando com seus arquivos de configuração sem problemas. Essa abordagem reduz a desordem e a confusão, tornando seu projeto mais gerenciável ao longo do tempo.

Treine e implante um modelo de ML personalizado compatível com GPU na Amazon SageMaker

Criado por Ankur Shukla (AWS)

Resumo

Treinar e implantar um modelo de aprendizado de máquina (ML) compatível com unidade de processamento gráfico (GPU) requer uma configuração e inicialização iniciais de determinadas variáveis de ambiente para aproveitar totalmente os benefícios da NVIDIA. GPUs No entanto, pode ser demorado configurar o ambiente e torná-lo compatível com a SageMaker arquitetura da Amazon na nuvem da Amazon Web Services (AWS).

Esse padrão ajuda você a treinar e criar um modelo de ML personalizado compatível com GPU usando a Amazon. SageMaker Ele fornece etapas para treinar e implantar um CatBoost modelo personalizado construído em um conjunto de dados de avaliações de código aberto da Amazon. Em seguida, você pode comparar seu desempenho em uma instância do `p3.16xlarge` Amazon Elastic Compute Cloud EC2 (Amazon).

Esse padrão é útil se sua organização quiser implantar modelos de ML existentes compatíveis com GPU no. SageMaker Seus cientistas de dados podem seguir as etapas desse padrão para criar contêineres compatíveis com GPU NVIDIA e implantar modelos de ML nesses contêineres.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket de origem do Amazon Simple Storage Service (Amazon S3) para armazenar os artefatos e as previsões do modelo.
- Uma compreensão das instâncias de SageMaker notebooks e notebooks Jupyter.
- Uma compreensão de como criar uma função do AWS Identity and Access Management (IAM) com permissões básicas de SageMaker função, permissões de acesso e atualização do bucket S3 e permissões adicionais para o Amazon Elastic Container Registry (Amazon ECR).

Limitações

- Esse padrão é destinado a workloads de ML supervisionadas com código train-and-deploy no Python.

Arquitetura

Pilha de tecnologia

- SageMaker
- Amazon ECR

Ferramentas

Ferramentas

- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagem de contêiner, seguro, escalável e confiável.
- Amazon SageMaker — SageMaker é um serviço de ML totalmente gerenciado.
- Docker: o Docker é uma plataforma de software para criar, testar e implantar aplicativos rapidamente.
- Python: Python é uma linguagem de programação.

Código

O código desse padrão está disponível em GitHub Implementação de um modelo de classificação de revisão com Catboost e SageMaker repositório.

Épicos

Preparar os dados

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM e anexar as políticas necessári as.	Faça login no Console de Gerenciamento da AWS, abra o console do IAM e crie um	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	novo perfil do IAM. Anexe as políticas a seguir ao perfil do IAM: • `AmazonEC2ContainerRegistryFullAccess` • `AmazonS3FullAccess` • `AmazonSageMakerFullAccess` Para obter mais informações sobre isso, consulte Criar uma instância de notebook na SageMaker documentação da Amazon.	
Crie a instância do SageMaker notebook.	Abra o SageMaker console, escolha Instâncias do Notebook e, em seguida, escolha Criar instância do notebook. Em Perfil do IAM, selecione o perfil do IAM que você criou anteriormente. Configure a instância do bloco de anotações de acordo com seus requisitos e escolha Criar instância do bloco de anotações. Para etapas e instruções detalhadas, consulte Criar uma instância de notebook na SageMaker documentação da Amazon.	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Abra o terminal na instância do SageMaker notebook e clone a GitHub Implement ação de um modelo de classificação de revisão com Catboost e SageMaker repositório executando o seguinte comando: `git clone https://github.com/aws-samples/review-classification-using-catboost-sagemaker.git`	
Inicie o servidor de caderno Jupyter.	Inicie `Review classification model with Catboost and SageMaker.ipynb` do caderno Jupyter, que contém as etapas predefinidas.	Cientista de dados

Engenharia de atributos

Tarefa	Descrição	Habilidades necessárias
Execute comandos no caderno Jupyter.	Abra o caderno Jupyter e execute os comandos dos históricos a seguir para preparar os dados para treinar seu modelo de ML.	Cientista de dados
Ler os dados do bucket do S3.	`import pandas as pd` `import csv`	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	`fname = 's3://amazon-reviews-pds/tsv/amazon_reviews_us_Digital_Video_Download_v1_00.tsv.gz'` `df = pd.read_csv(fname, sep='\t',delimiter='\t',error_bad_lines=False)`	

Tarefa	Descrição	Habilidades necessárias

Pré-processar os dados.	`import numpy as np`
	`def pre_process(df):`
	
	`  df.fillna(value={'`
	`review_body': '',`
	`'review_headline':`
	`''}, inplace=True)`
	`df.fillna( value={'v`
	`erified_purchase':`
	`'Unk'}, inplace=True)`
	
	`df.fillna(0,`
	`inplace=True)`
	`return df`
	`df = pre_process(df)`
	`df.review_date =`
	`pd.to_datetime(df.`
	`review_date)`
	`df['target'] =`
	`np.where(df['star_`
	`rating']>=4,1,0)`
	
	Note
	Esse código substitui valores nulos no `'review_body'` por uma string vazia e substitui a `'verified_purchase'` coluna por `'Unk'`, o que significa “desconhecido”.
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias

Dividir os dados em conjuntos de dados de treinamento, validação e teste.	Para manter a distribuição da label de destino idêntica nos conjuntos divididos, você deve estratificar a amostragem usando a biblioteca scikit-learn.
	
	`from sklearn.model_selection import StratifiedShuffleSplit`
	`sss = StratifiedShuffleSplit(n_splits=2, test_size=0.10, random_state=0)`
	`sss.get_n_splits(df, df['target'])`
	`for train_index, test_index in sss.split(df, df['target']):`
	`  X_train_vallid , X_test = df.iloc[train_index], df.iloc[test_index]`
	
	`sss.get_n_splits(X_train_vallid, X_train_vallid['target'])`
	`for train_index, test_index in sss.split(X_train_vallid, X_train_vallid['target']):`
	`  X_train , X_valid = X_train_vallid.iloc[train_index],`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	`X_train_vallid.ilo c[test_index]`	

Criar, executar e enviar a imagem do Docker para o Amazon ECR

Tarefa	Descrição	Habilidades necessárias
Preparar e enviar para a imagem do Docker.	No caderno Jupyter, execute os comandos dos histórico s a seguir para preparar a imagem do Docker e enviá-la para o Amazon ECR.	Engenheiro de ML

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

Tarefa	Descrição	Habilidades necessárias

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

Criar uma imagem do Docker localmente.	`docker build -t "${algorithm_name}" . docker tag ${algorit hm_name} ${fullname}`	Engenheiro de ML
Executar a imagem do Docker e enviá-la para o Amazon ECR.	`docker push ${fullname}`	Engenheiro de ML

Treinamento

Tarefa	Descrição	Habilidades necessárias
Crie um trabalho de ajuste de SageMaker hiperparâmetros.	No notebook Jupyter, execute os comandos das histórias a seguir para criar um trabalho de ajuste de SageMaker hiperparâmetros usando sua imagem do Docker.	Cientista de dados
Crie um SageMaker estimador .	Crie um SageMaker estimador usando o nome da imagem do Docker. `import sagemaker as sage`	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	from time import gmtime, strftime sess = sage.Session() from sagemaker.tuner import IntegerParameter, CategoricalParameter, ContinuousParameter, HyperparameterTuner account = sess.boto_session.client('sts').get_caller_identity()['Account'] region = sess.boto_session.region_name image = '{}.dkr.ecr.{}.amazonaws.com/sagemaker-catboost-github-gpu-img:latest'.format(account, region) tree_hpo = sage.estimator.Estimator(image, role, 1, 'ml.p3.16xlarge', train_volume_size = 100, output_path="s3://{}/sagemaker/DEMO-GPU-Catboost/output".format(bucket), sagemaker_session=sess)	

Tarefa	Descrição	Habilidades necessárias

Criar um trabalho do HPO.	Crie um trabalho de ajuste de otimização de hiperparâmetros (HPO) com intervalos de parâmetros e transmita os conjuntos de treinamento e validação como parâmetros para a função.
	
	`hyperparameter_ranges = {'iterations': IntegerParameter(80000, 130000),`
	
	`'max_depth': IntegerParameter(6, 10),`
	
	`'max_ctr_complexity': IntegerParameter(4, 10),`
	
	`'learning_rate': ContinuousParameter(0.01, 0.5)}`
	
	`objective_metric_name = 'auc'`
	`metric_definitions = [{'Name': 'auc',`
	
	`'Regex': 'auc: ([0-9\.]+)'}]`
	
	`tuner = HyperparameterTuner(tree_hpo,`
	
	`objective_metric_name,`
	
	`hyperparameter_ranges,`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias

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

Executar o trabalho do HPO.	`train_location = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/train/'`
	`valid_location = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/valid/'`
	
	`tuner.fit({'train': train_location, 'validation': valid_location})`
		Cientista de dados

Receber o trabalho de treinamento com melhor desempenho.	`import sagemaker as sage`
	`from time import gmtime, strftime`
	`sess = sage.Session()`
	
	`best_job =tuner.best_training_job()`
		Cientista de dados

Transformar em lote

Tarefa	Descrição	Habilidades necessárias
Crie um trabalho SageMaker de transformação em lote nos dados de teste para previsão do modelo.	No notebook Jupyter, execute os comandos das histórias a seguir para criar o modelo a partir do seu trabalho de ajuste de SageMaker hiperparâmetros e enviar um trabalho de transformação em SageMaker lote nos dados de teste para previsão do modelo.	Cientista de dados

Crie o SageMaker modelo.	Crie um modelo em SageMaker modelo usando o melhor trabalho de treinamento.
	`attached_estimator = sage.estimator.Estimator.attach(best_job)`
	`output_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test-predictions/'`
	`input_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test/'`
	`transformer = attached_estimator.transformer(instance_count=1,`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	`instance_type='ml.p3.16xlarge', assemble_with='Line', accept='text/csv', max_payload=1, output_path=output_path, env = {'SAGEMAKER_MODEL_SERVER_TIMEOUT' : '3600' })`	
Criar trabalho de transformação em lote.	Crie um trabalho de transformação em lote no conjunto de dados de teste. `transformer.transform(input_path, content_type='text/csv', split_type='Line')`	Cientista de dados

Analisar os resultados

Tarefa	Descrição	Habilidades necessárias
Leia os resultados e avalie o desempenho do modelo.	No caderno Jupyter, execute os comandos dos históricos a seguir para ler os resultados e avaliar o desempenho do modelo nas métricas do modelo Área abaixo da curva ROC (ROC-AUC) e Área abaixo da curva de recuperação de precisão (PR-AUC). Para obter mais informações , consulte os Principais conceitos do Amazon Machine Learning na documentação do Amazon Machine Learning (Amazon ML).	Cientista de dados

Leia os resultados do trabalho de transformação em lote.	Leia o lote e transforme os resultados do trabalho em um quadro de dados.
	
	`file_name = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test-predictions/file_1.out'`
	
	`results = pd.read_csv(file_name, names=['review_id','target','score'] ,sep='\t',escapechar ='\\' , quoting=csv.QUOTE_NONE,`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	`lineterminator='\n',quotechar='"').dropna()`	

Tarefa	Descrição	Habilidades necessárias

Avaliar as métricas de performance.	Avalie o desempenho do modelo no ROC-AUC e no PR-AUC.
	
	`from sklearn import metrics`
	`import matplotlib`
	`import pandas as pd`
	`matplotlib.use('agg', warn=False, force=True)`
	`from matplotlib import pyplot as plt`
	
	`%matplotlib inline`
	
	`def analyze_results(labels, predictions):`
	`precision, recall, thresholds = metrics.precision_recall_curve(labels, predictions)`
	`auc = metrics.auc(recall, precision)`
	
	`fpr, tpr, _ = metrics.roc_curve(labels, predictions)`
	`roc_auc_score = metrics.roc_auc_score(labels, predictions)`
	
	`print('Neural-Nets: ROC auc=%.3f' % ( roc_auc_score))`
	
	`plt.plot(fpr, tpr, label="data 1, auc=" + str(roc_auc_score))`
		Cientista de dados

Tarefa	Descrição	Habilidades necessárias

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

Tarefa	Descrição	Habilidades necessárias

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

Recursos relacionados

- Treine e hospede modelos Scikit-Learn na Amazon SageMaker criando um contêiner Scikit Docker

Mais informações

A lista a seguir mostra os diferentes elementos do Dockerfile que são executados no épico Criar, executar e enviar a imagem do Docker para o Amazon ECR.

Instale o Python com aws-cli.

```
FROM amazonlinux:1

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

Instale os pacotes do Python

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

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

Instale CUDA e CuDNN

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

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

Crie a estrutura de diretórios necessária para SageMaker

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

Defina as variáveis de ambiente NVIDIA

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

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

Copie arquivos de treinamento e inferência na imagem do Docker

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

Traduza a linguagem natural em consultas DSL para consultas OpenSearch e Elasticsearch

Criado por Tabby Ward (AWS), Nicholas Switzer (AWS) e Breanne Warner (AWS)

Resumo

Esse padrão demonstra como usar modelos de linguagem grande (LLMs) para converter consultas de linguagem natural em linguagem específica de domínio de consulta (consulta DSL), o que facilita a interação dos usuários com serviços de pesquisa, como OpenSearch o Elasticsearch, sem amplo conhecimento da linguagem de consulta. Esse recurso é particularmente valioso para desenvolvedores e cientistas de dados que desejam aprimorar aplicativos baseados em pesquisa com recursos de consulta em linguagem natural, melhorando a experiência do usuário e a funcionalidade de pesquisa.

O padrão ilustra técnicas de engenharia rápida, refinamento iterativo e incorporação de conhecimento especializado, todas cruciais na geração de dados sintéticos. Embora essa abordagem se concentre principalmente na conversão de consultas, ela demonstra implicitamente o potencial de aumento de dados e produção escalável de dados sintéticos. Essa base pode ser estendida para tarefas mais abrangentes de geração de dados sintéticos, para destacar o poder de unir entradas de LLMs linguagem natural não estruturadas com saídas estruturadas e específicas do aplicativo.

Essa solução não envolve ferramentas de migração ou implantação no sentido tradicional. Em vez disso, ele se concentra em demonstrar uma prova de conceito (PoC) para converter consultas de linguagem natural em consultas DSL usando. LLMs

- O padrão usa um notebook Jupyter como step-by-step guia para configurar o ambiente e implementar a text-to-query conversão.
- Ele usa o Amazon Bedrock para acessar LLMs, que são cruciais para interpretar a linguagem natural e gerar consultas apropriadas.
- A solução foi projetada para funcionar com o Amazon OpenSearch Service. Você pode seguir um processo semelhante para o Elasticsearch, e as consultas geradas poderiam ser adaptadas para mecanismos de pesquisa semelhantes.

O Query DSL é uma linguagem de pesquisa flexível, baseada em JSON, usada para criar consultas complexas tanto no Elasticsearch quanto no. OpenSearch Ele permite que você especifique

consultas no parâmetro de consulta das operações de pesquisa e oferece suporte a vários tipos de consulta. Uma consulta DSL inclui consultas de folha e consultas compostas. As consultas Leaf pesquisam valores específicos em determinados campos e abrangem consultas de texto completo, em nível de termo, geográficas, de junção, abrangência e especializadas. As consultas compostas atuam como invólucros para várias cláusulas de folha ou compostas e combinam seus resultados ou modificam seu comportamento. O Query DSL suporta a criação de pesquisas sofisticadas, desde consultas simples que combinam tudo até consultas complexas com várias cláusulas que produzem resultados altamente específicos. O Query DSL é particularmente valioso para projetos que exigem recursos avançados de pesquisa, construção flexível de consultas e estruturas de consulta baseadas em JSON.

Esse padrão usa técnicas como solicitação de poucas fotos, solicitações do sistema, saída estruturada, encadeamento de solicitações, provisão de contexto e solicitações específicas de tarefas para conversão de DSL. text-to-query Para obter definições e exemplos dessas técnicas, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

Para usar efetivamente o notebook Jupyter para converter consultas de linguagem natural em consultas DSL, você precisa:

- Familiaridade com os notebooks Jupyter. Compreensão básica de como navegar e executar código em um ambiente de notebook Jupyter.
- Ambiente Python. Um ambiente Python funcional, preferencialmente Python 3.x, com as bibliotecas necessárias instaladas.
- Elasticsearch ou OpenSearch conhecimento. Conhecimento básico do Elasticsearch or OpenSearch, incluindo sua arquitetura e como realizar consultas.
- Conta da AWS. Um ativo Conta da AWS para acessar o Amazon Bedrock e outros serviços relacionados.
- Bibliotecas e dependências. Instalação de bibliotecas específicas mencionadas no notebook, como `boto3` para AWS interação e quaisquer outras dependências necessárias para a integração do LLM.
- Acesso ao modelo no Amazon Bedrock. Esse padrão usa três Claude LLMs da Anthropic. Abra o console Amazon Bedrock e escolha Model access. Na próxima tela, escolha Ativar modelos específicos e selecione estes três modelos:

  - Soneto de Claude 3
  - Soneto de Claude 3.5
  - Claude 3 Haicai
- Políticas adequadas do IAM e função do IAM. Para executar o notebook em um Conta da AWS, sua função AWS Identity and Access Management (IAM) requer a `SagemakerFullAccess` política, bem como a política fornecida na seção Informações adicionais, que você pode nomear`APGtext2querydslpolicy`. Essa política inclui a assinatura dos três modelos Claude listados.

Ter esses pré-requisitos estabelecidos garante uma experiência tranquila ao trabalhar com o notebook e implementar a funcionalidade. text-to-query

Limitações

- Status da prova de conceito. Este projeto foi concebido principalmente como uma prova de conceito (PoC). Ele demonstra o potencial do uso LLMs para converter consultas de linguagem natural em DSL de consulta, mas pode não estar totalmente otimizado ou pronto para produção.
- Limitações do modelo:

  Restrições da janela de contexto. Ao usar os LLMs que estão disponíveis no Amazon Bedrock, esteja ciente das limitações da janela de contexto:

  Modelos Claude (em setembro de 2024):

  - Claude 3 Opus: 200.000 fichas
  - Soneto de Claude 3:200.000 fichas
  - Claude 3 Haiku: 200.000 fichas

  Outros modelos no Amazon Bedrock podem ter tamanhos de janela de contexto diferentes. Sempre verifique a documentação mais recente para obter as informações mais recentes.

  Disponibilidade do modelo.A disponibilidade de modelos específicos no Amazon Bedrock pode variar. Certifique-se de ter acesso aos modelos necessários antes de implementar essa solução.
- Limitações adicionais
  - Complexidade da consulta. A eficácia da linguagem natural para consultar a conversão DSL pode variar dependendo da complexidade da consulta de entrada.

- Compatibilidade de versões. A consulta DSL gerada pode precisar de ajustes com base na versão específica do Elasticsearch ou na OpenSearch que você usa.
- Desempenho. Esse padrão fornece uma implementação de PoC, portanto, a velocidade e a precisão da geração de consultas podem não ser ideais para uso em produção em grande escala.
- Custos. O uso LLMs no Amazon Bedrock gera custos. Esteja ciente da estrutura de preços do modelo escolhido. Para obter mais informações, consulte Preços do Amazon Bedrock.
- Manutenção. Atualizações regulares nos prompts e na seleção do modelo podem ser necessárias para acompanhar os avanços na tecnologia LLM e as mudanças na sintaxe DSL de consulta.

Versões do produto

Essa solução foi testada no Amazon OpenSearch Service. Se você quiser usar o Elasticsearch, talvez seja necessário fazer algumas alterações para replicar a funcionalidade exata desse padrão.

- OpenSearch compatibilidade de versões. OpenSearch mantém a compatibilidade com versões anteriores nas versões principais. Por exemplo:
  - OpenSearch Os clientes 1.x geralmente são compatíveis com clusters OpenSearch 1.x.
  - OpenSearch Os clientes 2.x geralmente são compatíveis com clusters OpenSearch 2.x.

  No entanto, é sempre melhor usar a mesma versão secundária para o cliente e o cluster, sempre que possível.
- OpenSearch Compatibilidade com a API. OpenSearch mantém a compatibilidade da API com o Elasticsearch OSS 7.10.2 para a maioria das operações. No entanto, existem algumas diferenças, especialmente nas versões mais recentes.
- OpenSearch considerações de atualização:
  - Não há suporte para downgrades diretos. Use instantâneos para reversão, se necessário.
  - Ao fazer o upgrade, verifique a matriz de compatibilidade e as notas de versão para ver se há alterações significativas.

Considerações sobre o Elasticsearch

- Versão Elasticsearch. A versão principal do Elasticsearch que você está usando é crucial, pois a sintaxe e os recursos da consulta podem mudar entre as versões principais. Atualmente, a versão

estável mais recente é o Elasticsearch 8.x. Certifique-se de que suas consultas sejam compatíveis com sua versão específica do Elasticsearch.

- Versão da biblioteca DSL de consulta do Elasticsearch. Se você estiver usando a biblioteca de consultas DSL Python do Elasticsearch, certifique-se de que sua versão corresponda à sua versão do Elasticsearch. Por exemplo:
  - Para o Elasticsearch 8.x, use uma `elasticsearch-dsl` versão maior ou igual à 8.0.0, mas menor que a 9.0.0.
  - Para o Elasticsearch 7.x, use uma `elasticsearch-dsl` versão maior ou igual à 7.0.0, mas menor que a 8.0.0.
- Versão da biblioteca cliente. Se você estiver usando o cliente oficial do Elasticsearch ou um cliente específico do idioma, certifique-se de que ele seja compatível com sua versão do Elasticsearch.
- Consulte a versão DSL. O Query DSL evolui com as versões do Elasticsearch. Alguns tipos ou parâmetros de consulta podem estar obsoletos ou introduzidos em versões diferentes.
- Versão de mapeamento. A maneira como você define mapeamentos para seus índices e muda entre as versões. Sempre verifique a documentação de mapeamento para sua versão específica do Elasticsearch.
- Versões de ferramentas de análise. Se você estiver usando analisadores, tokenizadores ou outras ferramentas de análise de texto, o comportamento ou a disponibilidade deles podem mudar entre as versões.

Arquitetura

Arquitetura de destino

O diagrama a seguir ilustra a arquitetura desse padrão.

em que:

1. Entrada do usuário e solicitação do sistema com alguns exemplos de solicitação. O processo começa com um usuário que fornece uma consulta de linguagem natural ou uma solicitação para geração de esquema.
2. Amazon Bedrock. A entrada é enviada para o Amazon Bedrock, que serve como interface para acessar o Claude LLM.
3. Claude 3 Sonnet LLM. O Amazon Bedrock usa o Claude 3 Sonnet da família Claude 3 para processar LLMs a entrada. Ele interpreta e gera o Elasticsearch ou OpenSearch DSL de consulta

apropriado. Para solicitações de esquema, ele gera mapeamentos ou Elasticsearch sintéticos. OpenSearch

4. Geração de consultas DSL. Para consultas em linguagem natural, o aplicativo pega a saída do LLM e a formata em uma DSL de consulta válida do Elasticsearch ou OpenSearch Service.
5. Geração de dados sintéticos. O aplicativo também usa esquemas para criar Elasticsearch sintético ou OpenSearch dados para serem carregados em uma coleção sem OpenSearch servidor para testes.
6. OpenSearch ou Elasticsearch. A consulta DSL gerada é consultada em relação a uma coleção OpenSearch Serverless em todos os índices. A saída JSON contém os dados relevantes e o número de ocorrências dos dados que residem na coleção OpenSearch Serverless.

Automação e escala

O código fornecido com esse padrão é criado estritamente para fins de PoC. A lista a seguir fornece algumas sugestões para automatizar e escalar ainda mais a solução e mover o código para a produção. Esses aprimoramentos estão fora do escopo desse padrão.

- Containerização:
  - Dockerize o aplicativo para garantir a consistência em diferentes ambientes.
  - Use plataformas de orquestração de contêineres, como Amazon Elastic Container Service (Amazon ECS) ou Kubernetes, para implantações escaláveis.
- Arquitetura sem servidor:
  - Converta a funcionalidade principal em AWS Lambda funções.
  - Use o Amazon API Gateway para criar RESTful endpoints para a entrada da consulta em linguagem natural.
- Processamento assíncrono:
  - Implemente o Amazon Simple Queue Service (Amazon SQS) para enfileirar as consultas recebidas.
  - Use AWS Step Functions para orquestrar o fluxo de trabalho de processamento de consultas e geração de consultas DSL.
- Armazenamento em cache:
  - Implemente um mecanismo para armazenar os prompts em cache.
- Monitoramento e registro:
  - Use a Amazon CloudWatch para monitoramento e alertas.

  - Implemente o registro centralizado com o Amazon CloudWatch Logs ou o Amazon OpenSearch Service para análise de registros.
- Aprimoramentos de segurança:
  - Implemente funções do IAM para um controle de acesso refinado.
  - Use AWS Secrets Manager para armazenar e gerenciar com segurança as chaves e credenciais da API.
- Implantação em várias regiões:
  - Considere implantar a solução em vários Regiões da AWS para melhorar a latência e a recuperação de desastres.
  - Use o Amazon Route 53 para roteamento inteligente de solicitações.

Ao implementar essas sugestões, você pode transformar essa PoC em uma solução robusta, escalável e pronta para produção. Recomendamos que você teste minuciosamente cada componente e todo o sistema antes da implantação completa.

Ferramentas

Ferramentas

- Os notebooks Amazon SageMaker AI são notebooks Jupyter totalmente gerenciados para desenvolvimento de aprendizado de máquina. Esse padrão usa notebooks como um ambiente interativo para exploração de dados, desenvolvimento de modelos e experimentação na Amazon SageMaker AI. Os notebooks oferecem integração perfeita com outros recursos de SageMaker IA e. Serviços da AWS
- Python é uma linguagem de programação de computador de uso geral. Esse padrão usa o Python como a linguagem principal para implementar a solução.
- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada. O Amazon Bedrock fornece acesso ao processamento LLMs de linguagem natural. Esse padrão usa modelos Anthropic Claude 3.
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script em Python, incluindo o Amazon Serviços da AWS Bedrock.
- O Amazon OpenSearch Service é um serviço gerenciado que ajuda você a implantar, operar e escalar clusters de OpenSearch serviços na nuvem da AWS. Esse padrão usa o OpenSearch Service como o sistema de destino para gerar a consulta DSL.

Repositório de código

O código desse padrão está disponível no repositório GitHub Prompt Engineering Text-to-QueryDSL Using Claude 3 Models. O exemplo usa um aplicativo de mídia social de saúde que cria publicações para usuários e perfis de usuário associados ao aplicativo de saúde.

Práticas recomendadas

Ao trabalhar com essa solução, considere o seguinte:

- A necessidade de AWS credenciais e permissões adequadas para acessar o Amazon Bedrock
- Custos potenciais associados ao uso Serviços da AWS e LLMs
- A importância de entender a consulta DSL para validar e potencialmente modificar as consultas geradas

Épicos

Configure o ambiente e prepare os dados

Tarefa	Descrição	Habilidades necessárias
Configure o ambiente de desenvolvimento.	**Note** Para obter instruções e códigos detalhados para essa e outras etapas desse padrão, consulte o passo a passo abrangente no GitHub repositório. 1. Instale os pacotes Python necessários, incluindo**boto3**,, **numpy** **awscliopensearch-py** ,	Python, pip, SDK da AWS

Tarefa	Descrição	Habilidades necessárias
	e **`requests-aws4auth`** usando pip. 2. Importe os módulos necessários `boto3json`, comoos,`opensearchpy` ,, `opensearchRequestsHttpConnection` bulk `deOpensearchpy` ,`opensearchpy.helpers` ,`sagemaker` ,`time`, `randomre`, e `AWS4Auth` de`requests_aws4auth` .	
Configure o AWS acesso.	Configure o cliente Amazon Bedrock e a sessão de SageMaker IA. Recupere o Amazon Resource Name (ARN) para SageMaker a função de execução de IA para uso posterior na criação OpenSearch da coleção Serverless.	IAM, AWS CLI, Amazon Bedrock, Amazon SageMaker
Carregue esquemas de aplicativos de saúde.	Leia e analise esquemas JSON para publicações de saúde e perfis de usuário a partir de arquivos predefinidos. Converta esquemas em strings para uso posterior em prompts.	DevOps engenheiro, AWS geral, Python, JSON

Gere dados sintéticos

Tarefa	Descrição	Habilidades necessárias

Crie um gerador de dados baseado em LLM.	Implemente a função generate_data () para chamar a API Amazon Bedrock Converse com modelos Claude 3. Configure o modelo IDs para Sonnet, Sonnet 3.5 e Haiku:
	`model_id_sonnet3_5 = "anthropic.claude-3-5-sonnet-20240620-v1:0"`
	`model_id_sonnet = "anthropic.claude-3-sonnet-20240229-v1:0"`
	`model_id_haiku = "anthropic.claude-3-haiku-20240307-v1:0"`
		Python, API Amazon Bedrock, solicitação de LLM

Crie postos de saúde sintéticos.	Use a função generate_data () com um prompt de mensagem específico para criar entradas sintéticas de postagem de saúde com base no esquema fornecido. A chamada da função tem a seguinte aparência: `health_post_data = generate_data(bedrock_rt, model_id_sonnet, system_prompt, message_healthpost, inference_config)`	Python, JSON

Tarefa	Descrição	Habilidades necessárias
Crie perfis de usuário sintéticos.	Use a função generate_data () com um prompt de mensagem específico para criar entradas sintéticas de perfil de usuário com base no esquema fornecido. Isso é semelhante à geração de postos de saúde, mas usa um prompt diferente.	Python, JSON

Configurar OpenSearch e ingerir dados

Tarefa	Descrição	Habilidades necessárias
Configure uma coleção OpenSearch sem servidor.	Use o Boto3 para criar uma coleção OpenSearch sem servidor com políticas apropriadas de criptografia, rede e acesso. A criação da coleção é assim: `collection = aoss_client.create_collection(name=es_name, type='SEARCH')` Para obter mais informações sobre o OpenSearch Serverless, consulte a AWS documentação.	OpenSearch Sem servidor, IAM
Defina OpenSearch índices.	Crie índices para postos de saúde e perfis de usuário usando o OpenSearch cliente, com base nos mapeament	OpenSearch, JSON

Tarefa	Descrição	Habilidades necessárias
	os de esquema predefinidos. A criação do índice tem a seguinte aparência: `response_health = oss_client.indices.create(healthpost_index, body=healthpost_body)`	
Carregue dados em OpenSearch.	Execute a função ingest_data () para inserir em massa as publicações de saúde sintéticas e os perfis de usuário em seus respectivos índices. OpenSearch A função usa o auxiliar em massa deopensearch-py : `success, failed = bulk(oss_client, actions)`	Python, OpenSearch API, operações de dados em massa

Gere e execute consultas

Tarefa	Descrição	Habilidades necessárias
Crie alguns exemplos de avisos rápidos.	Gere exemplos de consultas e perguntas de linguagem natural correspondentes usando modelos Claude 3 para servir como exemplos simples para geração de consultas. O prompt do sistema inclui estes exemplos:	Solicitação LLM, consulta DSL

Tarefa	Descrição	Habilidades necessárias
	`system_prompt_query_generation = [{"text": f"""You are an expert query dsl generator. ... Examples: {example_prompt} ..."""}]`	
Crie um conversor text-to-query DSL.	Implemente o prompt do sistema, que inclui esquemas, dados e alguns exemplos, para geração de consultas. Use o prompt do sistema para converter consultas de linguagem natural em consultas DSL. A chamada da função tem a seguinte aparência: `query_response = generate_data(bedrock_rt, model_id, system_prompt_query_generation, query, inference_config)`	Python, API Amazon Bedrock, solicitação de LLM

Tarefa	Descrição	Habilidades necessárias
Teste a consulta DSL ativada. OpenSearch	Execute a função query_oss () para executar a consulta DSL gerada na coleção OpenSearch Serverless e retornar os resultados. A função usa o método de pesquisa do OpenSearch cliente: `response = oss_client.search(index="_all", body=temp)`	Python, OpenSearch API, consulta DSL

Teste e avalie

Tarefa	Descrição	Habilidades necessárias
Crie um conjunto de consultas de teste.	Use Claude 3 para gerar um conjunto diversificado de perguntas de teste com base nos dados e esquemas sintéticos: `test_queries = generate_data(bedrock_rt, model_id_sonnet, query_system_prompt, query_prompt, inference_config)`	Solicitação de LLM
Avalie a precisão da conversão DSL da consulta.	Teste a consulta DSL gerada executando consultas OpenSearch e analisando a relevância e a precisão dos resultados retornados. Isso	Python, análise de dados, consulta DSL

Tarefa	Descrição	Habilidades necessárias
	envolve executar a consulta e inspecionar as ocorrências: `output = query_oss (response1) print("Response after running query against Opensearch") print(output)`	
Modelos Claude 3 de referência.	Compare o desempenho de diferentes modelos Claude 3 (Haiku, Sonnet, Sonnet 3.5) para geração de consultas em termos de precisão e latência. Para comparar, altere o `model_id` quando você chama generate_data () e meça o tempo de execução.	Python, benchmarking de desempenho

Limpe e documente

Tarefa	Descrição	Habilidades necessárias
Desenvolva um processo de limpeza.	Exclua todos os índices da coleção OpenSearch Serverless após o uso.	Python, SDK da AWS, API OpenSearch

Recursos relacionados

- Consulta DSL (OpenSearch documentação)
- Documentação OpenSearch do Amazon Service
- OpenSearch Coleções sem servidor
- Documentação do Amazon Bedrock

- Documentação da Amazon SageMaker AI
- AWS SDK para Python (Boto3) documentação

Mais informações

Política do IAM

Aqui está a `APGtext2querydslpolicy` política para a função do IAM usada nesse padrão:

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Allow",
      "Action": [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::sagemaker-*",
        "arn:aws:s3:::sagemaker-*/*"
      ]
    },
    { "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    { "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "aoss:*"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "sagemaker:*"
      ],
      "Resource": [
        "arn:aws:iam::*:role/*", "*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "sagemaker.amazonaws.com"
          }
      }
    },
    { "Effect": "Allow",
      "Action": [
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "aws-marketplace:Subscribe"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws-marketplace:ProductId": [
            "prod-6dw3qvchef7zy",
            "prod-m5ilt4siql27k",
```

```
            "prod-ozonys2hmmpeu"
          ]
        }
      }
    },
    { "Effect": "Allow",
      "Action": [
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*"
    }
  ]
}
```

Técnicas rápidas com modelos Anthropic Claude 3

Esse padrão demonstra as seguintes técnicas de solicitação para conversão text-to-query DSL usando modelos Claude 3.

- Solicitação de poucas fotos: a solicitação de poucas fotos é uma técnica poderosa para melhorar o desempenho dos modelos Claude 3 no Amazon Bedrock. Essa abordagem envolve fornecer ao modelo um pequeno número de exemplos que demonstram os input/output behavior before asking it to perform a similar task. When you use Claude 3 models on Amazon Bedrock, few-shot prompting can be particularly effective for tasks that require specific formatting, reasoning patterns, or domain knowledge. To implement this technique, you typically structure your prompt with two main components: the example section and the actual query. The example section contains one or more input/output pares desejados que ilustram a tarefa, e a seção de consulta apresenta a nova entrada para a qual você deseja uma resposta. Esse método ajuda Claude 3 a entender o contexto e o formato de saída esperado e geralmente resulta em uma resposta mais precisa e consistente.

  Exemplo:

```
"query": {
  "bool": {
    "must": [
      {"match": {"post_type": "recipe"}},
```

```
      {"range": {"likes_count": {"gte": 100}}},
      {"exists": {"field": "media_urls"}}
    ]
  }
}
Question: Find all recipe posts that have at least 100 likes and include media URLs.
```

- Solicitações do sistema: além de algumas solicitações, os modelos Claude 3 no Amazon Bedrock também oferecem suporte ao uso de solicitações do sistema. Os prompts do sistema são uma forma de fornecer contexto geral, instruções ou diretrizes ao modelo antes de apresentá-lo com entradas específicas do usuário. Eles são particularmente úteis para definir o tom, definir o papel do modelo ou estabelecer restrições para toda a conversa. Para usar um prompt do sistema com Claude 3 no Amazon Bedrock, você o inclui no `system` parâmetro da sua solicitação de API. Isso é separado das mensagens do usuário e se aplica a toda a interação. Os prompts detalhados do sistema são usados para definir o contexto e fornecer diretrizes para o modelo.

  Exemplo:

```
You are an expert query dsl generator. Your task is to take an input question and
 generate a query dsl to answer the question. Use the schemas and data below to
 generate the query.

Schemas: [schema details]
Data: [sample data]
Guidelines:
- Ensure the generated query adheres to DSL query syntax
- Do not create new mappings or other items that aren't included in the provided
 schemas.
```

- Saída estruturada: você pode instruir o modelo a fornecer saída em formatos específicos, como JSON ou em tags XML.

  Exemplo:

```
Put the query in json tags
```

- Encadeamento de prompts: o notebook usa a saída de uma chamada LLM como entrada para outra, como usar dados sintéticos gerados para criar exemplos de perguntas.
- Fornecimento de contexto: o contexto relevante, incluindo esquemas e dados de amostra, é fornecido nos prompts.

Exemplo:

```
Schemas: [schema details]
Data: [sample data]
```

- Solicitações específicas de tarefas: solicitações diferentes são criadas para tarefas específicas, como gerar dados sintéticos, criar exemplos de perguntas e converter consultas de linguagem natural em consultas DSL.

  Exemplo para gerar perguntas de teste:

```
Your task is to generate 5 example questions users can ask the health app based on
 provided schemas and data. Only include the questions generated in the response.
```

Use o Amazon Q Developer como assistente de codificação para aumentar sua produtividade

Criado por Ram Kandaswamy (AWS)

Resumo

Esse padrão usa um tic-tac-toe jogo para demonstrar como você pode aplicar o Amazon Q Developer em uma variedade de tarefas de desenvolvimento. Ele gera código para um tic-tac-toe jogo como um aplicativo de página única (SPA), aprimora sua interface de usuário e cria scripts para implantar o aplicativo. AWS

O Amazon Q Developer funciona como um assistente de codificação para ajudar a acelerar os fluxos de trabalho de desenvolvimento de software e aumentar a produtividade tanto para desenvolvedores quanto para não desenvolvedores. Independentemente de sua experiência técnica, ele ajuda você a criar arquiteturas e soluções de design para problemas de negócios, otimiza seu ambiente de trabalho, ajuda a implementar novos recursos e gera casos de teste para validação. Ele usa instruções em linguagem natural e recursos de IA para garantir um código consistente e de alta qualidade e para mitigar os desafios de codificação, independentemente de suas habilidades de programação.

A principal vantagem do Amazon Q Developer é sua capacidade de liberar você de tarefas repetitivas de codificação. Quando você usa a `@workspace` anotação, o Amazon Q Developer ingere e indexa todos os arquivos de código, configurações e estrutura do projeto em seu ambiente de desenvolvimento integrado (IDE) e fornece respostas personalizadas para ajudá-lo a se concentrar na solução criativa de problemas. Você pode dedicar mais tempo para projetar soluções inovadoras e aprimorar a experiência do usuário. Se você não é técnico, pode usar o Amazon Q Developer para simplificar os fluxos de trabalho e colaborar de forma mais eficaz com a equipe de desenvolvimento. O recurso de código Amazon Q Developer Explain oferece instruções e resumos detalhados, para que você possa navegar por bases de código complexas.

Além disso, o Amazon Q Developer fornece uma abordagem independente de linguagem que ajuda desenvolvedores de nível júnior e médio a expandir seus conjuntos de habilidades. Você pode se concentrar nos conceitos básicos e na lógica de negócios, em vez da sintaxe específica do idioma. Isso reduz a curva de aprendizado quando você troca de tecnologia.

Pré-requisitos e limitações

Pré-requisitos

- IDE (por exemplo, WebStorm ou Visual Studio Code) com o plug-in Amazon Q Developer instalado. Para obter instruções, consulte Instalando a extensão ou o plug-in do Amazon Q Developer em seu IDE na documentação do Amazon Q Developer.
- Uma Conta da AWS configuração ativa com o Amazon Q Developer. Para obter instruções, consulte Introdução na documentação do Amazon Q Developer.
- npm instalado. Para obter instruções, consulte a documentação do npm. Esse padrão foi testado com o npm versão 10.8.
- AWS Command Line Interface (AWS CLI) instalado. Para obter instruções, consulte a AWS CLI documentação.

Limitações

- O Amazon Q Developer pode realizar somente uma tarefa de desenvolvimento por vez.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Ferramentas

- Esse padrão requer um IDE, como o Visual Studio Code ou WebStorm. Para obter uma lista dos compatíveis IDEs, consulte a documentação do Amazon Q Developer.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.

Práticas recomendadas

Consulte as melhores práticas de codificação com o Amazon Q Developer na orientação AWS prescritiva. Além disso:

- Ao fornecer solicitações ao Amazon Q Developer, certifique-se de que suas instruções sejam claras e inequívocas. Adicione trechos de código e anotações, como no prompt, `@workspace` para fornecer mais contexto para seus prompts.
- Inclua bibliotecas relevantes e importe-as para evitar conflitos ou suposições incorretas pelo sistema.

- Se o código gerado não for preciso ou conforme o esperado, use a opção Fornecer feedback e regenerar. Tente dividir as instruções em instruções menores.

Épicos

Configurar o ambiente de trabalho

Tarefa	Descrição	Habilidades necessárias
Criar um novo projeto da .	Para criar um novo projeto em seu ambiente de trabalho, execute o comando a seguir e aceite as configura ções padrão para todas as perguntas: `npx create-next-app@la test`	Desenvolvedor de aplicativos, Programador, Desenvolvedor de software
Teste o aplicativo básico.	Execute o comando a seguir e confirme se o aplicativo base foi carregado com êxito no navegador: `npm run dev`	Desenvolvedor de aplicativos, Programador, Desenvolvedor de software
Limpe o código base.	Navegue até o `page.tsx` arquivo na `src/app` pasta e exclua o conteúdo padrão para obter uma página em branco. Após a exclusão, o arquivo deve ficar assim: `export default function Home() { return (<div></div> );`	Desenvolvedor de aplicativos, Programador, Desenvolvedor de software

Tarefa	Descrição	Habilidades necessárias
	`}`	

Use o Amazon Q Developer para criar um projeto de tic-tac-toe jogo

Tarefa	Descrição	Habilidades necessárias
Tenha uma visão geral das etapas.	1. No seu IDE, abra seu projeto e escolha o ícone Amazon Q para abrir o painel de bate-papo. 2. No painel de bate-papo do Amazon Q Developer, peça uma visão geral da criação de um aplicativo de página única (SPA). Por exemplo: `I would like to create a single-page application involving Next.js React framework for tic-tac-toe game. What are the steps?`	Desenvolvedor de aplicativos, Programador, Desenvolvedor de software
Gere código para tic-tac-toe.	No painel de bate-papo, inicie uma tarefa de desenvolv imento usando o `/dev` comando seguido pela descrição da tarefa. Por exemplo: `/dev Create a React-based single-page application written in TypeScript for a tic-tac-toe game with`	Desenvolvedor de aplicativos, Programador, Desenvolvedor de software

Tarefa	Descrição	Habilidades necessárias
	``` the following specifica tions: 1. Design an aesthetic ally pleasing interface with the game grid centered vertically and horizontally on the page. 2. Include a heading and clear instructions on how to play the game. 3. Implement color-cod ing for X and O marks to distinguish them easily. ``` O Amazon Q Developer gera código com base em suas instruções.	
Inspecione e aceite o código gerado.	Inspecione visualmente o código e escolha Aceitar código para substituir automaticamente o `page.tsx` arquivo. Se você tiver problemas, escolha Fornecer feedback e regenerar e descreva o problema que você encontrou.	Desenvolvedor de aplicativos, Programador, Desenvolvedor de software

Tarefa	Descrição	Habilidades necessárias
Corrija erros de fiapos.	O tic-tac-toe jogo de exemplo inclui uma grade. O código que o Amazon Q Developer gera pode usar o tipo padrãoany. Você pode adicionar segurança de tipos solicitando ao Amazon Q Developer o seguinte: `/dev Ensure proper TypeScript typing for the onSquare Click event handler to resolve any 'any' type issues.`	Desenvolvedor de aplicativos, Programador, Desenvolvedor de software

Tarefa	Descrição	Habilidades necessárias

Adicione apelo visual.	Você pode dividir o requisito original em fragmentos menores. Por exemplo, você pode melhorar a interface do jogo com as seguintes instruções nas tarefas de desenvolvimento. Esse prompt aprimora os estilos do Cascading Style Sheets (CSS) e exporta o aplicativo para implantação.
	
	`/dev Debug and fix any CSS issues to correctly display the game grid and overall layout.`
	
	`Simplify the code by removing game history functionality and related components.`
	
	`Implement static file export to an 'out' directory for easy deployment. The solution should be fully functional, visually appealing, and free of typing errors or layout issues.`
		Desenvolvedor de aplicativos, Programador, Desenvolvedor de software

Tarefa	Descrição	Habilidades necessárias

Teste novamente.	1. Agora que você concluiu o ciclo de vida de desenvolvimento, teste o código para confirmar se ele funciona conforme o esperado. Para executar o aplicativo localmente, use o comando:
	`npm run dev`
	2. Se o aplicativo funcionar conforme o esperado, use o `build` comando para exportar o aplicativo inteiro para a pasta de saída em preparação para a implantação:
	`npm run build`
		Desenvolvedor de aplicativos, Programador, Desenvolvedor de software

Implante o aplicativo no Nuvem AWS

Tarefa	Descrição	Habilidades necessárias

Crie pastas e arquivos para implantação.	No projeto em seu ambiente de trabalho, crie uma pasta de implantação e dois arquivos dentro dela: `pushtos3.sh` `ecloudformation.yml` :
	`mkdir deployment && cd deployment`
	`touch pushtos3.sh && chmod +x pushtos3.sh`
		Desenvolvedor de aplicativos, Programador, Desenvolvedor de software

Tarefa	Descrição	Habilidades necessárias
	`touch cloudform ation.yml`	
Gere código de automação.	1. No painel de bate-papo do Amazon Q Developer, forneça o seguinte aviso: `/dev Generate a Cloudformation template that creates two resources: tictactoe artifact bucket and CloudFron t. CloudFront should be configure d with this bucket as origin. Add cache policy appropriate for Amazon S3 and default root object as index.html. Ensure that origin access control is used and no public bucket is created. Output all the resources and their ARNs.` 2. Revise e aceite o código gerado. O `cloudform ation.yml` arquivo que você criou anteriormente agora deve ser preenchid o com um AWS CloudForm ation script que cria os recursos para o. Nuvem AWS	Administrador da AWS, AWS DevOps, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Gere conteúdo de script.	Para criar um script de implantação, use o seguinte prompt: `/dev Modify the pushtos3 shell script so that it can use AWS CLI commands to create a CloudFormation stack named tictactoe-stack if it does not exist already, and use cloudformation.yml as the source template. Wait for the stack to complete and sync the contents from the out folder to the S3 bucket. Perform invalidation of the CloudFront origin.`	Desenvolvedor de aplicativos, Programador, Desenvolvedor de software
Implante o aplicativo no Nuvem AWS.	1. Configure o ambiente de trabalho com AWS credenciais válidas. 2. Execute o script do shell para implantar o tic-tac-toe jogo totalmente funcional no Nuvem AWS.	Administrador da AWS, AWS DevOps, arquiteto de nuvem, desenvolvedor de aplicativos

Solução de problemas

Problema	Solução

A compilação não cria um aplicativo de página única nem o exporta para a pasta de saída.	Veja o conteúdo do `next.config.mjs` arquivo.
	
	Se o código tiver a seguinte configuração padrão:
	
	`const nextConfig = {};`
	
	modifique-o da seguinte forma:
	
	`const nextConfig = {`
	`  output: 'export',`
	`  distDir: 'out',`
	`};`

Recursos relacionados

- Criando um novo projeto React (documentação do React)
- Visão geral do Amazon Q Developer (AWS documentação)
- Melhores práticas do Amazon Q Developer (AWS orientação prescritiva)
- Instalando, configurando e usando o Amazon Q Developer com JetBrains IDEs (YouTube vídeo)
- Instalando o Amazon Q para a linha de comando (AWS documentação)

Use o SageMaker processamento para engenharia de recursos distribuídos de conjuntos de dados de ML em escala de terabytes

Criado por Chris Boomhower (AWS)

Resumo

Muitos conjuntos de dados em escala de terabytes ou maiores geralmente consistem em uma estrutura hierárquica de pastas e os arquivos no conjunto de dados às vezes compartilham interdependências. Por esse motivo, engenheiros de machine learning (ML) e cientistas de dados devem tomar decisões de design ponderadas para preparar esses dados para treinamento e inferência de modelos. Esse padrão demonstra como você pode usar técnicas manuais de macrofragmentação e microfragmentação em combinação com o Amazon SageMaker Processing e a paralelização de CPU virtual (vCPU) para escalar com eficiência os processos de engenharia de recursos para conjuntos de dados ML de big data complicados.

Esse padrão define macrofragmentação como a divisão de diretórios de dados em várias máquinas para processamento e microfragmentação como a divisão de dados em cada máquina em vários segmentos de processamento. O padrão demonstra essas técnicas usando a Amazon SageMaker com amostras de registros de formas de onda de séries temporais do conjunto de dados MIMIC-III. PhysioNet Ao implementar as técnicas nesse padrão, você pode minimizar o tempo de processamento e os custos da engenharia de atributos e, ao mesmo tempo, maximizar a utilização dos recursos e a eficiência de throughput. Essas otimizações dependem do SageMaker processamento distribuído nas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e v CPUs para conjuntos de dados grandes e semelhantes, independentemente do tipo de dados.

Pré-requisitos e limitações

Pré-requisitos

- Acesso às instâncias do SageMaker notebook ou ao SageMaker Studio, se você quiser implementar esse padrão para seu próprio conjunto de dados. Se você estiver usando a Amazon SageMaker pela primeira vez, consulte Comece a usar a Amazon SageMaker na documentação da AWS.
- SageMaker Studio, se você quiser implementar esse padrão com os dados de amostra do PhysioNet MIMIC-III.
- O padrão usa SageMaker Processing, mas não exige nenhuma experiência na execução de trabalhos SageMaker de Processing.

Limitações

- Esse padrão é adequado para conjuntos de dados de ML que incluem arquivos interdependentes. Essas interdependências são as que mais se beneficiam da fragmentação manual de macros e da execução paralela de várias tarefas de processamento de instância única SageMaker . Para conjuntos de dados em que essas interdependências não existem, o `ShardedByS3Key` recurso em SageMaker Processing pode ser uma alternativa melhor à macrofragmentação, pois envia dados fragmentados para várias instâncias que são gerenciadas pela mesma tarefa de Processamento. No entanto, você pode implementar a estratégia de microfragmentação desse padrão em ambos os cenários para melhor utilizar a instância v. CPUs

Versões do produto

- SDK do Amazon SageMaker Python versão 2

Arquitetura

Pilha de tecnologias de destino

- Amazon Simple Storage Service (Amazon S3)
- Amazon SageMaker

Arquitetura de destino

Macrofragmentação e instâncias distribuídas EC2

Os 10 processos paralelos representados nessa arquitetura refletem a estrutura do conjunto de dados MIMIC-III. (Os processos são representados por elipses para simplificar o diagrama.) Uma arquitetura semelhante se aplica a qualquer conjunto de dados quando você usa macrofragmentação manual. No caso do MIMIC-III, você pode usar a estrutura bruta do conjunto de dados a seu favor, processando cada pasta de grupo de pacientes separadamente, com o mínimo esforço. No diagrama a seguir, o bloco de grupos de registros aparece à esquerda (1). Dada a natureza distribuída dos dados, faz sentido fragmenta-los por grupo de pacientes.

No entanto, a fragmentação manual por grupo de pacientes significa que uma tarefa de processamento separada é necessária para cada pasta do grupo de pacientes, como você pode ver na seção central do diagrama (2), em vez de uma única tarefa de processamento com várias

EC2 instâncias. Como os dados do MIMIC-III incluem arquivos de forma de onda binários e arquivos de cabeçalho baseados em texto correspondentes, e há uma dependência necessária da biblioteca wfdb para extração de dados binários, todos os registros de um paciente específico devem ser disponibilizados na mesma instância. A única maneira de garantir que o arquivo de cabeçalho associado a cada arquivo de forma de onda binária também esteja presente é implementar a fragmentação manual para executar cada fragmento em seu próprio trabalho de processamento e especificar `s3_data_distribution_type='FullyReplicated'` quando você define a entrada do trabalho de processamento. Como alternativa, se todos os dados estivessem disponíveis em um único diretório e não existissem dependências entre os arquivos, uma opção mais adequada seria iniciar uma única tarefa de processamento com várias EC2 instâncias e `s3_data_distribution_type='ShardedByS3Key'` especificadas. A especificação `ShardedByS3Key` do tipo de distribuição de dados do Amazon S3 SageMaker direciona o gerenciamento automático da fragmentação de dados entre instâncias.

Iniciar uma tarefa de processamento para cada pasta é uma forma econômica de pré-processar os dados, pois a execução simultânea de várias instâncias economiza tempo. Para economizar custos e tempo adicionais, você pode usar a microfragmentação em cada tarefa de processamento.

Microfragmentação e parallel v CPUs

Em cada tarefa de processamento, os dados agrupados são divididos ainda mais para maximizar o uso de todos os v disponíveis CPUs na EC2 instância SageMaker totalmente gerenciada. Os blocos na seção central do diagrama (2) mostram o que acontece em cada tarefa de processamento principal. O conteúdo das pastas de registros do paciente é nivelado e dividido uniformemente com base no número de v disponíveis CPUs na instância. Depois que o conteúdo da pasta é dividido, o conjunto de arquivos de tamanho uniforme é distribuído em todos os v CPUs para processamento. Quando o processamento é concluído, os resultados de cada vCPU são combinados em um único arquivo de dados para cada tarefa de processamento.

No código em anexo, esses conceitos são representados na seção a seguir do arquivo `src/feature-engineering-pass1/preprocessing.py`.

```
def chunks(lst, n):
    """
    Yield successive n-sized chunks from lst.

    :param lst: list of elements to be divided
    :param n: number of elements per chunk
    :type lst: list
```

```
    :type n: int
    :return: generator comprising evenly sized chunks
    :rtype: class 'generator'
    """
    for i in range(0, len(lst), n):
        yield lst[i:i + n]


# Generate list of data files on machine
data_dir = input_dir
d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]
file_list = []
for ds in d_subs:
    file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))
dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in
 file_list if f[-4:] == '.dat']

# Split list of files into sub-lists
cpu_count = multiprocessing.cpu_count()
splits = int(len(dat_list) / cpu_count)
if splits == 0: splits = 1
dat_chunks = list(chunks(dat_list, splits))

# Parallelize processing of sub-lists across CPUs
ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in
 dat_chunks)

# Compile and pickle patient group dataframe
ws_df_group = pd.concat(ws_df_list)
ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})
ws_df_group.to_json(os.path.join(output_dir, group_data_out))
```

Uma função, `chunks`, é definida primeiro para consumir uma determinada lista dividindo-a em partes de tamanho uniforme `n` e retornando esses resultados como um gerador. Em seguida, os dados são agrupados nas pastas dos pacientes compilando uma lista de todos os arquivos binários de forma de onda que estão presentes. Depois disso, o número de v CPUs disponível na EC2 instância é obtido. A lista de arquivos de forma de onda binária é dividida uniformemente entre esses v CPUs por meio de uma chamada `echunks`, em seguida, cada sublista de forma de onda é processada em sua própria vCPU usando a classe Parallel do joblib. Os resultados são combinados automaticamente em uma única lista de dataframes pelo trabalho de processamento, que SageMaker então processa ainda mais antes de gravá-los no Amazon S3 após a conclusão do

trabalho. Neste exemplo, há 10 arquivos gravados no Amazon S3 pelos trabalhos de processamento (um para cada trabalho).

Quando todas as tarefas de processamento iniciais estiverem concluídas, uma tarefa de processamento secundária, mostrada no bloco à direita do diagrama (3), combina os arquivos de saída produzidos por cada tarefa de processamento principal e grava a saída combinada no Amazon S3 (4).

Ferramentas

Ferramentas

- Python: o código de amostra usado para esse padrão é Python (versão 3).
- SageMaker Studio — O Amazon SageMaker Studio é um ambiente de desenvolvimento integrado (IDE) baseado na web para aprendizado de máquina que permite criar, treinar, depurar, implantar e monitorar seus modelos de aprendizado de máquina. Você executa trabalhos SageMaker de processamento usando notebooks Jupyter dentro do Studio. SageMaker
- SageMaker Processamento — O Amazon SageMaker Processing fornece uma forma simplificada de executar suas cargas de trabalho de processamento de dados. Nesse padrão, o código de engenharia de recursos é implementado em escala usando trabalhos SageMaker de processamento.

Código

O arquivo .zip anexado fornece o código completo desse padrão. A seção a seguir descreve as etapas para criar a arquitetura para esse padrão. Cada etapa é ilustrada pelo código de amostra do anexo.

Épicos

Configure seu ambiente SageMaker Studio

Tarefa	Descrição	Habilidades necessárias
Acesse o Amazon SageMaker Studio.	Integre-se ao SageMaker Studio em sua conta da AWS seguindo as instruçõe	Cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias
	s fornecidas na SageMaker documentação da Amazon.	
Instale o utilitário wget.	Instale o wget se você embarcou com uma nova configuração do SageMaker Studio ou se nunca usou esses utilitários no Studio antes. SageMaker Para instalar, abra uma janela de terminal no console do SageMaker Studio e execute o seguinte comando: `sudo yum install wget`	Cientista de dados, engenheiro de ML

Faça download e descompacte o código de exemplo.	Faça o download do arquivo `attachments.zip` na seção Anexos. Em uma janela de terminal, navegue até a pasta em que você baixou o arquivo e extraia seu conteúdo:
	
	`unzip attachment.zip`
	
	Navegue até a pasta em que você extraiu o arquivo .zip e extraia o conteúdo do arquivo `Scaled-Processing.zip` .
	
	`unzip Scaled-Processing.zip`
		Cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias
Faça o download do conjunto de dados de amostra em physionet.org e faça o upload para o Amazon S3.	Execute o caderno Jupyter `get_data.ipynb` dentro da pasta que contém os arquivos `Scaled-Processing` . Este notebook baixa uma amostra do conjunto de dados MIMIC-III do physionet.org e a carrega em seu bucket de sessão do Studio no Amazon S3. SageMaker	Cientista de dados, engenheiro de ML

Configurar o primeiro script de pré-processamento

Tarefa	Descrição	Habilidades necessárias

Nivele a hierarquia de arquivos em todos os subdiretórios.	Em grandes conjuntos de dados, como o MIMIC-III , os arquivos geralmente são distribuídos em vários subdiretórios, mesmo dentro de um grupo pai lógico. Seu script deve ser configurado para nivelar todos os arquivos do grupo em todos os subdiretórios, conforme demonstra o código a seguir.
	`# Generate list of .dat files on machine`
	`data_dir = input_dir`
	`d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]`
	`file_list = []`
	`for ds in d_subs:`
		Cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias

	`file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))`
	`dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in file_list if f[-4:] == '.dat']`
	
	Note
	Os trechos de código de exemplo neste épico são do `src/feature-engineering-pass1/preprocessing.py` arquivo, que é fornecido no anexo.	

Tarefa	Descrição	Habilidades necessárias

Divida os arquivos em subgrupos com base na contagem de vCPUs.	Os arquivos devem ser divididos em subgrupos ou partes de tamanho uniforme, dependendo do número de v CPUs presente na instância que executa o script. Para esta etapa, você pode implementar um código semelhante ao seguinte.
	`# Split list of files into sub-lists`
	`cpu_count = multiprocessing.cpu_count()`
	`splits = int(len(dat_list) / cpu_count)`
	`if splits == 0: splits = 1`
	`dat_chunks = list(chunks(dat_list, splits))`
		Cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias

Paralelize o processamento de subgrupos em v. CPUs	A lógica do script deve ser configurada para processar todos os subgrupos em paralelo. Para fazer isso, use a classe `Parallel` e o método `delayed` da biblioteca Joblib da seguinte forma.
	`# Parallelize processing of sub-lists across CPUs`
	`ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in dat_chunks)`
		Cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias

Salve a saída de um único grupo de arquivos no Amazon S3.	Quando o processamento paralelo da vCPU estiver concluído, os resultados de cada vCPU deverão ser combinados e enviados para o caminho do bucket S3 do grupo de arquivos. Para esta etapa, você pode usar um código semelhante ao seguinte.
	`# Compile and pickle patient group dataframe`
	`ws_df_group = pd.concat(ws_df_list)`
	`ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})`
	`ws_df_group.to_json(os.path.join(output_dir, group_data_out))`
		Cientista de dados, engenheiro de ML

Configurar o segundo script de pré-processamento

Tarefa	Descrição	Habilidades necessárias
Combine arquivos de dados produzidos em todas as tarefas de processamento que executaram o primeiro script.	O script anterior gera um único arquivo para cada tarefa de SageMaker processamento que processa um grupo de arquivos do conjunto de dados. Em seguida, você precisa combinar esses	Cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias

	arquivos de saída em um único objeto e gravar um único conjunto de dados de saída no Amazon S3. Isso é demonstrado no arquivo `src/feature-engineering-pass1p5/preprocessing.py`, que é fornecido no anexo, da seguinte forma.
	
	`def write_parquet(wavs_df, path):`
	`    """`
	`    Write waveform summary dataframe to S3 in parquet format.`
	
	`    :param wavs_df: waveform summary dataframe`
	`    :param path: S3 directory prefix`
	`    :type wavs_df: pandas dataframe`
	`    :type path: str`
	`    :return: None`
	`    """`
	`    extra_args = {"ServerSideEncryption": "aws:kms"}`
	`    wr.s3.to_parquet(`
	`        df=wavs_df,`
	`        path=path,`
	`        compression='snappy',`
	`        s3_additional_kwargs=extra_args)`	

Tarefa	Descrição	Habilidades necessárias

	`def combine_data():`
	`    """`
	`    Get combined data and write to parquet.`
	
	`    :return: waveform summary dataframe`
	`    :rtype: pandas dataframe`
	`    """`
	`    wavs_df = get_data()`
	`    wavs_df = normalize_signal_names(wavs_df)`
	`    write_parquet(wavs_df, "s3://{}/{}/{}".format(bucket_xform, dataset_prefix, pass1p5out_data))`
	
	`    return wavs_df`
	
	`wavs_df = combine_data()`	

Executar tarefa de processamento

Tarefa	Descrição	Habilidades necessárias
Execute a primeira tarefa de processamento.	Para realizar a fragmentação de macros, execute uma tarefa de processamento separada para cada grupo de arquivos. A microfragmentação é executada dentro	Cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias

	de cada tarefa de processamento, porque cada tarefa executa seu primeiro script. O código a seguir demonstra como iniciar uma tarefa de processamento para cada diretório de grupo de arquivos no trecho a seguir (incluído em `notebooks/FeatExtract_Pass1.ipynb`).
	
	`pat_groups = list(range(30,40))`
	`ts = str(int(time.time()))`
	
	`for group in pat_groups:`
	`  sklearn_processor = SKLearnProcessor(framework_version='0.20.0',`
	
	`  role=role,`
	
	`  instance_type='ml.m5.4xlarge',`
	
	`  instance_count=1,`
	
	`  volume_size_in_gb=5)`
	`  sklearn_processor.run(`
	`  code='../src/feature-engineering-pass1/preprocessing.py',`	

Tarefa	Descrição	Habilidades necessárias
	job_name= '-'.join(['scaled-processing-p1', str(group), ts]), arguments=["input_path", "/opt/ml/processing/input", "output_path", "/opt/ml/processing/output", "group_data_out", "ws_df_group.json"], inputs= [ProcessingInput(source=f's3://{sess.default_bucket()}/data_inputs/{group}', destination='/opt/ml/processing/input', s3_data_distribution_type='FullyReplicated')], outputs= [ProcessingOutput(source='/opt/ml/processing/output', destination=f's3://{sess.default_buc	

Tarefa	Descrição	Habilidades necessárias

	<pre>ket()}/data_outputs/
	{group}'
	)
	],
	wait=False
	)</pre>	

Tarefa	Descrição	Habilidades necessárias

Execute a segunda tarefa de processamento.	Para combinar as saídas geradas pelo primeiro conjunto de trabalhos de processamento e realizar quaisquer cálculos adicionais para pré-processamento, você executa seu segundo script usando um único SageMaker trabalho de processamento. O código a seguir demonstra isso (incluído em `notebooks/FeatExtract_Pass1p5.ipynb`).
	
	`ts = str(int(time.time()))`
	`bucket = sess.default_bucket()`
	
	`sklearn_processor = SKLearnProcessor(framework_version='0.20.0',`
	
	`role=role,`
	
	`instance_type='ml.t3.2xlarge',`
	
	`instance_count=1,`
	
	`volume_size_in_gb=5)`
	`sklearn_processor.run(`
	`code='../src/feature-engineering-pass1p5/preprocessing.py',`
		Cientista de dados, engenheiro de ML

Tarefa	Descrição	Habilidades necessárias
	`job_name='-'.join(['scaled-processing', 'p1p5', ts]), arguments=['bucket', bucket, 'pass1out_prefix', 'data_outputs', 'pass1out_data', 'ws_df_group.json', 'pass1p5out_data', 'waveform_summary.parquet', 'statsdata_name', 'signal_stats.csv'], wait=True )`	

Recursos relacionados

- Integre-se ao Amazon SageMaker Studio usando o Quick Start (SageMaker documentação)
- Dados do processo (SageMaker documentação)
- Processamento de dados com scikit-learn (documentação) SageMaker
- Documentação do joblib.PARALLEL
- Moody, B., Moody, G., Villarroel, M., Clifford, G. D. e Silva, I. (2020). Banco de dados de formas de onda MIMIC-III (versão 1.0). PhysioNet.
- Johnson, A. E. W., Pollard, T.J., Shen, L., Lehman, L. H., Feng, M., Ghassemi, M., Moody, B., Szolovits, P., Celi, L. A. e Mark, R.G. (2016). MIMIC-III, um banco de dados de cuidados intensivos de acesso gratuito. Dados científicos, 3, 160035.
- Licença do banco de dados MIMIC-III Waveform

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Visualize os resultados do modelo de IA/ML usando o Flask e o AWS Elastic Beanstalk

Criado por Chris Caudill (AWS) e Durga Sury (AWS)

Resumo

A visualização do resultado dos serviços de inteligência artificial e machine learning (IA/ML) geralmente exige chamadas de API complexas que devem ser personalizadas por seus desenvolvedores e engenheiros. Isso pode ser uma desvantagem se seus analistas quiserem explorar rapidamente um novo conjunto de dados.

Você pode aprimorar a acessibilidade de seus serviços e fornecer uma forma mais interativa de análise de dados usando uma interface de usuário (UI) baseada na web que permite que os usuários carreguem seus próprios dados e visualizem os resultados do modelo em um painel.

Esse padrão usa Flask e Plotly para integrar o Amazon Comprehend a um aplicativo web personalizado e visualizar sentimentos e entidades a partir de dados fornecidos pelo usuário. O padrão também fornece as etapas para implantar um aplicativo usando o AWS Elastic Beanstalk. Você pode adaptar o aplicativo usando os serviços de IA da Amazon Web Services (AWS) ou com um modelo personalizado treinado hospedado em um endpoint (por exemplo, um SageMaker endpoint da Amazon).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI), instalada e configurada na sua máquina local. Para obter mais informações, consulte Noções básicas de configuração na documentação da AWS CLI. Você também pode usar um ambiente de desenvolvimento integrado (IDE) do AWS Cloud9; para obter mais informações a respeito, consulte Tutorial do Python para o AWS Cloud9 e Visualização de aplicativos em execução no IDE do AWS Cloud9 na documentação do AWS Cloud9.

  Aviso: não AWS Cloud9 está mais disponível para novos clientes. Os clientes existentes do AWS Cloud9 podem continuar usando o serviço normalmente. Saiba mais
- Uma compreensão da estrutura de aplicativos web do Flask. Para obter mais informações sobre o Flask, consulte Início rápido na documentação do Flask.

- A versão 3.6 ou superior do Phyton está instalada e configurada. Você pode instalar o Python seguindo as instruções em Configuração de seu ambiente de desenvolvimento em Python na documentação do AWS Elastic Beanstalk.
- Interface de linha de comando do Elastic Beanstalk (CLI do EB) instalada e configurada. Para obter mais informações a respeito, consulte Instalar a EB CLI e Configurar a EB CLI na documentação do AWS Elastic Beanstalk.

Limitações

- O aplicativo Flask deste padrão foi desenvolvido para funcionar com arquivos .csv que usam uma única coluna de texto e estão restritos a 200 linhas. O código do aplicativo pode ser adaptado para lidar com outros tipos de arquivos e volumes de dados.
- O aplicativo não considera a retenção de dados e continua agregando arquivos de usuário enviados até que eles sejam excluídos manualmente. Você pode integrar o aplicativo ao Amazon Simple Storage Service (Amazon S3) para armazenamento persistente de objetos ou usar um banco de dados como o Amazon DynamoDB para armazenamento de valores-chave de tecnologia sem servidor.
- O aplicativo considera apenas documentos no idioma inglês. No entanto, você pode usar o Amazon Comprehend para detectar o idioma principal de um documento. Para obter mais informações sobre os idiomas compatíveis para cada ação, consulte a Referência de APIs na documentação do Amazon Comprehend.
- Uma lista de solução de problemas que contém erros comuns e suas soluções está disponível na seção Informações adicionais.

Arquitetura

Arquitetura do aplicativo Flask

O Flask é uma estrutura leve para o desenvolvimento de aplicativos web em Python. Ele foi projetado para combinar o poderoso processamento de dados do Python com uma rica interface de usuário da web. O aplicativo Flask do padrão mostra como criar um aplicativo web que permite aos usuários fazer upload de dados, enviar os dados para o Amazon Comprehend para inferência e, em seguida, visualizar os resultados. O aplicativo possui a seguinte estrutura:

- `static`— Contém todos os arquivos estáticos que suportam a interface do usuário da web (por exemplo JavaScript, CSS e imagens)

- `templates`: contém todas as páginas HTML do aplicativo
- `userData`: armazena dados do usuário enviados
- `application.py`: o arquivo do aplicativo Flask
- `comprehend_helper.py`: funções para fazer chamadas de API para o Amazon Comprehend
- `config.py`: o arquivo de configuração de aplicativo
- `requirements.txt`: as dependências do Python exigidas pelo aplicativo

O script `application.py` contém a funcionalidade principal do aplicativo web, que consiste em quatro rotas do Flask. O diagrama a seguir mostra essas rotas do Flask.

- `/` é a raiz do aplicativo e direciona os usuários para a página `upload.html` (armazenada no diretório `templates`).
- `/saveFile` é uma rota invocada depois que um usuário carrega um arquivo. Essa rota recebe uma solicitação `POST` por meio de um formulário HTML, que contém o arquivo enviado pelo usuário. O arquivo é salvo no diretório `userData` e a rota redireciona os usuários para a rota `/dashboard`.
- `/dashboard` envia os usuários para a página `dashboard.html`. No HTML dessa página, ele executa o JavaScript código `static/js/core.js` que lê os dados da `/data` rota e, em seguida, cria visualizações para a página.
- `/data` é uma API JSON que apresenta os dados a serem visualizados no painel. Esta rota lê os dados fornecidos pelo usuário e usa as funções em `comprehend_helper.py` para enviar os dados do usuário ao Amazon Comprehend visando à análise de sentimentos e ao reconhecimento de entidade nomeada (NER). A resposta do Amazon Comprehend é formatada e retornada como um objeto JSON.

Arquitetura de implantação

Considerações sobre design

Para obter mais informações sobre considerações de design para aplicativos implantados usando o Elastic Beanstalk na nuvem da AWS, consulte a documentação do AWS Elastic Beanstalk.

Pilha de tecnologia

- Amazon Comprehend
- Elastic Beanstalk
- Flask

Automação e escala

As implantações do Elastic Beanstalk são configuradas automaticamente com balanceadores de carga e grupos do Auto Scaling. Para obter mais opções de configuração, consulte Configuração dos ambientes do Elastic Beanstalk na documentação do AWS Elastic Beanstalk.

Ferramentas

- A AWS Command Line Interface (AWS CLI) é uma ferramenta unificada que fornece uma interface consistente para interagir com todas as partes da AWS.
- O Amazon Comprehend usa processamento de linguagem natural (NLP) para extrair insights sobre o conteúdo dos documentos sem exigir um pré-processamento especial.
- O AWS Elastic Beanstalk ajuda você a implantar e gerenciar rapidamente aplicativos na nuvem da AWS sem precisar aprender sobre a infraestrutura que executa esses aplicativos.
- A CLI do Elastic Beanstalk (EB CLI) é uma interface de linha de comando para o AWS Elastic Beanstalk que fornece comandos interativos para simplificar a criação, a atualização e o monitoramento de ambientes a partir de um repositório local.
- A estrutura Flask executa processamento de dados e chamadas de API usando Python e oferece visualização web interativa com o Plotly.

Código

O código desse padrão está disponível nos resultados do modelo GitHub Visualize AI/ML usando o Flask e o repositório AWS Elastic Beanstalk.

Épicos

Configurar o aplicativo Flask

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Extraia o código do aplicativo dos resultados do modelo	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	GitHub Visualize AI/ML usando o Flask e o repositório AWS Elastic Beanstalk executando o seguinte comando: `git clone git@github.com:aws-samples/aws-comprehend-elasticbeanstalk-for-flask.git` **Note** Certifique-se de configurar suas chaves SSH com GitHub.	

Tarefa	Descrição	Habilidades necessárias

Instale os módulos do Python.	Depois de clonar o repositório, um novo diretório `aws-comprehend-elasticbeanstalk-for-flask` local é criado. Nesse diretório, o arquivo `requirements.txt` contém os módulos e versões do Python que executam o aplicativo. Use o comando a seguir para instalar os módulos:
	`cd aws-comprehend-elasticbeanstalk-for-flask`
	`pip install -r requirements.txt`
		Desenvolvedor de Python

Tarefa	Descrição	Habilidades necessárias

Testar o aplicativo localmente.	Execute o comando a seguir para iniciar o servidor do Flask:
	
	`python application.py`
	
	Isso retorna informações sobre o servidor em execução. Você deve conseguir acessar o aplicativo abrindo um navegador e visitando http://localhost:5000
	
	Note
	Se você estiver executando o aplicativo em um AWS Cloud9 IDE, precisará substituir `application.run()` o comando no arquivo `application.py` pela seguinte linha:
	
	`application.run(host=os.getenv('IP', '0.0.0.0'),port=int(os.getenv('PORT', 8080)))`
	
	Você deve reverter essa alteração antes da implantação.
		Desenvolvedor de Python

Implante o aplicativo no Elastic Beanstalk

Tarefa	Descrição	Habilidades necessárias
Inicie o aplicativo do Elastic Beanstalk.	Para iniciar seu projeto como um aplicativo do Elastic Beanstalk, execute o seguinte comando no diretório raiz do seu aplicativo: `eb init -p python-3.6 comprehend_flask --region us-east-1` ⚠ Important • `comprehend_flask` é o nome do aplicativo do Elastic Beanstalk e pode ser alterado de acordo com seus requisitos. • Você pode substituir a região da AWS por uma região de sua escolha. A região padrão na AWS CLI será usada se você não especificar uma região. • O aplicativo foi desenvolvido com a versão 3.6 do Python. Você poderá encontrar erros se usar outras versões do Python.	Arquiteto, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Execute o comando `eb init -i` para obter mais opções de configuração de implantação.	
Configure o ambiente do Elastic Beanstalk.	Execute o comando a seguir do diretório raiz do aplicativo: `eb create comprehend-flask-env` **Note** `comprehend-flask-env` é o nome do ambiente do Elastic Beanstalk e pode ser alterado de acordo com suas necessidades. O nome pode conter somente letras, números e hifens.	Arquiteto, desenvolvedor

Tarefa	Descrição	Habilidades necessárias

Autorize sua implantação para usar o Amazon Comprehend.	Embora seu aplicativo possa ser implantado com sucesso, você também deve fornecer à sua implantação acesso ao Amazon Comprehend. `ComprehendFullAccess` é uma política gerenciada pela AWS que fornece ao aplicativo implantado permissões para fazer chamadas de API para o Amazon Comprehend.
	
	Anexe a `ComprehendFullAccess` política a `aws-elasticbeanstalk-ec2-role` (essa função é criada automaticamente para as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) da sua implantação) executando o seguinte comando:
	
	`aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/ComprehendFullAccess --role-name aws-elasticbeanstalk-ec2-role`
	
	Important
	`aws-elasticbeanstalk-`
		Desenvolvedor, arquiteto de segurança

Tarefa	Descrição	Habilidades necessárias
	`ec2-role` é criado quando seu aplicativo é implantado. É necessário concluir o processo de implantação antes que seja possível anexar a política do AWS Identity and Access Management (IAM).	
Visite seu aplicativo implantado.	Depois que seu aplicativo for implantado com sucesso, você poderá visitá-lo executando o comando `eb open`. Você também pode executar o comando `eb status` para obter detalhes sobre sua implantação. O URL de implantação está sob `CNAME`.	Arquiteto, desenvolvedor

(Opcional) Personalize o aplicativo de acordo com seu modelo de ML

Tarefa	Descrição	Habilidades necessárias
Autorize o Elastic Beanstalk a acessar o novo modelo.	Certifique-se de que o Elastic Beanstalk tenha as permissões de acesso necessárias para seu novo modelo de endpoint. Por exemplo, se você usa um SageMaker endpoint da Amazon, sua implantação	Desenvolvedor, arquiteto de segurança

Tarefa	Descrição	Habilidades necessárias
	precisa ter permissão para invocar o endpoint. Para obter mais informaçõ es sobre isso, consulte InvokeEndpointa SageMaker documentação da Amazon.	

Tarefa	Descrição	Habilidades necessárias
Envie os dados do usuário para um novo modelo.	Para alterar o modelo de ML subjacente nesse aplicativo, você deve alterar os seguintes arquivos: • `comprehend_helper.py` : este é o script do Python que se conecta ao Amazon Comprehend, processa a resposta e retorna o resultado final para o aplicativo. Nesse script, você pode rotear os dados para outro serviço de IA na Nuvem AWS ou enviar os dados para um endpoint de modelo personalizado. Recomendamos que você também formate os resultados nesse script para a separação lógica e a reutilização desse padrão. • `application.py` : se você alterar o nome do script `comprehend_helper.py` ou das funções, precisará atualizar o script `application.py` do aplicativo para refletir essas alterações.	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
Atualize as visualizações do painel.	Normalmente, com a incorporação de um novo modelo de ML, as visualizações devem ser atualizadas para refletir os novos resultados. As alterações a seguir são feitas nos seguintes arquivos: • `templates/dashboard.html` : o aplicativo pré-construído responde apenas por duas visualizações básicas. Todo o layout da página pode ser ajustado neste arquivo. • `static/js/core.js` : este script captura o resultado formatado da rota `/data` do servidor Flask e usa o Plotly para criar visualizações. Você pode adicionar ou atualizar os gráficos da página.	Desenvolvedor web

(Opcional) Implante o aplicativo atualizado

Tarefa	Descrição	Habilidades necessárias
Atualize o arquivo de requisitos do seu aplicativo.	Antes de enviar alterações para o Elastic Beanstalk, atualize o arquivo `requirements.txt` para refletir quaisquer novos módulos do	Desenvolvedor de Python

Tarefa	Descrição	Habilidades necessárias
	Python executando o seguinte comando no diretório raiz do seu aplicativo: `pip freeze > requirements.txt`	
Configure o ambiente do Elastic Beanstalk.	Para garantir que as alterações do seu aplicativo sejam refletidas na implantação do Elastic Beanstalk, navegue até o diretório raiz do seu aplicativo e execute o seguinte comando: `eb deploy` Essa ação envia a versão mais recente do código do aplicativo para sua implantação existente do Elastic Beanstalk.	Administrador de sistemas, arquiteto

Recursos relacionados

- Chame um endpoint SageMaker modelo da Amazon usando o Amazon API Gateway e o AWS Lambda
- Implantar uma aplicação Flask no Elastic Beanstalk
- Referência de comandos da EB CLI
- Configurar seu ambiente de desenvolvimento Python

Mais informações

Lista de solução de problemas

Veja a seguir seis erros comuns e suas soluções.

Erro 1

```
Unable to assume role "arn:aws:iam::xxxxxxxxxx:role/aws-elasticbeanstalk-ec2-role".
 Verify that the role exists and is configured correctly.
```

Solução: se esse erro ocorrer durante a execução de `eb create`, crie um aplicativo de amostra no console do Elastic Beanstalk para desenvolver o perfil de instância padrão. Para obter mais informações a respeito, consulte Criação de um ambiente do Elastic Beanstalk na documentação do AWS Elastic Beanstalk.

Erro 2

```
Your WSGIPath refers to a file that does not exist.
```

Solução: esse erro ocorre nos logs de implantação porque o Elastic Beanstalk espera que o código do Flask seja nomeado como `application.py`. Se você escolher um nome diferente, execute `eb config` e edite o WSGIPath conforme mostrado no exemplo de código a seguir:

```
aws:elasticbeanstalk:container:python:
     NumProcesses: '1'
     NumThreads: '15'
     StaticFiles: /static/=static/
     WSGIPath: application.py
```

Certifique-se de substituir `application.py` pelo nome do seu arquivo.

Você também pode utilizar o Gunicorn e um Procfile. Para obter mais informações sobre essa abordagem, consulte Configuração do servidor WSGI com um Procfile na documentação do AWS Elastic Beanstalk.

Erro 3

```
Target WSGI script '/opt/python/current/app/application.py' does not contain WSGI
 application 'application'.
```

Solução: o Elastic Beanstalk espera que a variável que representa seu aplicativo Flask seja nomeada como `application`. Certifique-se de que o arquivo `application.py` use `application` como nome da variável:

```
application = Flask(__name__)
```

Erro 4

```
The EB CLI cannot find your SSH key file for keyname
```

Solução: use o EB CLI para especificar qual par de chaves usar ou para criar um par de chaves para as instâncias da EC2 sua implantação. Para resolver o erro, execute `eb init -i` e uma das opções perguntará:

```
Do you want to set up SSH for your instances?
```

Responda com Y para criar um par de chaves ou especificar um par de chaves existente.

Erro 5

Eu atualizei e reimplantei meu código, mas minha implantação não está refletindo minhas alterações.

Solução: se você estiver usando um repositório Git com sua implantação, certifique-se de adicionar e confirmar suas alterações antes da reimplantação.

Erro 6

Você está visualizando o aplicativo Flask a partir de um IDE do AWS Cloud9 e se depara com erros.

Solução: para obter mais informações a respeito, consulte Visualização de aplicativos em execução no IDE do AWS Cloud9 na documentação do AWS Cloud9.

Usar o Amazon Comprehend para processamento de linguagem natural

Ao optar pelo Amazon Comprehend, você pode detectar entidades personalizadas em documentos de texto individuais executando análises em tempo real ou tarefas em lotes assíncronos. O Amazon Comprehend também permite que você treine modelos personalizados de reconhecimento de entidades e de classificação de texto que podem ser usados em tempo real criando um endpoint.

Esse padrão usa tarefas em lotes assíncronos para detectar sentimentos e entidades a partir de um arquivo de entrada que contém vários documentos. O aplicativo de amostra fornecido por esse padrão foi projetado para que os usuários façam upload de um arquivo .csv contendo uma única coluna com um documento de texto por linha. O `comprehend_helper.py` arquivo nos resultados

do modelo GitHub Visualize AI/ML usando o Flask e o repositório AWS Elastic Beanstalk lê o arquivo de entrada e envia a entrada para o Amazon Comprehend para processamento.

BatchDetectEntities

O Amazon Comprehend inspeciona o texto de um lote de documentos em busca de entidades nomeadas e retorna a entidade detectada, a localização, o tipo de entidade e uma pontuação que indica o nível de confiança do Amazon Comprehend. No máximo 25 documentos podem ser enviados em uma chamada de API, sendo que cada documento deve ter até 5.000 bytes. Você pode filtrar os resultados para mostrar somente determinadas entidades com base no caso de uso. Por exemplo, você pode ignorar o tipo de entidade `'quantity'` e definir uma pontuação limite para a entidade detectada (por exemplo, 0,75). Recomendamos que você explore os resultados para seu caso de uso específico antes de escolher um valor limite. Para obter mais informações sobre isso, consulte a BatchDetectEntitiesdocumentação do Amazon Comprehend.

BatchDetectSentiment

O Amazon Comprehend inspeciona um lote de documentos recebidos e retorna o sentimento predominante de cada documento (`POSITIVE`, `NEUTRAL`, `MIXED` ou `NEGATIVE`). No máximo 25 documentos podem ser enviados em uma chamada de API, sendo que cada documento deve ter até 5.000 bytes. Analisar o sentimento é simples e você escolhe o sentimento com a pontuação mais alta para ser exibido nos resultados finais. Para obter mais informações sobre isso, consulte a BatchDetectSentimentdocumentação do Amazon Comprehend.

Processamento de configuração do Flask

Os servidores Flask usam uma série de variáveis de configuração para controlar sua execução. Essas variáveis podem conter resultados de depuração, tokens de sessão ou outras configurações do aplicativo. Também é possível definir variáveis personalizadas que podem ser acessadas enquanto o aplicativo está em execução. Há várias abordagens para definir variáveis de configuração.

Nesse padrão, a configuração é definida em `config.py` e herdada em `application.py`.

- **Note**

  `config.py` contém as variáveis de configuração definidas no startup do aplicativo. Nesse aplicativo, uma variável `DEBUG` é definida para instruir o aplicativo a executar o servidor no

modo de depuração. : o modo de depuração não deve ser usado ao executar um aplicativo em um ambiente de produção. `UPLOAD_FOLDER`é uma variável personalizada que é definida para ser referenciada posteriormente no aplicativo e informá-la onde os dados do usuário enviados devem ser armazenados.

- `application.py` inicia o aplicativo Flask e herda as configurações definidas em `config.py`. Isso é realizado pelo seguinte código:

```
application = Flask(__name__)
application.config.from_pyfile('config.py')
```

Mais padrões

- Automatize as operações de AWS infraestrutura usando o Amazon Bedrock
- Implemente uma ChatOps solução para gerenciar os resultados do escaneamento SAST usando o Amazon Q Developer em aplicativos de bate-papo, ações personalizadas e AWS CloudFormation
- Gere insights de dados usando o AWS Mainframe Modernization e o Amazon Q em QuickSight
- Gere insights de dados do Db2 z/OS usando o AWS Mainframe Modernization Amazon Q em QuickSight
- Conceda às instâncias do SageMaker notebook acesso temporário a um CodeCommit repositório em outra conta da AWS
- Gerencie AWS Organizations políticas como código usando o AWS CodePipeline Amazon Bedrock
- Migre o ML Crie, treine e implante cargas de trabalho para a Amazon SageMaker usando as ferramentas do desenvolvedor da AWS
- Modernize o aplicativo de CardDemo mainframe usando AWS Transform
- Execute análises avançadas usando o Amazon Redshift ML
- Simplifique o desenvolvimento e a implantação de bots do Amazon Lex usando um fluxo de trabalho automatizado
- Solucione problemas de estados AWS Step Functions usando o Amazon Bedrock

Analytics

Tópicos

- Analisar dados do Amazon Redshift no Microsoft SQL Server Analysis Services
- Analise e visualize dados JSON aninhados com o Amazon Athena e o Amazon QuickSight
- Automatize a ingestão de dados a partir do Amazon AWS Data Exchange S3
- Automatize a aplicação da criptografia no AWS Glue usando um modelo da AWS CloudFormation
- Crie um pipeline de dados para ingerir, transformar e analisar dados do Google Analytics usando o AWS DataOps Development Kit
- Crie um pipeline de processamento de vídeo usando o Amazon Kinesis Video Streams e o AWS Fargate
- Criar um pipeline de serviços de ETL para carregar dados incrementalmente do Amazon S3 ao Amazon Redshift usando o AWS Glue
- Crie uma malha de dados corporativa com a Amazon DataZone, AWS CDK, e AWS CloudFormation
- Calcule o value at risk (VaR – valor em risco) usando os serviços da AWS
- Configurar o acesso entre contas para um Catálogo de Dados do AWS Glue compartilhado usando o Amazon Athena
- Converta o atributo temporal Teradata NORMALIZE em Amazon Redshift SQL
- Converter o atributo Teradata RESET WHEN para Amazon Redshift SQL
- Implante e gerencie um data lake de tecnologia sem servidor na Nuvem AWS usando a infraestrutura como código
- Imponha a marcação dos clusters do Amazon EMR no lançamento
- Garanta que o registro do Amazon EMR no Amazon S3 esteja habilitado no lançamento
- Gerar dados de teste usando um trabalho do AWS Glue e Python
- Ingerir dados de IoT de forma econômica diretamente no Amazon S3 usando o AWS IoT Greengrass
- Executar uma tarefa do Spark em um cluster EMR transitório usando uma função do Lambda
- Migre cargas de trabalho do Apache Cassandra para o Amazon Keyspaces usando o AWS Glue
- Migre dados do Hadoop para o Amazon S3 usando o Migrator WANdisco LiveData
- Migrar o Oracle Business Intelligence 12c para a Nuvem AWS a partir de servidores on-premises

- Migre um cluster Apache Kafka local para o Amazon MSK usando MirrorMaker
- Migre um pilha ELK para a Nuvem Elastic na AWS
- Migre dados para o Nuvem AWS usando o Starburst
- Otimize a ingestão de ETL do tamanho do arquivo de entrada na AWS
- Orquestre um pipeline de ETL com validação, transformação e particionamento usando o AWS Step Functions
- Execute análises avançadas usando o Amazon Redshift ML
- Consulte tabelas do Amazon DynamoDB com SQL usando o Amazon Athena
- Acesse, consulte e una tabelas do Amazon DynamoDB usando o Athena
- Configure um espaço de dados mínimo viável para compartilhar dados entre organizações
- Configure a classificação específica do idioma para os resultados da consulta do Amazon Redshift usando uma UDF escalar do Python
- Assine uma função do Lambda para notificações de eventos de buckets do S3 em diferentes regiões da AWS
- Três tipos de trabalho de ETL do AWS Glue para converter dados em Apache Parquet
- Visualize os logs de auditoria do Amazon Redshift usando o Amazon Athena e o Amazon QuickSight
- Visualize relatórios de credenciais do IAM para todas as contas da AWS usando a Amazon QuickSight
- Mais padrões

Analisar dados do Amazon Redshift no Microsoft SQL Server Analysis Services

Criado por Sunil Vora (AWS)

Resumo

Esse padrão descreve como conectar e analisar dados do Amazon Redshift no Microsoft SQL Server Analysis Services, usando o Intellisoft OLE DB Provider ou o CData ADO.NET Provider para acesso ao banco de dados.

O Amazon Redshift é um serviço de data warehouse totalmente gerenciado e em escala de petabytes na Nuvem . O SQL Server Analysis Services é uma ferramenta de processamento analítico on-line (OLAP) que você pode usar para analisar dados de data marts e data warehouses, como o Amazon Redshift. Você pode usar o SQL Server Analysis Services para criar cubos OLAP a partir de seus dados para uma análise de dados rápida e avançada.

Pré-requisitos e limitações

Suposições

- Esse padrão descreve como configurar o SQL Server Analysis Services e o Intellisoft OLE DB Provider ou CData ADO.NET Provider para o Amazon Redshift em uma instância do Amazon Elastic Compute Cloud (Amazon). EC2 Como alternativa, você pode instalar ambos em um host em seu datacenter corporativo.

Pré-requisitos

- Uma conta AWS ativa
- Um cluster do Amazon Redshift com credenciais

Arquitetura

Pilha de tecnologia de origem

- Um cluster do Amazon Redshift

Pilha de tecnologias de destino

- Microsoft SQL Server Analysis Services

Arquitetura de origem e destino

Ferramentas

- Microsoft Visual Studio 2019 (Community Edition)
- Intellisoft OLE DB Provider para Amazon Redshift (teste) CData ou ADO.NET Provider para Amazon Redshift (teste)

Épicos

Analisar tabelas

Tarefa	Descrição	Habilidades necessárias
Analise as tabelas e os dados a serem importados.	Identifique as tabelas do Amazon Redshift a serem importadas e seus tamanhos.	DBA

Configurar a EC2 instância e instalar ferramentas

Tarefa	Descrição	Habilidades necessárias
Configure uma EC2 instância.	Na sua conta da AWS, crie uma EC2 instância em uma sub-rede pública ou privada.	Administrador de sistemas
Instale ferramentas para acesso ao banco de dados.	Baixe e instale o Intelliso ft OLE DB Provider para Amazon Redshift (CData ou ADO.NET Provider para Amazon Redshift).	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Instale o Visual Studio.	Baixe e instale o Visual Studio 2019 (Community Edition).	Administrador de sistemas
Iniciar as extensões.	Instale a extensão Microsoft Analysis Services Projects no Visual Studio.	Administrador de sistemas
Crie um projeto.	Crie um novo projeto de modelo tabular no Visual Studio para armazenar seus dados do Amazon Redshift. No Visual Studio, escolha a opção Projeto tabular do Analysis Services ao criar seu projeto.	DBA

Criar fonte de dados e importar tabelas

Tarefa	Descrição	Habilidades necessárias
Crie uma fonte de dados do Amazon Redshift.	Crie uma fonte de dados do Amazon Redshift usando o Intellisoft OLE DB Provider para Amazon Redshift (ou ADO.NET CData Provider para Amazon Redshift) e suas credenciais do Amazon Redshift.	Amazon Redshift, DBA
Importar tabelas.	Selecione e importe tabelas e visualizações do Amazon Redshift para seu projeto do SQL Server Analysis Services.	Amazon Redshift, DBA

Limpar após a migração

Tarefa	Descrição	Habilidades necessárias
Exclua a EC2 instância.	Exclua a EC2 instância que você executou anteriormente.	Administrador de sistemas

Recursos relacionados

- Amazon Redshift (documentação do AWS)
- Instalar o SQL Server Analysis Services (documentação da Microsoft)
- Designer de modelo tabular (documentação da Microsoft)
- Visão geral dos cubos OLAP para análises avançadas (documentação da Microsoft)
- Microsoft Visual Studio 2019 (Community Edition)
- Intellisoft OLE DB Provider para Amazon Redshift (teste)
- CData Provedor ADO.NET para Amazon Redshift (teste)

Analise e visualize dados JSON aninhados com o Amazon Athena e o Amazon QuickSight

Criado por Anoop Singh (AWS)

Resumo

Esse padrão explica como traduzir uma estrutura de dados aninhada e formatada em JSON em uma visualização tabular usando o Amazon Athena e, em seguida, visualizar os dados na Amazon. QuickSight

Você pode usar dados formatados em JSON para feeds de dados alimentados por API de sistemas operacionais para criar produtos de dados. Esses dados também podem ajudar você a entender melhor seus clientes e suas interações com seus produtos, para que você possa personalizar as experiências do usuário e prever resultados.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um arquivo JSON que representa uma estrutura de dados aninhada (esse padrão fornece um arquivo de amostra)

Limitações:

- Os recursos JSON se integram bem às funções orientadas a SQL existentes no Athena. No entanto, eles não são compatíveis com ANSI SQL, e espera-se que o arquivo JSON carregue cada registro em uma linha separada. Talvez seja necessário usar a `ignore.malformed.json` propriedade no Athena para indicar se registros JSON malformados devem ser transformados em caracteres nulos ou gerar erros. Para obter mais informações, consulte Práticas recomendadas para leitura de dados JSON na documentação do Athena.
- Esse padrão considera somente quantidades simples e pequenas de dados formatados em JSON. Se você quiser usar esses conceitos em grande escala, considere aplicar o particionamento de dados e consolidar seus dados em arquivos maiores.

Arquitetura

O diagrama a seguir mostra a arquitetura e o fluxo de trabalho desse padrão. As estruturas de dados aninhadas são armazenadas no Amazon Simple Storage Service (Amazon S3) no formato JSON. No Athena, os dados JSON são mapeados para uma estrutura de dados do Athena. Em seguida, você cria uma visualização para analisar os dados e visualizar a estrutura de dados em QuickSight.

Ferramentas

Serviços da AWS

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados. Esse padrão usa o Amazon S3 para armazenar o arquivo JSON.
- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão. Esse padrão usa o Athena para consultar e transformar os dados JSON. Com algumas ações no AWS Management Console, você pode direcionar o Athena para seus dados no Amazon S3 e usar o SQL padrão para executar consultas únicas. O Athena não tem servidor, portanto, não há infraestrutura para configurar ou gerenciar, e você paga somente pelas consultas que executa. O Athena escala automaticamente e executa consultas em paralelo, para que os resultados sejam rápidos, mesmo com grandes conjuntos de dados e consultas complexas.
- QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel. QuickSight permite criar e publicar facilmente painéis interativos que incluem insights de aprendizado de máquina (ML). Você pode acessar esses painéis de qualquer dispositivo e incorporá-los aos seus aplicativos, portais e sites.

Código de exemplo

O arquivo JSON a seguir fornece uma estrutura de dados aninhada que você pode usar nesse padrão.

```
{
  "symbol": "AAPL",
  "financials": [
    {
```

```
      "reportDate": "2017-03-31",
      "grossProfit": 20591000000,
      "costOfRevenue": 32305000000,
      "operatingRevenue": 52896000000,
      "totalRevenue": 52896000000,
      "operatingIncome": 14097000000,
      "netIncome": 11029000000,
      "researchAndDevelopment": 2776000000,
      "operatingExpense": 6494000000,
      "currentAssets": 101990000000,
      "totalAssets": 334532000000,
      "totalLiabilities": 200450000000,
      "currentCash": 15157000000,
      "currentDebt": 13991000000,
      "totalCash": 67101000000,
      "totalDebt": 98522000000,
      "shareholderEquity": 134082000000,
      "cashChange": -1214000000,
      "cashFlow": 12523000000,
      "operatingGainsLosses": null
    }
  ]
}
```

Épicos

Configurar um bucket S3

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Para criar um bucket para armazenar o arquivo JSON, faça login no AWS Management Console, abra o console do Amazon S3 e escolha Create bucket. Para obter mais informações, consulte Criar um bucket na documentação do Amazon S3.	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Adicione os dados JSON aninhados.	Faça upload do seu arquivo JSON para o bucket do S3. Para ver um exemplo de arquivo JSON, consulte a seção anterior. Para obter instruções, consulte Fazer uploads de objetos na documentação do Amazon S3.	Administrador de sistemas

Analise dados no Athena

Tarefa	Descrição	Habilidades necessárias
Crie uma tabela para mapear os dados JSON.	1. Abra o console do Athena. 2. Crie um banco de dados seguindo as instruções na documentação do Athena. 3. No menu Banco de dados, escolha o banco de dados que você criou. 4. No editor de consultas , insira uma `CREATE TABLE` declaração como a seguinte: `CREATE EXTERNAL TABLE financials_json ( symbol string, financials array< struct<reportdate: string, grossprofit: bigint, totalrevenue: bigint,`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias

	<pre>totalcash
	: bigint,
	totaldebt
	: bigint,
	researcha
	nddevelopment:
	bigint>>
	)
	ROW FORMAT SERDE
	'org.openx.data.js
	onserde.JsonSerDe'
	LOCATION 's3://s3b
	ucket-for-athena/'</pre> onde `LOCATION` especifica a localização do bucket do S3 que contém o arquivo JSON.
	5. Escolha Executar para criar a tabela.
	
	Para obter mais informações sobre a criação de tabelas, consulte a documentação do Athena.	

Tarefa	Descrição	Habilidades necessárias
Crie uma visualização para análise de dados.	1. Abra o console do Athena. 2. Crie um banco de dados seguindo as instruções na documentação do Athena. 3. No menu Banco de dados, escolha o banco de dados que você criou. 4. No editor de consultas , insira uma `CREATE VIEW` declaração como a seguinte: `CREATE OR REPLACE VIEW financial_json_view AS SELECT symbol, financials[1].reportdate one_report_date, -- indexes start with 1 financials[1].totalrevenue one_total_revenue, financials[1].reportdate another_report_date, financials[1].totalrevenue another_total_revenue FROM financials_json where symbol='AAPL' ORDER BY 1` 5. Selecione Run (Executar) para criar a visualização.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações sobre a criação de visualizações, consulte a documentação do Athena.	
Analise e valide os dados.	1. Abra o console do Athena. 2. No editor de consultas, execute consultas usando a exibição que você criou na etapa anterior. 3. Valide os dados em relação ao arquivo JSON para confirmar se os nomes das colunas e os tipos de dados estão mapeados corretamente.	Desenvolvedor

Visualize dados em QuickSight

Tarefa	Descrição	Habilidades necessárias
Configure o Athena como fonte de dados em. QuickSight	1. Abra o console de QuickSight . 2. Escolha Conjuntos de dados, Novo conjunto de dados. 3. Escolha Athena como fonte de dados. 4. Escolha o banco de dados que inclui a exibição que você criou.	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	5. Escolha a visualização para a qual você deseja criar um conjunto de dados. 6. Na página Concluir criação do conjunto de dados, escolha Consultar diretamente seus dados. 7. Escolha Visualize.	
Visualize dados em QuickSight.	1. Depois de visualizar o conjunto de dados, escolha as imagens no painel esquerdo e escolha os campos para o conjunto de dados. Para obter mais informações, consulte o tutorial na QuickSight documentação. 2. Salve as alterações na análise. 3. Escolha Publicar painel para publicar os elementos visuais que você criou.	Analista de dados

Recursos relacionados

- Documentação do Amazon Athena
- QuickSight Tutoriais da Amazon
- Trabalhando com JSON aninhado (postagem no blog)

Automatize a ingestão de dados a partir do Amazon AWS Data Exchange S3

Criado por Adnan Alvee (AWS) e Manikanta Gona (AWS)

Resumo

Esse padrão fornece um AWS CloudFormation modelo que permite que você consuma automaticamente dados do AWS Data Exchange seu data lake no Amazon Simple Storage Service (Amazon S3).

AWS Data Exchange é um serviço que facilita a troca segura de conjuntos de dados baseados em arquivos na nuvem da AWS. AWS Data Exchange os conjuntos de dados são baseados em assinatura. Como assinante, você também pode acessar as revisões do conjunto de dados à medida que os provedores publicam novos dados.

O AWS CloudFormation modelo cria um evento no Amazon CloudWatch Events e uma AWS Lambda função. O evento observa todas as atualizações do conjunto de dados no qual você se inscreveu. Se houver uma atualização, CloudWatch inicia uma função Lambda, que copia os dados para o bucket do S3 que você especificar. Quando os dados forem copiados com sucesso, o Lambda enviará uma notificação enviada pelo Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Assinatura de um conjunto de dados em AWS Data Exchange

Limitações

- O AWS CloudFormation modelo deve ser implantado separadamente para cada conjunto de dados inscrito em. AWS Data Exchange

Arquitetura

Pilha de tecnologias de destino

- AWS Lambda
- Amazon S3
- AWS Data Exchange
- Amazon CloudWatch
- Amazon SNS

Arquitetura de destino

Automação e escala

Você pode usar o AWS CloudFormation modelo várias vezes para os conjuntos de dados que deseja ingerir no data lake.

Ferramentas

- AWS Data Exchangefacilita que os AWS clientes troquem com segurança conjuntos de dados baseados em arquivos no. Nuvem AWS Como assinante, você pode encontrar e assinar centenas de produtos de provedores de dados qualificados. Em seguida, você pode baixar rapidamente o conjunto de dados ou copiá-lo para o Amazon S3 para uso em uma variedade de serviços de AWS análise e aprendizado de máquina. Qualquer pessoa com um Conta da AWS pode ser AWS Data Exchange assinante.
- O AWS Lambda permite que você execute código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga somente pelo tempo de computação utilizado; não há cobrança quando seu código não está em execução. Com o Lambda, você pode executar código para praticamente qualquer tipo de aplicativo ou serviço de back-end sem nenhuma administração. O Lambda executa seu código em uma infraestrutura computacional de alta disponibilidade e gerencia todos os recursos computacionais, incluindo manutenção do servidor e do sistema operacional, provisionamento de capacidade e escalabilidade automática, monitoramento de código e registro.
- O Amazon S3 fornece armazenamento para a Internet. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.
- A Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. Usando regras simples que você pode configurar

rapidamente, você pode combinar eventos e roteá-los para uma ou mais funções ou fluxos de destino. CloudWatch Os eventos ficam cientes das mudanças operacionais à medida que elas ocorrem. Ele responde a essas alterações operacionais e executa a ação corretiva conforme necessário, enviando mensagens para responder ao ambiente, ativando funções, fazendo alterações e capturando informações de estado. Você também pode usar CloudWatch Eventos para programar ações automatizadas que se iniciam automaticamente em determinados momentos usando expressões cron ou rate.

- O Amazon Simple Notification Service (Amazon SNS) permite que aplicativos, usuários finais e dispositivos enviem e recebam instantaneamente notificações da nuvem. O Amazon SNS fornece tópicos (canais de comunicação) para mensagens de alta taxa de transferência, baseadas em push. many-to-many Usando tópicos do Amazon SNS, os editores podem distribuir mensagens para um grande número de assinantes para processamento paralelo, incluindo filas do Amazon Simple Queue Service (Amazon SQS), funções Lambda e webhooks HTTP/S. Também é possível usar o Amazon SNS para enviar notificações para usuários finais usando push móvel, SMS e e-mail.

Épicos

Inscrever-se em um conjunto de dados

Tarefa	Descrição	Habilidades necessárias
Assine um conjunto de dados	No AWS Data Exchange console, assine um conjunto de dados. Para obter instruções, consulte Assinatura de produtos de dados AWS Data Exchange na AWS documentação.	AWS geral
Observe os atributos do conjunto de dados.	Anote Região da AWS o ID e o ID da revisão do conjunto de dados. Você precisará disso para o AWS CloudFormation modelo na próxima etapa.	AWS geral

Implante o AWS CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Crie um bucket e uma pasta no S3.	Se você já tiver um data lake no Amazon S3, crie uma pasta para armazenar os dados a serem ingeridos. AWS Data Exchange Se você estiver implantando o modelo para fins de teste, crie um novo bucket do S3 e anote o nome do bucket e o prefixo da pasta para a próxima etapa.	AWS geral
Implante o AWS CloudFormation modelo.	Implante o AWS CloudFormation modelo fornecido como anexo a esse padrão. Para obter instruções, consulte a AWS CloudFormation documentação. Configure os seguintes parâmetros para corresponder às suas configurações Conta da AWS, do conjunto de dados e do bucket do S3: conjunto de dados Região da AWS, ID do conjunto de dados, ID da revisão, nome do bucket do S3 (por exemplo,**DOC-EXAMPLE-BUCKET**), prefixo da pasta (por exemplo,**myfolder/**) e e-mail para notificação do SNS. Você pode definir o parâmetro Nome do conjunto	AWS geral

Tarefa	Descrição	Habilidades necessárias
	de dados como qualquer nome. Quando você implanta o modelo, ele executa uma função do Lambda para ingerir automaticamente o primeiro conjunto de dados disponíve l no conjunto de dados. A ingestão subsequente ocorre automaticamente, à medida que novos dados chegam ao conjunto de dados.	

Recursos relacionados

- Assinatura de produtos de dados em AWS Data Exchange (AWS Data Exchange documentação)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Automatize a aplicação da criptografia no AWS Glue usando um modelo da AWS CloudFormation

Criado por Diogo Guedes (AWS)

Resumo

Esse padrão mostra como configurar e automatizar a aplicação da criptografia no AWS Glue usando um CloudFormation modelo da AWS. O modelo cria todas as configurações e recursos necessários para aplicar a criptografia. Esses recursos incluem uma configuração inicial, um controle preventivo criado por uma EventBridge regra da Amazon e uma função do AWS Lambda.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões para implantar o CloudFormation modelo e seus recursos

Limitações

Esse controle de segurança é regional. Você deve implementar o controle de segurança em cada região da AWS em que deseja configurar a aplicação da criptografia no AWS Glue.

Arquitetura

Pilha de tecnologias de destino

- Amazon CloudWatch Logs (do AWS Lambda)
- EventBridge Regra da Amazon
- Pilha da AWS CloudFormation
- AWS CloudTrail
- Perfil e política gerenciada do AWS do perfil do Identity and Access Management (IAM)
- AWS Key Management Service (AWS KMS)
- AWS KMS: alias
- Função do AWS Lambda
- AWS Systems Manager Parameter Store

Arquitetura de destino

O diagrama a seguir mostra como automatizar a aplicação da criptografia no AWS Glue.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um CloudFormation modelo cria todos os recursos, incluindo a configuração inicial e o controle de detetive para a aplicação da criptografia no AWS Glue.
2. Uma EventBridge regra detecta uma alteração de estado na configuração de criptografia.
3. Uma função Lambda é invocada para avaliação e registro por meio de registros. CloudWatch Para uma detecção não compatível, o Parameter Store é recuperado com um nome de recurso da nome do recurso da Amazon (ARN) (ARN) para uma chave do AWS KMS. O serviço é corrigido para o status compatível com a criptografia ativada.

Automação e escala

Se você estiver usando o AWS Organizations, poderá usar CloudFormation StackSets a AWS para implantar esse modelo em várias contas nas quais deseja habilitar a aplicação da criptografia no AWS Glue.

Ferramentas

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, funções do Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras contas da AWS.
- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- CloudTrailA AWS ajuda você a viabilizar a auditoria operacional e de risco, a governança e a conformidade da sua conta da AWS.
- O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.

- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Systems Manager ajuda você a gerenciar seus aplicativos e infraestrutura em execução na nuvem AWS. Isso simplifica o gerenciamento de aplicações e recursos, diminui o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus recursos da AWS de modo seguro e em grande escala.

Código

O código desse padrão está disponível no repositório GitHub aws-custom-guardrail-eventcontrolado.

Práticas recomendadas

O AWS Glue oferece suporte à criptografia de dados em repouso para trabalhos de criação no AWS Glue e desenvolvimento de scripts usando endpoints de desenvolvimento.

Considere as seguintes práticas recomendadas:

- Você pode configurar trabalhos de ETL e endpoints de desenvolvimento para usar chaves do AWS KMS para gravar dados criptografados em repouso.
- Criptografe os metadados armazenados no Catálogo de Dados do AWS Glue usando chaves que você gerencia por meio do AWS KMS.
- Além disso, você pode usar a chave do AWS KMS para criptografar marcadores de trabalho e os logs gerados pelos crawlers e trabalhos de ETL.

Épicos

Inicie o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	Baixe o `aws-custom-guardrail-event-`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`driven.yaml` modelo do GitHub repositório e, em seguida, implante o modelo. O `CREATE_COMPLETE` status indica que seu modelo foi implantado com sucesso. **Note** O modelo não requer parâmetros de entrada.	

Verifique as configurações de criptografia no AWS Glue

Tarefa	Descrição	Habilidades necessárias
Verifique as configurações das chaves do AWS KMS.	1. Faça login no Console de Gerenciamento da AWS e abra o Console do AWS Glue. 2. No painel de navegação , em Catálogo de dados, escolha Configurações do catálogo. 3. Verifique se as configurações de criptografia de metadados e Criptografar senhas de conexão estão sinalizadas e configuradas para uso. `KMSKeyGlue`	Arquiteto de nuvem

Teste a aplicação da criptografia

Tarefa	Descrição	Habilidades necessárias
Identifique a configuração de criptografia em CloudFormation.	1. Faça login no AWS Management Console e, em seguida, abra o CloudFormation console. 2. No painel de navegação, escolha Stacks (Pilhas) e escolha a pilha desejada. 3. Escolha a guia Recursos. 4. Na tabela Recursos, encontre a configuração de criptografia por ID lógica.	Arquiteto de nuvem
Mude a infraestrutura provisionada para um estado incompatível.	1. Faça login no Console de Gerenciamento da AWS e abra o Console do AWS Glue. 2. No painel de navegação, em Catálogo de dados, escolha Configurações do catálogo. 3. Desmarque a caixa de seleção Criptografia de metadados. 4. Desmarque a caixa de seleção Criptografar senhas de conexão. 5. Escolha Salvar. 6. Atualize o console do AWS Glue.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	A barreira de proteção detecta o estado de inconformidade no AWS Glue depois que você desmarca as caixas de seleção e, em seguida, impõe a conformidade ao corrigir automaticamente a configuração incorreta da criptografia. Como resultado, as caixas de seleção de criptografia devem ser marcadas novamente após a atualização da página.	

Recursos relacionados

- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS (documentação da CloudTrail Amazon CloudWatch)
- Configuração da criptografia no AWS Glue (documentação do AWS Glue)

Crie um pipeline de dados para ingerir, transformar e analisar dados do Google Analytics usando o AWS DataOps Development Kit

Criado por Anton Kukushkin (AWS) e Rudy Puig (AWS)

Resumo

Esse padrão descreve como criar um pipeline de dados para ingerir, transformar e analisar dados do Google Analytics usando o AWS DataOps Development Kit (AWS DDK) e outros. Serviços da AWS O AWS DDK é uma estrutura de desenvolvimento de código aberto que ajuda você a criar fluxos de trabalho de dados e uma arquitetura de dados moderna. AWS Um dos principais objetivos do AWS DDK é economizar o tempo e o esforço normalmente dedicados às tarefas trabalhosas do pipeline de dados, como orquestrar pipelines, criar infraestrutura e criar a base dessa infraestrutura. DevOps Você pode transferir essas tarefas trabalhosas para o AWS DDK para se concentrar em escrever código e outras atividades de alto valor.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um AppFlow conector Amazon para o Google Analytics, configurado
- Python e pip (gerenciador de pacotes do Python)
- Git, instalado e configurado
- AWS Command Line Interface (AWS CLI), instalado e configurado
- AWS Cloud Development Kit (AWS CDK), instalado

Versões do produto

- Python 3.7 ou superior
- pip 9.0.3 ou superior

Arquitetura

Pilha de tecnologia

- Amazon AppFlow
- Amazon Athena
- Amazon CloudWatch
- Amazon EventBridge
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Queue Service (Amazon SQS)
- AWS DataOps Kit de desenvolvimento (AWS DDK)
- AWS Lambda

Arquitetura de destino

O diagrama a seguir mostra o processo orientado por eventos que ingere, transforma e analisa os dados do Google Analytics.

O diagrama mostra o seguinte fluxo de trabalho:

1. Uma regra de evento CloudWatch agendado da Amazon invoca a Amazon. AppFlow
2. A Amazon AppFlow ingere dados do Google Analytics em um bucket do S3.
3. Depois que os dados são ingeridos pelo bucket do S3, as notificações de eventos EventBridge são geradas, capturadas por uma regra de CloudWatch eventos e, em seguida, colocadas em uma fila do Amazon SQS.
4. Uma função Lambda consome eventos da fila do Amazon SQS, lê os respectivos objetos do S3, transforma os objetos no formato Apache Parquet, grava os objetos transformados no bucket do S3 e, em seguida, cria ou atualiza a definição da tabela. AWS Glue Data Catalog
5. Uma consulta do Athena é executada na tabela.

Ferramentas

AWS ferramentas

- AppFlowA Amazon é um serviço de integração totalmente gerenciado que permite que você troque dados com segurança entre aplicativos de software como serviço (SaaS).
- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão.

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Cloud Development Kit (AWS CDK)é uma estrutura para definir a infraestrutura de nuvem em código e provisioná-la por meio dela. AWS CloudFormation
- AWS DataOps O Development Kit (AWS DDK) é uma estrutura de desenvolvimento de código aberto para ajudá-lo a criar fluxos de trabalho de dados e uma arquitetura de dados moderna. AWS

Código

O código desse padrão está disponível no GitHub AWS DataOps Development Kit (AWS DDK) e na análise de dados do Google Analytics com os repositórios Amazon AppFlow, Amazon Athena AWS DataOps e Development Kit.

Épicos

Prepare o ambiente

Tarefa	Descrição	Habilidades necessárias
Clone o código-fonte.	Para clonar o código-fonte, execute o seguinte comando:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/aws-samples/aws-ddk-examples.git`	
Crie um ambiente virtual.	Navegue até o diretório do código-fonte e execute o seguinte comando para criar um ambiente virtual: `cd google-analytics-data-using-appflow/python && python3 -m venv .venv`	DevOps engenheiro
Instale as dependências.	Para ativar o ambiente virtual e instalar as dependências, execute o seguinte comando: `source .venv/bin/activate && pip install -r requirements.txt`	DevOps engenheiro

Implante o aplicativo que usa seu pipeline de dados

Tarefa	Descrição	Habilidades necessárias
Faça o bootstrap do ambiente.	1. Confirme se o AWS CLI está configurado com credenciais válidas para o seu Conta da AWS. Para obter mais informações, consulte Usando perfis nomeados na AWS CLI documentação.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	2. Execute o comando `cdk bootstrap --profile [AWS_PROFILE] .`	
Implante os dados.	Para implantar o pipeline de dados, execute o comando `cdk deploy --profile [AWS_PROFILE] .`	DevOps engenheiro

Teste a implantação

Tarefa	Descrição	Habilidades necessárias
Valide o status da pilha.	1. Abra o console de AWS CloudFormation. 2. Na página Stacks, confirme se o status da pilha `DdkAppflowAthenaStack` é `CREATE_COMPLETE` .	DevOps engenheiro

Solução de problemas

Problema	Solução
A implantação falha durante a criação de um recurso `AWS::AppFlow::Flow` e você recebe o seguinte erro: `Connector Profile with name ga-connection does not exist`	Confirme se você criou um AppFlow conector Amazon para o Google Analytics e o nome`ga-connection` . Para obter instruções, consulte o Google Analytics na AppFlow documentação da Amazon.

Recursos relacionados

- AWS DataOps Kit de desenvolvimento (AWS DDK) (GitHub)
- AWS Exemplos de DDK () GitHub

Mais informações

AWS Os pipelines de dados do DDK são compostos por um ou vários estágios. Nos exemplos de código a seguir, você usa `AppFlowIngestionStage` para ingerir dados do Google Analytics, `SqsToLambdaStage` lidar com a transformação de dados e `AthenaSQLStage` para executar a consulta do Athena.

Primeiro, os estágios de transformação e ingestão de dados são criados, conforme mostra o exemplo de código a seguir:

```
        appflow_stage = AppFlowIngestionStage(
            self,
            id="appflow-stage",
            flow_name=flow.flow_name,
        )
        sqs_lambda_stage = SqsToLambdaStage(
            self,
            id="lambda-stage",
            lambda_function_props={
                "code": Code.from_asset("./ddk_app/lambda_handlers"),
                "handler": "handler.lambda_handler",
                "layers": [
                    LayerVersion.from_layer_version_arn(
                        self,
                        id="layer",
                        layer_version_arn=f"arn:aws:lambda:
{self.region}:336392948345:layer:AWSDataWrangler-Python39:1",
                    )
                ],
                "runtime": Runtime.PYTHON_3_9,
            },
        )
        # Grant lambda function S3 read & write permissions
        bucket.grant_read_write(sqs_lambda_stage.function)
        # Grant Glue database & table permissions
        sqs_lambda_stage.function.add_to_role_policy(
```

```
            self._get_glue_db_iam_policy(database_name=database.database_name)
        )
        athena_stage = AthenaSQLStage(
            self,
            id="athena-sql",
            query_string=[
                (
                    "SELECT year, month, day, device, count(user_count) as cnt "
                    f"FROM {database.database_name}.ga_sample "
                    "GROUP BY year, month, day, device "
                    "ORDER BY cnt DESC "
                    "LIMIT 10; "
                )
            ],
            output_location=Location(
                bucket_name=bucket.bucket_name, object_key="query-results/"
            ),
            additional_role_policy_statements=[
                self._get_glue_db_iam_policy(database_name=database.database_name)
            ],
        )
```

Em seguida, a `DataPipeline` construção é usada para “conectar” os estágios usando EventBridge regras, como mostra o exemplo de código a seguir:

```
        (
            DataPipeline(self, id="ingestion-pipeline")
            .add_stage(
                stage=appflow_stage,
                override_rule=Rule(
                    self,
                    "schedule-rule",
                    schedule=Schedule.rate(Duration.hours(1)),
                    targets=appflow_stage.targets,
                ),
            )
            .add_stage(
                stage=sqs_lambda_stage,
                # By default, AppFlowIngestionStage stage emits an event after the flow
run finishes successfully
                # Override rule below changes that behavior to call the the stage when
data lands in the bucket instead
                override_rule=Rule(
```

```
                self,
                "s3-object-created-rule",
                event_pattern=EventPattern(
                    source=["aws.s3"],
                    detail={
                        "bucket": {"name": [bucket.bucket_name]},
                        "object": {"key": [{"prefix": "ga-data"}]},
                    },
                    detail_type=["Object Created"],
                ),
                targets=sqs_lambda_stage.targets,
            ),
        )
        .add_stage(stage=athena_stage)
    )
```

Para ver mais exemplos de código, consulte o repositório GitHub Analisando dados do Google Analytics com Amazon AppFlow, Amazon Athena e AWS DataOps Development Kit.

Crie um pipeline de processamento de vídeo usando o Amazon Kinesis Video Streams e o AWS Fargate

Criado por Piotr Chotkowski (AWS) e Pushparaju Thangavel (AWS)

Resumo

Esse padrão demonstra como usar o Amazon Kinesis Video Streams e o AWS Fargate para extrair quadros de um stream de vídeo e armazená-los como arquivos de imagem para processamento adicional no Amazon Simple Storage Service (Amazon S3).

O padrão fornece um aplicativo de amostra na forma de um projeto Java Maven. Esse aplicativo define a infraestrutura da AWS usando o AWS Cloud Development Kit (AWS CDK). Tanto a lógica de processamento de quadros quanto as definições de infraestrutura são escritas na linguagem de programação Java. Você pode usar esse aplicativo de amostra como base para desenvolver seu próprio pipeline de processamento de vídeo em tempo real ou para criar a etapa de pré-processamento de vídeo de um pipeline de machine learning.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Java SE Development Kit (JDK) 11 instalado
- Apache Maven, instalado
- AWS Cloud Development Kit (AWS CDK), instalado
- AWS Command Line Interface (AWS CLI) versão 2, instalado
- Docker (necessário para criar imagens do Docker para usar nas definições de tarefas do AWS Fargate), instalado

Limitações

Esse padrão serve como uma prova de conceito ou como base para um maior desenvolvimento. Ele não deve ser usado na sua forma atual para implantações de produção.

Versões do produto

- Esse padrão foi testado com o AWS CDK versão 1.77.0 (consulte as versões do AWS CDK)
- JDK 11
- AWS CLI versão 2

Arquitetura

Pilha de tecnologias de destino

- Amazon Kinesis Video Streams
- Tarefa do AWS Fargate
- Fila do Amazon Simple Queue Service (Amazon SQS)
- Bucket do Amazon S3

Arquitetura de destino

O usuário cria um stream de vídeo do Kinesis, carrega um vídeo e envia uma mensagem JSON que contém detalhes sobre o stream de vídeo do Kinesis de entrada e o bucket S3 de saída para uma fila SQS. O AWS Fargate, que está executando o aplicativo principal em um contêiner, extrai a mensagem da fila do SQS e começa a extrair os quadros. Cada quadro é salvo em um arquivo de imagem e armazenado no bucket S3 de destino.

Automação e escala

O aplicativo de amostra pode escalar horizontal e verticalmente em uma única região da AWS. A escalabilidade horizontal pode ser alcançada aumentando o número de tarefas implantadas do AWS Fargate que são lidas da fila do SQS. O dimensionamento vertical pode ser obtido aumentando o número de segmentos de divisão de quadros e publicação de imagens no aplicativo. Essas configurações são passadas como variáveis de ambiente para o aplicativo na definição do QueueProcessingFargateServicerecurso no AWS CDK. Devido à natureza da implantação do AWS CDK stack, você pode implantar esse aplicativo em várias regiões e contas da AWS sem nenhum esforço adicional.

Ferramentas

Ferramentas

- O AWS CDK é uma estrutura de desenvolvimento de software para definir sua infraestrutura e seus recursos de nuvem usando linguagens de programação como TypeScript, Python JavaScript, Java e C#/.Net.
- O Amazon Kinesis Video Streams é um serviço da AWS totalmente gerenciado que você pode usar para fazer streaming de vídeos ao vivo de dispositivos para a Nuvem AWS ou criar aplicativos para processamento de vídeo em tempo real ou análise de vídeo orientada por lotes.
- O AWS Fargate é um mecanismo de computação de tecnologia sem servidor para contêineres. O Fargate elimina a necessidade de provisionar e gerenciar servidores e permite que você se concentre no desenvolvimento de seus aplicativos.
- O Amazon S3 é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e desempenho.
- O Amazon SQS é um serviço de filas de mensagens totalmente gerenciado que facilita o desacoplamento e a escala de microsserviços, sistemas distribuídos e aplicativos com tecnologia sem servidor.

Código

- Um arquivo .zip do projeto de aplicativo de amostra (`frame-splitter-code.zip`) está anexado.

Épicos

Implante a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Inicie o daemon do Docker.	Inicie o daemon do Docker em seu sistema local. O AWS CDK usa o Docker para criar a imagem que é usada na tarefa do AWS Fargate. Você deve executar o Docker antes de prosseguir para a próxima etapa.	Desenvolvedor, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Crie o projeto.	Baixe o aplicativo de amostra `frame-splitter-code` (anexado) e extraia seu conteúdo em uma pasta na sua máquina local. Antes de implantar a infraestrutura, você precisa criar o projeto Java Maven. Em um prompt de comando, navegue até o diretório raiz do projeto e crie o projeto executando o comando: `mvn clean install`	Desenvolvedor, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Faça o bootstrap do AWS CDK.	(Somente usuários iniciantes do AWS CDK) Se for a primeira vez que você usa o AWS CDK, talvez seja necessário fazer o bootstrap do ambiente executando o comando da AWS CLI: `cdk bootstrap --profile "$AWS_PROFILE_NAME"` onde `$AWS_PROFILE_NAME` contém o nome do perfil da AWS a partir de suas credenciais da AWS. Ou você pode remover esse parâmetro para usar o perfil padrão. Para obter mais informações, consulte a documentação do AWS CDK.	Desenvolvedor, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Implante a pilha de CDK da AWS.	Nesta etapa, você cria os recursos de infraestrutura necessários (fila SQS, bucket S3, definição de tarefa do AWS Fargate) em sua conta da AWS, cria a imagem do Docker necessária para a tarefa do AWS Fargate e implanta o aplicativo. Em um prompt de comando, navegue até o diretório raiz do projeto e execute o comando: `cdk deploy --profile "$AWS_PROFILE_NAME" --all` onde `$AWS_PROFILE_NAME` contém o nome do perfil da AWS a partir de suas credenciais da AWS. Ou você pode remover esse parâmetro para usar o perfil padrão. Confirme a implantação. Observe os valores QueueUrle o Bucket da saída de implantação do CDK; você precisará deles em etapas posteriores. O AWS CDK cria os ativos, os carrega na sua conta da AWS e cria todos os recursos de infraestrutura. Você pode observar o processo de criação de recursos no CloudFormation	Desenvolvedor, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	console da AWS. Para obter mais informações, consulte a CloudFormation documentação da AWS e a documentação do AWS CDK.	

Tarefa	Descrição	Habilidades necessárias
Crie um streaming de vídeo.	Nesta etapa, você cria um stream de vídeo do Kinesis que servirá como stream de entrada para processamento de vídeo. Certifique-se de que a AWS CLI esteja instalada e configurada. Na AWS CLI, execute: `aws kinesisvideo --profile "$AWS_PROFILE_NAME" create-stream --stream-name "$STREAM_NAME" --data-retention-in-hours "24"` onde `$AWS_PROFILE_NAME` contém o nome do perfil da AWS de suas credenciais da AWS (ou remove esse parâmetro para usar o perfil padrão) e `$STREAM_NAME` é qualquer nome de stream válido. Como alternativa, você pode criar um stream de vídeo usando o console do Kinesis seguindo as etapas na documentação do Kinesis Video Streams. Observe o nome de recurso da AWS (ARN) do stream criado; você precisará dele mais tarde.	Desenvolvedor, DevOps engenheiro

Execute um exemplo

Tarefa	Descrição	Habilidades necessárias
Faça o upload do vídeo para o stream.	Na pasta do projeto do aplicativo `frame-splitter-code` de amostra, abra o arquivo `ProcessingTaskTest.java` na pasta `src/test/java/amazon/awscdk/examples/splitter`. Substitua as variáveis `profileName` e `streamName` pelos valores que você usou nas etapas anteriores. Para fazer o upload do vídeo de exemplo para o stream de vídeo do Kinesis que você criou na etapa anterior, execute: `amazon.awscdk.examples.splitter.ProcessingTaskTest#testExample test` Como alternativa, você pode enviar seu vídeo usando um dos métodos descritos na documentação do Kinesis Video Streams.	Desenvolvedor, DevOps engenheiro
Inicie o processamento de vídeo.	Agora que você enviou um vídeo para o stream de vídeo do Kinesis, pode começar a processá-lo. Para iniciar	Desenvolvedor, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	a lógica de processamento, você precisa enviar uma mensagem com detalhes para a fila do SQS que o AWS CDK criou durante a implantação. Para enviar uma mensagem usando a AWS CLI, execute:
	
	`aws sqs --profile "$AWS_PROFILE_NAME" send-message --queue-url QUEUE_URL --message-body MESSAGE`
	
	where `$AWS_PROFILE_NAME` contém o nome do perfil da AWS a partir de suas credenciais da AWS (remova esse parâmetro para usar o perfil padrão), `QUEUE_URL` é o QueueUrlvalor da saída do AWS CDK e `MESSAGE` é uma string JSON no seguinte formato:
	
	`{ "streamARN": "STREAM_ARN", "bucket": "BUCKET_NAME", "s3Directory": "test-output" }`
	
	onde `STREAM_ARN` é o ARN do stream de vídeo que você criou em uma etapa anterior e `BUCKET_NAME` é o valor	

Tarefa	Descrição	Habilidades necessárias
	do Bucket da saída do AWS CDK. O envio dessa mensagem inicia o processamento do vídeo. Como alternativa, você pode enviar uma mensagem usando o console do Amazon SQS, conforme descrito na documentação do Amazon SQS.	
Visualize imagens dos quadros de vídeo.	Você pode ver as imagens resultantes no bucket de saída `s3://BUCKET_NAME/test-output` do S3, onde `BUCKET_NAME` está o valor do bucket da saída do AWS CDK.	Desenvolvedor, DevOps engenheiro

Recursos relacionados

- Documentação do AWS CDK
- Referência da API AWS CDK
- Workshop introdutório do AWS CDK
- Documentação do Amazon Kinesis Video Streams
- Exemplo: identificação de objetos em fluxos de vídeo usando SageMaker
- Exemplo: análise e renderização de fragmentos do Kinesis Video Streams
- Analise vídeos ao vivo em grande escala em tempo real usando o Amazon Kinesis Video Streams SageMaker e a Amazon (publicação no blog do AWS Machine Learning)
- Conceitos básicos do AWS Fargate

Mais informações

Escolhendo um IDE

Recomendamos que você use seu IDE Java favorito para criar e explorar esse projeto.

Liberar

Depois de concluir a execução deste exemplo, remova todos os recursos implantados para evitar custos adicionais de infraestrutura da AWS.

Para remover a infraestrutura e o stream de vídeo, use esses dois comandos na AWS CLI:

```
cdk destroy --profile "$AWS_PROFILE_NAME" --all
```

```
aws kinesisvideo --profile "$AWS_PROFILE_NAME" delete-stream --stream-arn "$STREAM_ARN"
```

Como alternativa, você pode remover os recursos manualmente usando o CloudFormation console da AWS para remover a CloudFormation pilha da AWS e o console do Kinesis para remover o stream de vídeo do Kinesis. Observe que `cdk destroy` não remove o bucket S3 de saída nem as imagens nos repositórios () do Amazon Elastic Container Registry (Amazon ECR) (`aws-cdk/assets`). Você precisa removê-los manualmente.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Criar um pipeline de serviços de ETL para carregar dados incrementalmente do Amazon S3 ao Amazon Redshift usando o AWS Glue

Criado por Rohan Jamadagni (AWS) e Arunabha Datta (AWS)

Resumo

Esse padrão fornece orientação sobre como configurar o Amazon Simple Storage Service (Amazon S3) para obter o desempenho ideal do data lake e, em seguida, carregar alterações incrementais de dados do Amazon S3 para o Amazon Redshift usando o AWS Glue, executando operações de extração, transformação e carregamento (ETL).

Os arquivos de origem no Amazon S3 podem ter formatos diferentes, incluindo valores separados por vírgula (CSV), XML e arquivos JSON. Esse padrão descreve como você pode usar o AWS Glue para converter os arquivos de origem em um formato com custo otimizado e desempenho, como o Apache Parquet. Você pode consultar arquivos do Parquet diretamente do Amazon Athena e do Amazon Redshift Spectrum. Você também pode carregar arquivos do Parquet no Amazon Redshift, agregá-los e compartilhar os dados agregados com os consumidores, ou visualizar os dados usando a Amazon. QuickSight

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket de origem do S3 que tem os privilégios certos e contém arquivos CSV, XML ou JSON.

Suposições

- Os arquivos de origem CSV, XML ou JSON já estão carregados no Amazon S3 e podem ser acessados na conta em que o AWS Glue e o Amazon Redshift estão configurados.
- As melhores práticas para carregar os arquivos, dividir os arquivos, compactar e usar um manifesto são seguidas, conforme discutido na documentação do Amazon Redshift.
- A estrutura do arquivo de origem permanece inalterada.
- O sistema de origem é capaz de ingerir dados no Amazon S3 seguindo a estrutura de pastas definida no Amazon S3.

- O cluster do Amazon Redshift abrange uma única zona de disponibilidade. (Essa arquitetura é apropriada porque o AWS Lambda, o AWS Glue e o Amazon Athena têm tecnologia sem servidor.) Para alta disponibilidade, os instantâneos do cluster são tirados com frequência regular.

Limitações

- Os formatos de arquivo são limitados aos que atualmente são compatíveis com o AWS Glue.
- Não há suporte para relatórios downstream em tempo real.

Arquitetura

Pilha de tecnologia de origem

- Bucket S3 com arquivos CSV, XML ou JSON

Pilha de tecnologias de destino

- Data lake S3 (com armazenamento de arquivos Parquet particionado)
- Amazon Redshift

Arquitetura de destino

Fluxo de dados

Ferramentas

- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável. O Amazon S3 pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- AWS Lambda: o AWS Lambda permite executar código sem provisionar ou gerenciar servidores. O AWS Lambda é um serviço orientado por eventos; você pode configurar seu código para iniciar automaticamente a partir de outros serviços da AWS.

- Amazon Redshift: o Amazon Redshift é um serviço de data warehouse em escala de petabytes totalmente gerenciado. Com o Amazon Redshift, você pode consultar petabytes de dados estruturados e semiestruturados em seu data warehouse e em seu data lake usando SQL padrão.
- AWS Glue: o AWS Glue é um serviço de ETL totalmente gerenciado que facilita a preparação e o carregamento de dados para análise. O AWS Glue descobre seus dados e armazena os metadados associados (por exemplo, definições de tabela e esquema) no Catálogo de dados do AWS Glue. Depois de catalogados, os dados se tornarão imediatamente pesquisáveis, consultáveis e disponíveis para ETL.
- AWS Secrets Manager: o AWS Secrets Manager facilita a proteção e o gerenciamento centralizado dos segredos necessários para o acesso a aplicativos ou serviços. O serviço armazena credenciais de banco de dados, chaves de API e outros segredos, além de eliminar a necessidade de codificar informações confidenciais em formato de texto sem formatação. O Secrets Manager também oferece rotação de chaves para atender às necessidades de segurança e conformidade. Ele tem integração integrada com o Amazon Redshift, Amazon Relational Database Service (Amazon RDS) e Amazon DocumentDB. Você pode armazenar e gerenciar segredos de forma centralizada usando o console do Secrets Manager, a interface de linha de comando (CLI) ou a API Secrets Manager e. SDKs
- Amazon Athena: o Amazon Athena é um serviço de consultas interativas que facilita a análise de dados armazenada no Amazon S3. O Athena tem tecnologia sem servidor e está integrado ao AWS Glue, portanto, pode consultar diretamente os dados que são catalogados usando o AWS Glue. O Athena é dimensionado de forma elástica para oferecer desempenho de consultas interativas.

Épicos

Crie os buckets e a estrutura de pastas do S3

Tarefa	Descrição	Habilidades necessárias
Analise os sistemas de origem quanto à estrutura e aos atributos dos dados.	Execute essa tarefa para cada fonte de dados que contribui para o data lake do Amazon S3.	Engenheiro de dados
Defina a estratégia de partição e acesso.	Essa estratégia deve ser baseada na frequência	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	das capturas de dados, no processamento delta e nas necessidades de consumo. Certifique-se de que os buckets do S3 não estejam abertos ao público e que o acesso seja controlad o somente por políticas específicas baseadas em perfis de serviço. Para mais informações, consulte a documentação do Amazon S3.	
Crie buckets S3 separados para cada tipo de fonte de dados e um bucket S3 separado por fonte para os dados processados (Parquet).	Crie um bucket separado para cada fonte e, em seguida, crie uma estrutura de pastas com base na frequência de ingestão de dados do sistema de origem; por exemplo, `s3://source-system-name/date/hour` . Para os arquivos processados (convertidos para o formato Parquet), crie uma estrutura semelhante; por exemplo, `s3://source-processed-bucket/date/hour` . Para obter mais informações sobre como ciar buckets do S3, consulte a Documentação do Amazon S3.	Engenheiro de dados

Criar um data warehouse no Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Inicie o cluster do Amazon Redshift com os grupos de parâmetros e a estratégia de manutenção e backup apropriados.	Use o segredo do banco de dados do Secrets Manager para credenciais de usuário administrador ao criar o cluster Amazon Redshift. Para obter informações sobre como criar e dimensionar um cluster do Amazon Redshift, consulte a documentação do Amazon Redshift e o whitepaper Dimensionamento de Data Warehouses na nuvem.	Engenheiro de dados
criar e associar o perfil de serviço do IAM ao cluster do Amazon Redshift.	O perfil de serviço AWS Identity and Access Management (IAM) garante acesso ao Secrets Manager e aos buckets de origem do S3. Para obter mais informaçõ es, consulte a documentação da AWS sobre autorização e adição de uma função.	Engenheiro de dados
Crie o esquema do banco de dados.	Siga as práticas recomenda das do Amazon Redshift para design de tabelas. Com base no caso de uso, escolha as chaves de classificação e distribuição apropriadas e a melhor codificação de compactação possível. Para obter as melhores práticas,	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	consulte a documentação da AWS.	
Configure o gerenciamento do workload.	Configure filas de workload (WLM - workload managemen t), aceleração de consultas curtas (SQA - short query acceleration) ou escalabil idade de simultaneidade, dependendo de suas necessidades. Para obter mais informações, consulte Implementar o gerenciamento de workload na documentação do Amazon Redshift.	Engenheiro de dados

Crie um segredo no Secrets Manager

Tarefa	Descrição	Habilidades necessárias
Crie um novo segredo para armazenar as credenciais de login do Amazon Redshift no Secrets Manager.	Esse segredo armazena as credenciais do usuário administrador, bem como dos usuários individuais do serviço de banco de dados. Para obter instruções, consulte a documentação do Secrets Manager. Escolha o Amazon Redshift Cluster como o tipo de segredo. Além disso, na página de rotação secreta, ative a rotação. Isso criará o usuário apropriado no cluster do Amazon Redshift	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	e alternará os segredos da chave em intervalos definidos.	
Crie uma política do IAM para restringir o acesso ao Secrets Manager.	Restrinja o acesso ao Secrets Manager somente aos administradores do Amazon Redshift e ao AWS Glue.	Engenheiro de dados

Configurar o AWS Glue

Tarefa	Descrição	Habilidades necessárias
No Catálogo de Dados do AWS Glue, adicione uma conexão para o Amazon Redshift.	Para obter instruções, consulte a documentação do AWS Glue.	Engenheiro de dados
Crie e anexe um perfil de serviço do IAM para o AWS Glue acessar os buckets do Secrets Manager, do Amazon Redshift e do S3.	Para obter mais informações, consulte a documentação do AWS Glue.	Engenheiro de dados
Defina o Catálogo de dados do AWS Glue para a fonte.	Essa etapa envolve a criação de um banco de dados e das tabelas necessárias no Catálogo de Dados do AWS Glue. Você pode usar um crawler para catalogar as tabelas no banco de dados AWS Glue ou defini-las como tabelas externas do Amazon Athena. Você também pode acessar as tabelas externas definidas no Athena por	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	meio do Catálogo de Dados do AWS Glue. Consulte a documentação da AWS para obter mais informações sobre como definir o catálogo de dados e criar uma tabela externa no Athena.	
Crie um trabalho do AWS Glue para processar dados de origem.	O trabalho do AWS Glue pode ser um shell do Python ou PySpark padronizar, desduplicar e limpar os arquivos de dados de origem. Para otimizar o desempenho e evitar a necessidade de consultar todo o bucket de origem do S3, particione o bucket do S3 por data, dividido por ano, mês, dia e hora como uma redução de predicado para o trabalho do AWS Glue. Para obter mais informações, consulte a documentação do AWS Glue. Carregue os dados processados e transformados nas partições de bucket do S3 processadas no formato Parquet. Você pode consultar os arquivos do Parquet do Athena.	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
Crie um trabalho do AWS Glue para carregar dados no Amazon Redshift.	O trabalho do AWS Glue pode ser um shell do Python ou PySpark carregar os dados atualizando os dados, seguido por uma atualização completa. Para obter detalhes, consulte a documentação do AWS Glue e a seção Informações adicionais.	Engenheiro de dados
(Opcional) Programe trabalhos do AWS Glue usando gatilhos conforme necessário.	A carga incremental de dados é impulsionada principalmente por um evento do Amazon S3 que faz com que uma função do Lambda da AWS chame a tarefa do AWS Glue. Use o agendamento baseado em gatilho do AWS Glue para qualquer carga de dados que exija agendamento baseado em tempo em vez de agendamento baseado em eventos.	Engenheiro de dados

Criar uma função do Lambda

Tarefa	Descrição	Habilidades necessárias
Crie e anexe uma função vinculada ao serviço do IAM para que o AWS Lambda acesse buckets do S3 e o trabalho do AWS Glue.	Crie uma função vinculada ao serviço do IAM para o AWS Lambda com uma política para ler objetos e buckets do Amazon S3 e uma política para acessar a API do AWS	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	Glue para iniciar um trabalho do AWS Glue. Para obter mais informações, consulte o Centro de Conhecimentos.	
Crie uma função do Lambda para executar o trabalho do AWS Glue com base no evento definido do Amazon S3.	A função do Lambda deve ser iniciada pela criação do arquivo de manifesto do Amazon S3. A função Lambda deve passar a localização da pasta Amazon S3 (por exemplo, bucket/year/month/date/hour source_) para o trabalho do AWS Glue como parâmetro. O trabalho do AWS Glue usará esse parâmetro como uma redução de predicado para otimizar o acesso a arquivos e o desempenho do processam ento de trabalhos. Para obter mais informações, consulte a documentação do AWS Glue.	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
Crie um evento de objeto PUT do Amazon S3 para detectar a criação de objetos e chame a respectiva função do Lambda.	O evento de objeto PUT do Amazon S3 deve ser iniciado somente pela criação do arquivo de manifesto. O arquivo de manifesto controla a função do Lambda e a simultaneidade de trabalhos do AWS Glue e processa a carga como um lote, em vez de processar arquivos individuais que chegam em uma partição específica do bucket de origem do S3. Para obter mais informações, consulte a documentação do Lambda.	Engenheiro de dados

Recursos relacionados

- Documentação do Amazon S3
- Documentação do AWS Glue
- Documentação do Amazon Redshift
- AWS Lambda
- Amazon Athena
- AWS Secrets Manager

Mais informações

Abordagem detalhada para atualização inicial e completa

Upsert: para conjuntos de dados que exigem agregação histórica, dependendo do caso de uso comercial. Siga uma das abordagens descritas em Atualização e inserção de novos dados (documentação do Amazon Redshift) com base nas necessidades da sua empresa.

Atualização completa: para pequenos conjuntos de dados que não precisam de agregações históricas. Siga uma dessas abordagens:

1. Leve a tabela do Amazon Redshift.
2. Carregue a partição atual da área de armazenamento

ou:

1. Crie uma tabela temporária com dados de partição atuais.
2. Spçte a tabela de destino no Amazon Redshift.
3. Renomeie a tabela temporária para tabela de destino.

Crie uma malha de dados corporativa com a Amazon DataZone, AWS CDK, e AWS CloudFormation

Criado por Dhrubajyoti Mukherjee (AWS), Adjoa Taylor (AWS), Ravi Kumar (AWS) e Weizhou Sun (AWS)

Resumo

Na Amazon Web Services (AWS), os clientes entendem que os dados são a chave para acelerar a inovação e gerar valor comercial para sua empresa. Para gerenciar esses dados massivos, você pode adotar uma arquitetura descentralizada, como malha de dados. Uma arquitetura de malha de dados facilita o pensamento sobre o produto, uma mentalidade que leva em consideração os clientes, as metas e o mercado. A malha de dados também ajuda a estabelecer um modelo de governança federada que fornece acesso rápido e seguro aos seus dados.

Estratégias para criar uma solução corporativa baseada em malha de dados em AWS discute como você pode usar a Estrutura de Estratégia de Malha de Dados para formular e implementar uma estratégia de malha de dados para sua organização. Ao usar o Data Mesh Strategy Framework, você pode otimizar a organização das equipes e suas interações para acelerar sua jornada de malha de dados.

Este documento fornece orientação sobre como criar uma malha de dados corporativa com a Amazon DataZone. DataZone A Amazon é um serviço de gerenciamento de dados para catalogar, descobrir, compartilhar e governar dados armazenados localmente e em AWS fontes terceirizadas. O padrão inclui artefatos de código que ajudam você a implantar a infraestrutura de solução de dados baseada em malha de dados usando e. AWS Cloud Development Kit (AWS CDK) AWS CloudFormation Esse padrão é destinado a arquitetos e DevOps engenheiros de nuvem.

Para obter informações sobre os objetivos desse padrão e o escopo da solução, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Um mínimo de dois ativos Contas da AWS: um para a conta de governança central e outro para a conta do membro
- AWS credenciais de administrador para a conta de governança central em seu ambiente de desenvolvimento

- AWS Command Line Interface (AWS CLI) instalado para gerenciar seu a Serviços da AWS partir da linha de comando
- Node.js e Node Package Manager (npm) instalados para gerenciar aplicativos AWS CDK
- AWS CDK Kit de ferramentas instalado globalmente em seu ambiente de desenvolvimento usando npm, para sintetizar e implantar aplicativos AWS CDK

```
npm install -g aws-cdk
```

- Python versão 3.12 instalada em seu ambiente de desenvolvimento
- TypeScript instalado em seu ambiente de desenvolvimento ou instalado globalmente usando o compilador npm:

```
npm install -g typescript
```

- Docker instalado em seu ambiente de desenvolvimento
- Um sistema de controle de versão, como o Git, para manter o código-fonte da solução (recomendado)
- Um ambiente de desenvolvimento integrado (IDE) ou editor de texto com suporte para Python e TypeScript (altamente recomendado)

Limitações

- A solução foi testada somente em máquinas que executam Linux ou macOS.
- Na versão atual, a solução não suporta a integração da Amazon DataZone e, AWS IAM Identity Center por padrão. No entanto, você pode configurá-lo para oferecer suporte a essa integração.

Versões do produto

- Python versão 3.12

Arquitetura

O diagrama a seguir mostra uma arquitetura de referência de malha de dados. A arquitetura é baseada na Amazon DataZone e usa o Amazon Simple Storage Service (Amazon S3) AWS Glue Data Catalog e como fontes de dados. O Serviços da AWS que você usa com a Amazon DataZone

em sua implementação de malha de dados pode ser diferente, com base nos requisitos da sua organização.

1. Nas contas do produtor, os dados brutos são adequados para consumo em sua forma atual ou são transformados para consumo por meio do uso AWS Glue. Os metadados técnicos dos dados são armazenados no Amazon S3 e avaliados usando AWS Glue um rastreador de dados. A qualidade dos dados é medida usando a Qualidade AWS Glue dos Dados. O banco de dados de origem no catálogo de dados é registrado como um ativo no DataZone catálogo da Amazon. O DataZone catálogo da Amazon é hospedado na conta de governança central usando trabalhos de fonte DataZone de dados da Amazon.
2. A conta de governança central hospeda o DataZone domínio da Amazon e o portal de DataZone dados da Amazon. Os produtores e consumidores Contas da AWS de dados estão associados ao DataZone domínio da Amazon. Os DataZone projetos da Amazon dos produtores e consumidores de dados são organizados sob as unidades de DataZone domínio correspondentes da Amazon.
3. Os usuários finais dos ativos de dados fazem login no portal de DataZone dados da Amazon usando suas credenciais AWS Identity and Access Management (IAM) ou login único (com integração por meio do IAM Identity Center). Eles pesquisam, filtram e visualizam informações de ativos (por exemplo, informações de qualidade de dados ou metadados comerciais e técnicos) no catálogo de DataZone dados da Amazon.
4. Depois que um usuário final encontra o ativo de dados que deseja, ele usa o recurso de DataZone assinatura da Amazon para solicitar acesso. O proprietário dos dados da equipe de produtores recebe uma notificação e avalia a solicitação de assinatura no portal de DataZone dados da Amazon. O proprietário dos dados aprova ou rejeita a solicitação de assinatura com base em sua validade.
5. Depois que a solicitação de assinatura é concedida e atendida, o ativo é acessado na conta do consumidor para as seguintes atividades:
   - Desenvolvimento de modelos de IA/ML usando Amazon AI SageMaker
   - Análises e relatórios usando o Amazon Athena e a Amazon QuickSight

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que ajuda a análise de dados diretamente no Amazon Simple Storage Service (Amazon S3) usando SQL padrão.

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- DataZoneA Amazon é um serviço de gerenciamento de dados que ajuda você a catalogar, descobrir, compartilhar e controlar dados armazenados localmente e em fontes terceirizadas. AWS
- QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel.
- O Amazon SageMaker AI é um serviço gerenciado de aprendizado de máquina (ML) que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Repositório de código

A solução está disponível no repositório GitHub data-mesh-datazone-cdk-cloudformation.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositór io, execute o seguinte comando em seu ambiente de desenvolvimento local (Linux ou macOS):	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/aws-samples/data-mesh-data zone-cdk-cloudformation`	

Criar o ambiente	Para criar o ambiente virtual Python, execute os seguintes comandos:
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip install -r requirements.txt`
		Arquiteto de nuvem, DevOps engenheiro

Inicialize a conta.	Para inicializar a conta de governança central usando AWS CDK, execute o seguinte comando: `cdk bootstrap aws://<GOVERNANCE_ACCOUNT_ID>/<AWS_REGION>` Faça login no AWS Management Console, abra o console central da conta de governança e obtenha o Amazon Resource Name (ARN) da função de AWS CDK execução.	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Construa o `DzDataMeshMemberStackSet.yaml` arquivo.	Para construir o `DzDataMeshMemberStackSet.yaml` arquivo, a partir do diretório raiz do repositório, inicie o seguinte script bash: `./lib/scripts/create_dz_data_mesh_member_stack_set.sh`	Arquiteto de nuvem, DevOps engenheiro
Confirme a criação do modelo.	Certifique-se de que o arquivo de AWS CloudFormation modelo seja criado no `lib/cfn-templates/DzDataMeshMemberStackSet.yaml` local.	Arquiteto de nuvem, DevOps engenheiro

Implemente recursos na conta de governança central

Tarefa	Descrição	Habilidades necessárias

Modifique a configuração.	No `config/Config.ts` arquivo, modifique os seguintes parâmetros:
	`DZ_APPLICATION_NAME - Name of the application.`
	`DZ_STAGE_NAME - Name of the stage.`
	`DZ_DOMAIN_NAME - Name of the Amazon DataZone domain`
	`DZ_DOMAIN_DESCRIPTION - Description of the Amazon DataZone domain`
		Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	DZ_DOMAIN_TAG - Tag of the Amazon DataZone domain DZ_ADMIN_PROJECT_NAME - Name of the Amazon DataZone project for administrators DZ_ADMIN_PROJECT_DESCRIPTION - Description of the Amazon DataZone project for administrators CDK_EXEC_ROLE_ARN - ARN of the cdk execution role DZ_ADMIN_ROLE_ARN - ARN of the administrator role Mantenha os parâmetros restantes vazios.	

Tarefa	Descrição	Habilidades necessárias
Atualize a configuração do DataZone glossário da Amazon.	Para atualizar a configuração do DataZone glossário da Amazon no `lib/utils/glossary_config.json` arquivo, use o seguinte exemplo de configuração: `{ "GlossaryName": "PII Data", "GlossaryDescription": "If data source contains PII attributes", "GlossaryTerms": [{ "Name": "Yes", "ShortDescription": "Yes", "LongDescription": "Yes Glossary Term" }, { "Name": "No", "ShortDescription": "No", "LongDescription": "No Glossary Term" } ] }`	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Atualize a configuração do formulário de DataZone metadados da Amazon.	Para atualizar a configuração do formulário de DataZone metadados da Amazon `nolib/utils/metadata_form_config.json file`, use o seguinte exemplo de configuração: `{ "FormName": "ScheduleDataRefresh", "FormDescription": "Form for data refresh schedule", "FormSmithyModel": "@amazon.datazone#displayname(defaultName: \"Data Refresh Schedule\")\nstructure ScheduleDataRefresh {\n @documentation(\"Schedule of Data Refresh\")\n @required\n @amazon.datazone#searchable\n @amazon.datazone#displayname(defaultName: \"Data Refresh Schedule\")\n data_refresh_schedule: String\n}" }`	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Exporte as AWS credenciais.	Para exportar AWS credencia is para seu ambiente de desenvolvimento para a função do IAM com permissõe s administrativas, use o seguinte formato: `export AWS_ACCES S_KEY_ID= export AWS_SECRE T_ACCESS_KEY= export AWS_SESSI ON_TOKEN=`	Arquiteto de nuvem, DevOps engenheiro
Sintetize o modelo.	Para sintetizar o AWS CloudFormation modelo, execute o seguinte comando: `npx cdk synth`	Arquiteto de nuvem, DevOps engenheiro
Implante a solução.	Para implantar a solução, execute o seguinte comando: `npx cdk deploy --all`	Arquiteto de nuvem, DevOps engenheiro

Configurar novas contas de membros

Tarefa	Descrição	Habilidades necessárias
Implante o modelo.	Implante o AWS CloudForm ation modelo localizado `lib/cfn-templates/ DzDataMeshCfnStack SetExecutionRole.y`	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`aml` na conta do membro com os seguintes parâmetros de entrada: • `GovernanceAccountID` – ID da conta de governança • `DataZoneKMSKeyID` – ID da chave AWS Key Management Service (AWS KMS) que criptografa os metadados da Amazon DataZone • `NotificationQueueName` – Nome da fila de notificação do Amazon SQS na conta de governança	
Atualize ARNs o.	Para atualizar a lista de funções ARNs de AWS CloudFormation StackSet execução das contas dos membros, use o código a seguir: `DZ_MEMBER_STACK_SET_EXEC_ROLE_LIST - List of Stack set execution role arns for the member accounts.`	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Sintetize e implante.	Para sintetizar o AWS CloudFormation modelo e implantar a solução, execute os seguintes comandos:
	`npx cdk synth`
	`npx cdk deploy --all`
		Arquiteto de nuvem, DevOps engenheiro

Associe a conta do membro.	Para associar a conta do membro à conta de governanç a central, faça o seguinte: 1. Faça login no console da conta de governança central e abra o DataZone console da Amazon em https://console.aws.amazon.com/datazone/. 2. Escolha o domínio que você criou. 3. Role até a guia Contas associadas e escolha Solicitar associação. 4. Forneça o ID da conta da AWS e escolha AWSRAMPermissionDataZonePortalReadWritecomo política de RAM. 5. Escolha Solicitar associaçã o. 6. Espere até receber uma notificação por e-mail de que sua conta foi inicializ ada com sucesso.	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Atualize os parâmetros.	Para atualizar os parâmetros específicos da conta do membro no arquivo de configuração em `config/Config.ts`, use o seguinte formato: `export const DZ_MEMBER_ACCOUNT_CONFIG: memberAccountConfig = { '123456789012' : { PROJECT_NAME: 'TEST-PROJECT-123456789012', PROJECT_DESCRIPTION: 'TEST-PROJECT-123456789012', PROJECT_EMAIL: 'user@xyz.com' } }`	Arquiteto de nuvem, DevOps engenheiro

Sintetize e implante o modelo.	Para sintetizar o AWS CloudFormation modelo e implantar a solução, execute os seguintes comandos:
	`npx cdk synth`
	`npx cdk deploy --all`
		Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Adicione contas de membros.	Para criar e configurar contas de membros adicionais na solução de dados, repita as etapas anteriores para cada conta de membro. Essa solução não diferencia entre produtores e consumidores de dados.	Arquiteto de nuvem, DevOps engenheiro

Limpeza

Tarefa	Descrição	Habilidades necessárias
Desassocie as contas dos membros.	Para desassociar as contas, faça o seguinte: 1. Faça login no console e abra o DataZone console da Amazon. 2. Escolha Exibir domínios. 3. Selecione o domínio que você criou. 4. Escolha a guia Associações de contas. 5. Selecione a conta de membro que você deseja desassociar. 6. Escolha Desassociar e insira `disassociate` para confirmar.	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	7. Repita as etapas de 3 a 6 para todas as contas de membros.	

Tarefa	Descrição	Habilidades necessárias
Exclua as instâncias da pilha.	Para excluir as instâncias da AWS CloudFormation pilha, faça o seguinte: 1. Abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation/. 2. No painel de navegação, escolha StackSets. 3. Escolha o conjunto de pilhas chamado StackSet-DataZone - DataMesh - Member e escolha a guia Stack instances. 4. Copie o Conta da AWS ID da conta de membro que você deseja remover da associação. 5. Escolha Ações, escolha Excluir pilhas StackSet de e mantenha as opções padrão. 6. No campo Números da conta, insira o ID da conta. 7. Na lista suspensa Especificar regiões, escolha o. Região da AWS 8. Escolha Avançar e, em seguida, escolha Enviar. 9. Na guia Operações, confirme se a operação foi bem-sucedida. A exclusão	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	da pilha pode levar algum tempo. 10. Repita as etapas de 2 a 9 para todas as contas de membros.	
Destrua todos os recursos.	Para destruir recursos, implemente as seguintes etapas em seu ambiente de desenvolvimento local (Linux ou macOS): 1. Navegue até o diretório raiz do seu repositório. 2. Exporte AWS as credencia is da função do IAM que você usou para criar a AWS CDK pilha. 3. Para destruir os recursos da nuvem, execute o seguinte comando: `npx cdk destroy --all`	Arquiteto de nuvem, DevOps engenheiro

Recursos relacionados

- DataZone Início rápido da Amazon com dados AWS Glue
- Tutorial: Crie seu primeiro AWS CDK aplicativo
- Começando com AWS CloudFormation
- Estratégias para criar uma solução corporativa baseada em malha de dados em AWS

Mais informações

Objetivos

A implementação desse padrão alcança o seguinte:

- Propriedade descentralizada dos dados – Transfira a propriedade dos dados de uma equipe central para equipes que representam os sistemas de origem, as unidades de negócios ou os casos de uso da sua organização.
- Pensamento sobre o produto – Apresente uma mentalidade baseada em produtos que inclua clientes, o mercado e outros fatores ao considerar os ativos de dados em sua organização.
- Governança federada – Melhore as barreiras de segurança, os controles e a conformidade em todos os produtos de dados da sua organização.
- Suporte para várias contas e vários projetos – Support o compartilhamento e a colaboração de dados eficientes e seguros entre as unidades de negócios ou projetos de sua organização.
- Monitoramento e notificações centralizados – Monitore os recursos de nuvem de sua malha de dados usando a Amazon CloudWatch e notifique os usuários quando uma nova conta de membro for associada.
- Escalabilidade e extensibilidade – Adicione novos casos de uso à malha de dados à medida que sua organização evolui.

Escopo da solução

Ao usar essa solução, você pode começar aos poucos e escalar à medida que avança em sua jornada de malha de dados. Geralmente, quando uma conta membro adota a solução de dados, ela contém configurações de conta específicas para a organização, projeto ou unidade de negócios. Essa solução acomoda essas diversas Conta da AWS configurações ao oferecer suporte aos seguintes recursos:

- AWS Glue Data Catalog como fonte de dados para a Amazon DataZone
- Gerenciamento do domínio de DataZone dados da Amazon e do portal de dados relacionado
- Gerenciamento da adição de contas de membros na solução de dados baseada em malha de dados
- Gestão de DataZone projetos e ambientes da Amazon
- Gerenciamento de DataZone glossários e formulários de metadados da Amazon

- Gerenciamento de funções do IAM que correspondem aos usuários da solução de dados baseada em malha de dados
- Notificação de usuários da solução de dados baseada em malha de dados
- Monitoramento da infraestrutura de nuvem provisionada

  Essa solução usa AWS CDK e implementa AWS CloudFormation a infraestrutura em nuvem. Ele costuma AWS CloudFormation fazer o seguinte:

  - Defina e implemente recursos de nuvem em um nível mais baixo de abstração.
  - Implemente recursos de nuvem a partir do AWS Management Console. Ao usar essa abordagem, você pode implantar a infraestrutura sem um ambiente de desenvolvimento.

  A solução de malha de dados é usada AWS CDK para definir recursos em um nível de abstração mais alto. Como resultado, a solução fornece uma abordagem desacoplada, modular e escalável ao escolher a ferramenta relevante para implantar os recursos de nuvem.

Próximas etapas

Você pode entrar em contato com AWSespecialistas para obter orientação sobre como criar uma malha de dados com a Amazon DataZone.

A natureza modular dessa solução oferece suporte à criação de soluções de gerenciamento de dados com diferentes arquiteturas, como estrutura de dados e lagos de dados. Além disso, com base nos requisitos da sua organização, você pode estender a solução para outras fontes de DataZone dados da Amazon.

Calcule o value at risk (VaR – valor em risco) usando os serviços da AWS

Criado por Sumon Samanta (AWS)

Resumo

Esse padrão descreve como implementar um sistema de cálculo de valor em risco (VaR) usando os serviços da AWS. Em um ambiente on-premises, a maioria dos sistemas VaR usa uma infraestrutura grande e dedicada e um software de agendamento de rede interno ou comercial para executar processos em lote. Esse padrão apresenta uma arquitetura simples, confiável e escalável para lidar com o processamento de VaR na nuvem AWS. Ele cria uma arquitetura sem servidor que usa o Amazon Kinesis Data Streams como um serviço de streaming, o Amazon Simple Queue Service (Amazon SQS) como um serviço gerenciado de filas, a Amazon como um serviço de cache e o ElastiCache AWS Lambda para processar pedidos e calcular riscos.

O VaR é uma medida estatística que os negociadores e gerentes de risco usam para estimar a perda potencial em seu portfólio além de um certo nível de confiança. A maioria dos sistemas VaR envolve a execução de um grande número de cálculos matemáticos e estatísticos e o armazenamento dos resultados. Esses cálculos exigem recursos computacionais significativos, portanto, os processos em lote do VaR precisam ser divididos em conjuntos menores de tarefas computacionais. É possível dividir um lote grande em tarefas menores porque essas tarefas são, em sua maioria, independentes (ou seja, os cálculos de uma tarefa não dependem de outras tarefas).

Outro requisito importante para uma arquitetura VaR é a escalabilidade computacional. Esse padrão usa uma arquitetura com tecnologia sem servidor que aumenta ou diminui automaticamente com base na carga computacional. Como a demanda de computação em lote ou on-line é difícil de prever, o escalonamento dinâmico é necessário para concluir o processo dentro do cronograma imposto por um Acordo de Serviço (SLA). Além disso, uma arquitetura com custo otimizado deve ser capaz de reduzir a escala verticalmente para cada recurso computacional assim que as tarefas desse recurso forem concluídas.

Os serviços da AWS são adequados para cálculos de VaR porque oferecem capacidade de computação e armazenamento escalável, serviços de análise para processamento de forma econômica e diferentes tipos de agendadores para executar seus fluxos de trabalho de gerenciamento de riscos. Além disso, você paga apenas pelos recursos de computação e armazenamento que usa na AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Arquivos de entrada, que dependem dos requisitos da sua empresa. Um caso de uso típico envolve os seguintes arquivos de entrada:
  - Arquivo de dados de mercado (entrada para o mecanismo de cálculo do VaR)
  - Arquivo de dados comerciais (a menos que os dados comerciais venham por meio de um fluxo).
  - Arquivo de dados de configuração (modelo e outros dados estáticos de configuração)
  - Arquivos de modelo do mecanismo de cálculo (bibliotecas quantitativas)
  - Arquivo de dados de séries temporais (para dados históricos, como o preço das ações nos últimos cinco anos)
- Se os dados de mercado ou outras informações chegarem por meio de um stream, o Amazon Kinesis Data Streams será configurado e as permissões do Amazon Identity and Access Management (IAM) serão configuradas para gravar no stream.

Esse padrão cria uma arquitetura na qual os dados comerciais são gravados de um sistema de negociação em um fluxo de dados do Kinesis. Em vez de usar um serviço de streaming, você pode salvar os dados de negociação em pequenos lotes, armazená-los em um bucket do Amazon Simple Storage Service (Amazon S3) e invocar um evento para começar a processar os dados.

Limitações

- O sequenciamento do fluxo de dados do Kinesis é garantido em cada fragmento, portanto, não é garantido que as ordens de negociação gravadas em vários fragmentos sejam entregues na mesma ordem das operações de gravação.
- Atualmente, o limite de runtime do AWS Lambda é de 15 minutos. (Para obter mais informações, consulte as perguntas frequentes do Lambda.)

Arquitetura

Arquitetura de destino

O diagrama de arquitetura a seguir mostra os serviços e fluxos de trabalho da AWS para o sistema de avaliação de risco.

O diagrama ilustra o seguinte:

1. As negociações chegam do sistema de gerenciamento de pedidos.
2. A função do Lambda de compensação da posição do tíquete processa os pedidos e grava mensagens consolidadas para cada ticker em uma fila de risco no Amazon SQS.
3. A função Lambda do mecanismo de cálculo de risco processa as mensagens do Amazon SQS, realiza cálculos de risco e atualiza as informações de lucros e perdas (PnL) do VaR no cache de risco na Amazon. ElastiCache
4. A função Lambda de leitura de ElastiCache dados recupera os resultados de risco e os armazena em um banco de dados ElastiCache e em um bucket do S3.

Para obter mais informações sobre esses serviços e etapas, consulte a seção Épicos.

Automação e escala

Você pode implantar toda a arquitetura usando o AWS Cloud Development Kit (AWS CDK) ou os CloudFormation modelos da AWS. A arquitetura pode suportar tanto o processamento em lote quanto o processamento intradiário (em tempo real).

O dimensionamento é incorporado à arquitetura. À medida que mais negociações são gravadas no fluxo de dados do Kinesis e aguardam para serem processadas, funções adicionais do Lambda podem ser invocadas para processar essas negociações e, em seguida, podem reduzir a escala verticalmente após a conclusão do processamento. O processamento por meio de várias filas de cálculo de risco do Amazon SQS também é uma opção. Se for necessária uma ordenação ou consolidação estritas nas filas, o processamento não poderá ser paralelizado. No entanto, para um end-of-the-day lote ou um mini lote intradiário, as funções Lambda podem processar paralelamente e armazenar os resultados finais em. ElastiCache

Ferramentas

Serviços da AWS

- O Amazon Aurora MySQL-Compatible Edition é um mecanismo de banco de dados relacional totalmente gerenciado e compatível com MySQL que ajuda você a configurar, operar e dimensionar implantações do MySQL. Esse padrão usa o MySQL como exemplo, mas você pode usar qualquer sistema RDBMS para armazenar dados.

- ElastiCacheA Amazon ajuda você a configurar, gerenciar e escalar ambientes distribuídos de cache na memória na nuvem da AWS.
- O Amazon Kinesis Data Streams ajuda a coletar e processar grandes fluxos de registros de dados em tempo real.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Código

Esse padrão fornece um exemplo de arquitetura para um sistema VaR na Nuvem AWS e descreve como você pode usar funções do Lambda para cálculos de VaR. Para criar suas funções do Lambda, consulte os exemplos de código na documentação do Lambda. Para obter ajuda, entre em contato com o AWS Professional Services.

Práticas recomendadas

- Mantenha cada tarefa de computação do VaR tão pequena e leve quanto possível. Experimente diferentes números de negociações em cada tarefa de computação para ver qual delas é a mais otimizada para tempo e custo de computação.
- Armazene objetos reutilizáveis na Amazon. ElastiCache Use uma estrutura como o Apache Arrow para reduzir a serialização e a desserialização.
- Considere a limitação de tempo do Lambda. Se você acha que suas tarefas de computação podem exceder 15 minutos, tente dividi-las em tarefas menores para evitar o tempo limite do Lambda. Se isso não for possível, considere uma solução de orquestração de contêiner com o AWS Fargate, o Amazon Elastic Container Service (Amazon ECS) e o Amazon Elastic Kubernetes Service (Amazon EKS).

Épicos

Fluxo comercial para o sistema de risco

Tarefa	Descrição	Habilidades necessárias
Comece a escrever negociaçõ es.	Negociações novas, liquidada s ou parcialmente liquidada s são gravadas do sistema de gerenciamento de pedidos em um fluxo de risco. Esse padrão usa o Amazon Kinesis como serviço de streaming gerenciado. O hash do ticker da ordem comercial é usado para colocar ordens comerciai s em vários fragmentos.	Amazon Kinesis

Execute funções do Lambda para processamento de pedidos

Tarefa	Descrição	Habilidades necessárias
Inicie o processamento de riscos com o Lambda.	Execute uma função do AWS Lambda para os novos pedidos. Com base no número de pedidos de negociação pendentes, o Lambda será escalado automaticamente. Cada instância do Lambda tem um ou mais pedidos e recupera a posição mais recente de cada ticker da Amazon. ElastiCache (Você pode usar uma ID CUSIP, um nome de curva ou um nome de índice para outros produtos	Amazon Kinesis, AWS Lambda, Amazon ElastiCache

Tarefa	Descrição	Habilidades necessárias
	derivados financeiros como uma chave para armazenar e recuperar dados.) ElasticCache Em ElastiCache, a posição total (quantidade) e o par de valores-chave < ticker, posição líquida >, em que a posição líquida é o fator de escala, são atualizados uma vez para cada ticker.	

Escreva mensagens para cada ticker na fila

Tarefa	Descrição	Habilidades necessárias
Grave mensagens consolidadas na fila de risco.	Escrever a mensagem em uma fila. Esse padrão usa o Amazon SQS como um serviço gerenciado de filas. Uma única instância do Lambda pode receber um pequeno lote de ordens comerciais a qualquer momento, mas gravará somente uma única mensagem para cada ticker no Amazon SQS. Um fator de escala é calculado: (posição líquida antiga + posição atual) /posição líquida antiga.	Amazon SQS, AWS Lambda

Invoque o mecanismo de risco

Tarefa	Descrição	Habilidades necessárias
Inicie os cálculos de risco.	A função do Lambda para o mecanismo de risco do lambda é invocada. Cada posição é processada por uma única função do Lambda. No entanto, para fins de otimização, cada função do Lambda pode processar várias mensagens do Amazon SQS.	Amazon SQS, AWS Lambda

Recupere resultados de risco do cache

Tarefa	Descrição	Habilidades necessárias
Recupere e atualize o cache de riscos.	O Lambda recupera a posição líquida atual de cada ticker de. ElastiCache Ele também recupera uma matriz de lucros e perdas (PnL) do VaR para cada ticker de. ElastiCache Se a matriz PnL já existir, a função do Lambda atualiza a matriz e o VaR com uma escala, que vem da mensagem do Amazon SQS escrita pela função netting Lambda. Se a matriz PnL não estiver ativada ElasticCache, um novo PnL e VaR serão calculados usando dados	Amazon SQS, AWS Lambda, Amazon ElastiCache

Tarefa	Descrição	Habilidades necessárias
	simulados da série de preços do ticker.	

Atualize dados no Elastic Cache e armazene no banco de dados

Tarefa	Descrição	Habilidades necessárias
Armazene os resultados de risco.	Depois que os números VaR e PnL são atualizad os ElastiCache, uma nova função Lambda é invocada a cada cinco minutos. Essa função lê todos os dados armazenados ElastiCache e os armazena em um banco de dados compatível com o Aurora MySQL e em um bucket do S3.	AWS Lambda, Amazon ElastiCache

Recursos relacionados

- Estrutura VaR de Basileia

Configurar o acesso entre contas para um Catálogo de Dados do AWS Glue compartilhado usando o Amazon Athena

Criado por Denis Avdonin (AWS)

Resumo

Esse padrão fornece step-by-step instruções, incluindo exemplos de políticas do AWS Identity and Access Management (IAM), para configurar o compartilhamento entre contas de um conjunto de dados armazenado em um bucket do Amazon Simple Storage Service (Amazon S3) usando o AWS Glue Data Catalog. Você pode armazenar o conjunto de dados em um bucket do S3. Os metadados são coletados por um crawler do AWS Glue e colocados no catálogo de dados do AWS Glue. O bucket do S3 e o Catálogo de Dados do AWS Glue residem em uma conta da AWS chamada de conta de dados. Você pode fornecer acesso às entidades principais do IAM em outra conta da AWS chamada de conta do consumidor. Os usuários podem consultar os dados na conta do consumidor usando o mecanismo de consulta de tecnologia sem servidor Amazon Athena.

Pré-requisitos e limitações

Pré-requisitos

- Duas contas da AWS ativas.
- Um bucket do S3 em uma das contas da AWS
- Mecanismo do Athena versão 2
- AWS Command Line Interface (AWS CLI), instalada e configurada (ou AWS para executar comandos CloudShell da AWS CLI)

Versões do produto

Esse padrão funciona somente com a versão 2 do mecanismo Athena e a versão 3 do mecanismo Athena. Recomendamos que você faça upgrade para a versão 3 do mecanismo Athena. Se você não conseguir fazer o upgrade da versão 1 do Athena Engine para a versão 3 do Athena Engine, siga a abordagem discutida em Acesso entre contas ao AWS Glue Data Catalog com o Amazon Athena no blog de Big Data da AWS.

Arquitetura

Pilha de tecnologias de destino

- Amazon Athena
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (AWS KMS)

O diagrama a seguir mostra uma arquitetura que usa permissões do IAM para compartilhar dados em um bucket do S3 em uma conta da AWS (conta de dados) com outra conta da AWS (conta de consumidor) por meio do Catálogo de Dados do AWS Glue.

O diagrama mostra o seguinte fluxo de trabalho:

1. A política de bucket do S3 na conta de dados concede permissões para um perfil do IAM na conta do consumidor e para o perfil de serviço do crawler AWS Glue na conta de dados.
2. A política de chaves do AWS KMS na conta de dados concede permissões para o perfil do IAM na conta do consumidor e para o perfil de serviço do crawler AWS Glue na conta de dados.
3. O crawler do AWS Glue na conta de dados descobre o esquema dos dados armazenados no bucket do S3.
4. A política de recursos do Catálogo de Dados do AWS Glue na conta de dados concede acesso ao perfil do IAM na conta do consumidor.
5. Um usuário cria uma referência de catálogo nomeada na conta do consumidor usando um comando da AWS CLI.
6. Uma política do IAM concede a um perfil do IAM na conta do consumidor acesso aos recursos na conta de dados. A política de confiança da função do IAM permite que os usuários na conta do consumidor assumam a função do IAM.
7. Um usuário na conta do consumidor assume o perfil do IAM e acessa objetos no catálogo de dados usando consultas SQL.
8. O mecanismo de tecnologia sem servidor do Athena executa as consultas SQL.

> **Note**
>
> As melhores práticas do IAM recomendam que você conceda permissões para uma função do IAM e use a federação de identidades.

Ferramentas

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.

Épicos

Configurar permissões na conta de dados

Tarefa	Descrição	Habilidades necessárias
Conceder acesso aos dados no bucket do S3.	Crie uma política de bucket do S3 com base no modelo a seguir e atribua a política ao bucket em que os dados estão armazenados. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": [`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	"arn:aws:iam::<consumer account id>:role/<role name>",
	
	"arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler"
	]
	},
	"Action": "s3:GetObject",
	"Resource": "arn:aws:s3:::data-bucket/*"
	},
	{
	"Effect": "Allow",
	"Principal": {
	"AWS": [
	
	"arn:aws:iam::<consumer account id>:role/<role name>",
	
	"arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler"
	]
	},
	"Action": "s3:ListBucket",
	"Resource": "arn:aws:s3:::data-bucket"
	}	

Tarefa	Descrição	Habilidades necessárias
	<pre>] }</pre> A política de bucket concede permissões para o perfil do IAM na conta do consumidor e para o perfil de serviço do crawler AWS Glue na conta de dados.	

Tarefa	Descrição	Habilidades necessárias
(Se necessário) Conceder acesso à chave de criptografia de dados.	Se o bucket do S3 for criptografado por uma chave do AWS KMS, conceda permissão `kms:Decrypt` na chave para o perfil do IAM na conta do consumidor e para o perfil de serviço do crawler do AWS Glue na conta de dados. Atualize a política de chave com a seguinte instrução: `{ "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Conceder ao crawler o acesso aos dados.	Anexe a seguinte política do IAM ao perfil de serviço do crawler: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" } ] }`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
(Se necessário) Conceder ao crawler o acesso à chave de criptografia de dados.	Se o bucket do S3 for criptografado por uma chave do AWS KMS, conceda a permissão `kms:Decrypt` sobre a chave para o perfil de serviço do crawler, anexando a ela a seguinte política: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Conceder ao perfil do IAM na conta do consumidor e ao crawler o acesso ao catálogo de dados.	1. Faça login no Console de Gerenciamento da AWS e abra o Console do AWS Glue. 2. No painel de navegação, em Catálogo de dados, escolha Configurações. 3. Na seção Permissões, adicione a seguinte declaração e escolha Salvar. `{ "Version" : "2012-10-17", "Statement" : [ { "Effect" : "Allow", "Principal" : { "AWS" : [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, "Action" : "glue:*",`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	<pre>"Resource
	" : [
	
	"arn:aws:glue:<reg
	ion>:<data account
	id>:catalog",
	
	"arn:aws:glue:<reg
	ion>:<data account
	id>:database/*",
	
	"arn:aws:glue:<reg
	ion>:<data account
	id>:table/*"
	]
	}
	]
	}</pre> Essa política permite todas as ações do AWS Glue em todos os bancos de dados e tabelas na conta de dados. Você pode personalizar a política para conceder somente as permissões necessárias aos consumidores das entidades principais. Por exemplo, você pode fornecer acesso somente de leitura a tabelas ou visualizações específicas em um banco de dados.	

Acessar os dados da conta do consumidor

Tarefa	Descrição	Habilidades necessárias
Criar uma referência nomeada para o catálogo de dados.	Para criar uma referência de catálogo de dados nomeada, use CloudShellou uma AWS CLI instalada localmente para executar o seguinte comando: `aws athena create-data-catalog --name <shared catalog name> --type GLUE --parameters catalog-id=<data account id>`	Administrador de nuvem
Conceder ao perfil do IAM na conta do consumidor o acesso aos dados.	Anexe a política a seguir ao perfil do IAM na conta do consumidor para conceder ao perfil o acesso entre contas aos dados: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow",`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	<pre>"Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" }, { "Effect": "Allow", "Action": "glue:*", "Resource": ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> Em seguida, use o modelo a seguir para especificar quais usuários podem aceitar o perfil do IAM em sua política de confiança: <pre>{ "Version": "2012-10-17", "Statement": [</pre>	

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	"Effect": "Allow",
	"Principal": {
	"AWS": "arn:aws:iam::<consumer account id>:user/<IAM user>"
	},
	"Action": "sts:AssumeRole"
	}
	]
	}</pre>
	Por fim, conceda permissões ao usuário para assumir o perfil do IAM anexando a mesma política ao grupo de usuários ao qual ele pertence.	

Tarefa	Descrição	Habilidades necessárias
(Se necessário) Conceder ao perfil do IAM na conta do consumidor o acesso à chave de criptografia de dados.	Se o bucket do S3 for criptografado por uma chave do AWS KMS, conceda a permissão `kms:Decrypt` sobre a chave para o perfil do IAM na conta do consumidor, anexando a ela a seguinte política: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de nuvem
Mudar para o perfil do IAM na conta do consumidor para acessar os dados.	Como consumidor de dados, mude para o perfil do IAM para acessar os dados na conta de dados.	Consumidor de dados

Tarefa	Descrição	Habilidades necessárias

Acessar os dados.	Dados da consulta usando o Athena. Por exemplo, abra o editor de consultas do Athena e execute a seguinte consulta:
	`SELECT * FROM <shared catalog name>.<database name>.<table name>`
	Em vez de usar uma referênci a de catálogo nomeada, você também pode se referir ao catálogo pelo seu nome do recurso da Amazon (ARN).
	Note
	Se você usar uma referência de catálogo dinâmico em uma consulta ou exibição, coloque a referênci a entre aspas duplas de escape (\"). Por exemplo:
	`SELECT * FROM \"glue:arn:aws:glue:<region>:<data account id>:catalog\".<database name>.<table name>`
		Consumidor de dados

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte Acesso entre contas aos catálogos de dados do AWS Glue no Guia do usuário do Amazon Athena.	

Recursos relacionados

- Acesso entre contas aos catálogos de dados do AWS Glue (documentação do Athena)
- (AWS CLI) (Referência de comandos create-data-catalog da CLI da AWS)
- Acesso entre contas ao Catálogo de Dados do AWS Glue com o Amazon Athena (blog de big data da AWS)
- Práticas recomendadas de segurança no IAM (documentação do IAM)

Mais informações

Usando o Lake Formation como uma alternativa para compartilhamento entre contas

Você também pode usar o AWS Lake Formation para compartilhar o acesso aos objetos do catálogo do AWS Glue entre contas. O Lake Formation fornece controle de acesso refinado no nível de coluna e linha, controle de acesso baseado em tags, tabelas governadas para transações ACID e outras funcionalidades. Embora o Lake Formation esteja bem integrado ao Athena, ele requer configuração adicional em comparação com a abordagem exclusiva de IAM desse padrão. Recomendamos que você considere a decisão de usar o Lake Formation ou os controles de acesso somente do IAM dentro do contexto mais amplo da arquitetura geral da solução. As considerações incluem quais outros serviços estão envolvidos e como eles se integram às duas abordagens.

Converta o atributo temporal Teradata NORMALIZE em Amazon Redshift SQL

Criado por Po Hong (AWS)

Resumo

NORMALIZE é uma extensão Teradata do padrão ANSI SQL. Quando uma tabela SQL inclui uma coluna que tem um tipo de dados PERIOD, NORMALIZE combina valores que se encontram ou se sobrepõem nessa coluna para formar um único período que consolida vários valores de períodos individuais. Para usar NORMALIZE, pelo menos uma coluna na lista SQL SELECT deve ser do tipo de dados PERIOD temporal do Teradata. Para obter mais informações sobre NORMALIZE, consulte a Documentação do Teradata.

O Amazon Redshift não é compatível com NORMALIZE, mas você pode implementar essa funcionalidade usando a sintaxe SQL nativa e a função de janela LAG no Amazon Redshift. Esse padrão se concentra no uso da extensão NORMALIZE do Teradata com a condição ON MEETS OR OVERLAPS, que é o formato mais popular. Ele explica como esse atributo funciona no Teradata e como ele pode ser convertido na sintaxe SQL nativa do Amazon Redshift.

Pré-requisitos e limitações

Pré-requisitos

- Conhecimento e experiência básicos em Teradata SQL
- Conhecimento e experiência no Amazon Redshift

Arquitetura

Pilha de tecnologia de origem

- Data warehouse Teradata

Pilha de tecnologias de destino

- Amazon Redshift

Arquitetura de destino

Para obter uma arquitetura de alto nível para migrar um banco de dados Teradata para o Amazon Redshift, consulte o padrão Migrar um banco de dados Teradata para o Amazon Redshift usando agentes de extração de dados da AWS SCT. A migração não converte automaticamente a frase NORMALIZE do Teradata para SQL do Amazon Redshift. Você pode converter essa extensão do Teradata seguindo as diretrizes nesse padrão.

Ferramentas

Código

Para ilustrar o conceito e a funcionalidade do NORMALIZE, considere a seguinte definição de tabela no Teradata:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          duration      PERIOD(DATE)
     );
```

Execute o código SQL a seguir para inserir dados de exemplo na tabela:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  PERIOD(DATE '2010-01-10',
 DATE '2010-03-20') );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  PERIOD(DATE '2010-03-20',
 DATE '2010-07-15') );

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  PERIOD(DATE
 '2010-06-15', DATE '2010-08-18') );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  PERIOD(DATE '2010-03-10',
 DATE '2010-07-20') );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  PERIOD(DATE
 '2020-05-10', DATE '2020-09-20') );

END TRANSACTION;
```

Resultados:

```
select * from systest.project order by 1,2,3;
```

```
 *** Query completed. 4 rows found. 4 columns returned.
 *** Total elapsed time was 1 second.

     emp_id  project_name              dept_id  duration
-----------  --------------------  -----------  ------------------------
         10  First Phase                  1000  ('10/01/10', '10/03/20')
         10  First Phase                  2000  ('10/03/20', '10/07/15')
         10  Second Phase                 2000  ('10/06/15', '10/08/18')
         20  First Phase                  2000  ('10/03/10', '10/07/20')
         20  Second Phase                 1000  ('20/05/10', '20/09/20')
```

Caso de uso do Teradata NORMALIZE

Agora, adicione a cláusula Teradata NORMALIZE SQL à instrução SELECT:

```
SELECT NORMALIZE ON MEETS OR OVERLAPS emp_id, duration
FROM systest.project
ORDER BY 1,2;
```

Essa operação NORMALIZE é executada em uma única coluna (emp_id). Para emp_id=10, os três valores de período sobrepostos na duração se aglutinam em um único valor de período, da seguinte forma:

```
     emp_id  duration
-----------  ------------------------
         10  ('10/01/10', '10/08/18')
         20  ('10/03/10', '10/07/20')
         20  ('20/05/10', '20/09/20')
```

A instrução SELECT a seguir executa uma operação NORMALIZE em project_name e dept_id. Observe que a lista SELECT contém somente uma coluna PERIOD, duração.

```
SELECT NORMALIZE project_name, dept_id, duration
FROM systest.project;
```

Saída:

```
project_name              dept_id  duration
--------------------  -----------  ------------------------
First Phase                  1000  ('10/01/10', '10/03/20')
```

```
Second Phase                1000  ('20/05/10', '20/09/20')
First Phase                 2000  ('10/03/10', '10/07/20')
Second Phase                2000  ('10/06/15', '10/08/18')
```

SQL equivalente ao Amazon Redshift

No momento, o Amazon Redshift não oferece suporte ao tipo de dados PERIOD em uma tabela. Em vez disso, você precisa dividir um campo de dados do Teradata PERIOD em duas partes: start_date e end_date, da seguinte forma:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          start_date  DATE,
          end_date    DATE
     );
```

Insira os dados de amostra na tabela:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  DATE '2010-01-10', DATE
 '2010-03-20' );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  DATE '2010-03-20', DATE
 '2010-07-15');

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  DATE '2010-06-15', DATE
 '2010-08-18' );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  DATE '2010-03-10', DATE
 '2010-07-20' );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  DATE '2020-05-10', DATE
 '2020-09-20' );

END TRANSACTION;
```

Saída:

```
 emp_id | project_name | dept_id | start_date |  end_date
--------+--------------+---------+------------+------------
     10 | First Phase  |    1000 | 2010-01-10 | 2010-03-20
```

```
     10 | First Phase  |    2000 | 2010-03-20 | 2010-07-15
     10 | Second Phase |    2000 | 2010-06-15 | 2010-08-18
     20 | First Phase  |    2000 | 2010-03-10 | 2010-07-20
     20 | Second Phase |    1000 | 2020-05-10 | 2020-09-20
(5 rows)
```

Para reescrever a cláusula NORMALIZE do Teradata, você pode usar a função de janela LAG no Amazon Redshift. Esta função retorna os valores para uma linha em determinado deslocamento acima (antes) da linha atual na partição.

Você pode usar a função LAG para identificar cada linha que inicia um novo período determinando se um período atende ou se sobrepõe ao período anterior (0 se sim e 1 se não). Quando esse sinalizador é resumido cumulativamente, ele fornece um identificador de grupo que pode ser usado na cláusula externa Group By para chegar ao resultado desejado no Amazon Redshift.

Aqui está um exemplo de instrução SQL do Amazon Redshift que usa LAG():

```
SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project
ORDER BY 1,2;
```

Saída:

```
 emp_id | start_date |  end_date  | groupstartflag
--------+------------+------------+----------------
     10 | 2010-01-10 | 2010-03-20 |              1
     10 | 2010-03-20 | 2010-07-15 |              0
     10 | 2010-06-15 | 2010-08-18 |              0
     20 | 2010-03-10 | 2010-07-20 |              1
     20 | 2020-05-10 | 2020-09-20 |              1
(5 rows)
```

A seguinte instrução SQL do Amazon Redshift normaliza somente na coluna emp_id:

```
SELECT T2.emp_id, MIN(T2.start_date) as new_start_date, MAX(T2.end_date) as
 new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY emp_id ORDER BY start_date ROWS
 UNBOUNDED PRECEDING) As GroupID
```

```
FROM ( SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.emp_id, T2.GroupID
ORDER BY 1,2;
```

Saída:

```
 emp_id | new_start_date | new_end_date
--------+----------------+-------------------------------------
     10 | 2010-01-10     | 2010-08-18
     20 | 2010-03-10     | 2010-07-20
     20 | 2020-05-10     | 2020-09-20
(3 rows)
```

A seguinte instrução SQL do Amazon Redshift normaliza em ambas as colunas project_name e dept_id:

```
SELECT T2.project_name, T2.dept_id, MIN(T2.start_date) as new_start_date,
 MAX(T2.end_date) as new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY project_name, dept_id ORDER BY
 start_date ROWS UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT project_name, dept_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY project_name,
 dept_id ORDER BY start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.project_name, T2.dept_id, T2.GroupID
ORDER BY 1,2,3;
```

Saída:

```
 project_name | dept_id | new_start_date | new_end_date
--------------+---------+----------------+--------------
 First Phase  |    1000 | 2010-01-10     | 2010-03-20
 First Phase  |    2000 | 2010-03-10     | 2010-07-20
 Second Phase |    1000 | 2020-05-10     | 2020-09-20
```

```
 Second Phase |    2000 | 2010-06-15     | 2010-08-18
(4 rows)
```

Épicos

Converta NORMALIZE em Amazon Redshift SQL

Tarefa	Descrição	Habilidades necessárias
Crie o seu código SQL do Teradata.	Use a frase NORMALIZE de acordo com as suas necessidades.	SQL Developer
Converter o código para Amazon Redshift SQL.	Para converter seu código, siga as diretrizes na seção “Ferramentas” desse padrão.	SQL Developer
Executar o código no Amazon Redshift.	Crie sua tabela, carregue dados na tabela e execute seu código no Amazon Redshift.	SQL Developer

Recursos relacionados

Referências

- Atributo temporal do Teradata NORMALIZE (documentação do Teradata)
- Função de janela LAG (documentação do Amazon Redshift)
- Migre para o Amazon Redshift (site da AWS)
- Migre um banco de dados Teradata para o Amazon Redshift usando agentes de extração de dados da AWS SCT (Recomendações da AWS)
- Converta o atributo Teradata RESET WHEN para o Amazon Redshift SQL (Recomendações da AWS)

Ferramentas

- AWS Schema Conversion Tool (AWS SCT)

Parceiros

- Parceiros de competência em migração da AWS

Converter o atributo Teradata RESET WHEN para Amazon Redshift SQL

Criado por Po Hong (AWS)

Resumo

RESET WHEN é um atributo do Teradata usado nas funções de janela analítica do SQL. É uma extensão do padrão ANSI SQL. RESET WHEN determina a partição na qual uma função de janela SQL opera com base em alguma condição especificada. Se a condição for avaliada como TRUE, uma nova subpartição dinâmica será criada dentro da partição da janela existente. Para obter mais informações sobre RESET WHEN, consulte a Documentação do Teradata.

O Amazon Redshift não oferece suporte para RESET WHEN em funções de janela SQL. Para implementar essa funcionalidade, você precisa converter RESET WHEN para a sintaxe SQL nativa no Amazon Redshift e usar várias funções aninhadas. Esse padrão demonstra como você pode usar o atributo do Teradata RESET WHEN e como convertê-lo para a sintaxe SQL do Amazon Redshift.

Pré-requisitos e limitações

Pré-requisitos

- Conhecimento básico do data warehouse Teradata e sua sintaxe SQL
- Bom entendimento do Amazon Redshift e de sua sintaxe SQL

Arquitetura

Pilha de tecnologia de origem

- Data warehouse Teradata

Pilha de tecnologias de destino

- Amazon Redshift

Arquitetura

Para obter uma arquitetura de alto nível para migrar um banco de dados Teradata para o Amazon Redshift, consulte o padrão Migrar um banco de dados Teradata para o Amazon Redshift usando agentes de extração de dados do AWS SCT. A migração não converte automaticamente a frase RESET WHEN do Teradata em SQL do Amazon Redshift. Você pode converter essa extensão do Teradata seguindo as diretrizes na próxima seção.

Ferramentas

Código

Para ilustrar o conceito e a funcionalidade do RESET WHEN, considere a seguinte definição de tabela no Teradata:

```
create table systest.f_account_balance
( account_id integer NOT NULL,
  month_id integer,
  balance integer )
unique primary index (account_id, month_id);
```

Execute o código SQL a seguir para inserir dados de exemplo na tabela:

```
BEGIN TRANSACTION;
Insert Into systest.f_account_balance values (1,1,60);
Insert Into systest.f_account_balance values (1,2,99);
Insert Into systest.f_account_balance values (1,3,94);
Insert Into systest.f_account_balance values (1,4,90);
Insert Into systest.f_account_balance values (1,5,80);
Insert Into systest.f_account_balance values (1,6,88);
Insert Into systest.f_account_balance values (1,7,90);
Insert Into systest.f_account_balance values (1,8,92);
Insert Into systest.f_account_balance values (1,9,10);
Insert Into systest.f_account_balance values (1,10,60);
Insert Into systest.f_account_balance values (1,11,80);
Insert Into systest.f_account_balance values (1,12,10);
END TRANSACTION;
```

A tabela de amostra tem os seguintes dados:

account_id	month_id	balance

1	1	60
1	2	99
1	3	94
1	4	90
1	5	80
1	6	88
1	7	90
1	8	92
1	9	10
1	10	60
1	11	80
1	12	10

Para cada conta, suponhamos que você queira analisar a sequência de aumentos de saldo mensais consecutivos. Quando o saldo de um mês for menor ou igual ao saldo do mês anterior, o requisito é zerar o contador e reiniciá-lo.

Caso de uso do RESET WHEN do Teradata

Para analisar esses dados, o Teradata SQL usa uma função de janela com um agregado aninhado e uma frase RESET WHEN, da seguinte forma:

```
SELECT account_id, month_id, balance,
 ( ROW_NUMBER() OVER (PARTITION BY account_id ORDER BY month_id
RESET WHEN balance <= SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS
 BETWEEN 1 PRECEDING AND 1 PRECEDING) ) -1 ) as balance_increase
FROM systest.f_account_balance
ORDER BY 1,2;
```

Saída:

account_id	month_id	balance	balance_increase
1	1	60	0
1	2	99	1
1	3	94	0
1	4	90	0
1	5	80	0
1	6	88	1
1	7	90	2
1	8	92	3
1	9	10	0
1	10	60	1
1	11	80	2
1	12	10	0

A consulta é processada da seguinte forma no Teradata:

1. A função agregada SUM (balance) calcula a soma de todos os saldos de uma determinada conta em um determinado mês.
2. Verificamos se o saldo em um determinado mês (para uma determinada conta) é maior que o saldo do mês anterior.
3. Se o saldo aumentar, rastreamos um valor de contagem cumulativa. Se a condição RESET WHEN avalia como falsa, o que significa que o saldo aumentou em meses sucessivos, a contagem continua aumentando.
4. A função analítica ordenada ROW_NUMBER () calcula o valor da contagem. Quando atingimos um mês cujo saldo é menor ou igual ao saldo do mês anterior, a condição RESET WHEN é avaliada como verdadeira. Nesse caso, iniciamos uma nova partição e ROW_NUMBER () reinicia

a contagem a partir de 1. Usamos LINHAS ENTRE 1 ANTERIOR E 1 ANTERIOR para acessar o valor da linha anterior.

5. Subtraímos 1 para garantir que o valor da contagem comece com 0.

SQL equivalente ao Amazon Redshift

O Amazon Redshift não oferece suporte para RESET WHEN em uma função de janela SQL analítica. Para produzir o mesmo resultado, você deve reescrever o SQL Teradata usando a sintaxe SQL nativa do Amazon Redshift e subconsultas aninhadas, da seguinte forma:

```
SELECT account_id, month_id, balance,
   (ROW_NUMBER() OVER(PARTITION BY account_id, new_dynamic_part ORDER BY month_id) -1)
 as balance_increase
FROM
( SELECT account_id, month_id, balance, prev_balance,
SUM(dynamic_part) OVER (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN
 UNBOUNDED PRECEDING AND CURRENT ROW) As new_dynamic_part
FROM ( SELECT account_id, month_id, balance,
SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN 1 PRECEDING
 AND 1 PRECEDING) as prev_balance,
(CASE When balance <= prev_balance Then 1 Else 0 END) as dynamic_part
FROM systest.f_account_balance ) A
) B
ORDER BY 1,2;
```

Como o Amazon Redshift não oferece suporte a funções de janela aninhadas na cláusula SELECT de uma única instrução SQL, você deve usar duas subconsultas aninhadas.

- Na subconsulta interna (alias A), um indicador de partição dinâmica (dynamic_part) é criado e preenchido. O dynamic_part é definido como 1 se o saldo de um mês for menor ou igual ao saldo do mês anterior; caso contrário, será definido como 0.
- Na próxima camada (alias B), um atributo new_dynamic_part é gerado como resultado de uma função de janela SUM.
- Finalmente, você adiciona new_dynamic_part como um novo atributo de partição (partição dinâmica) ao atributo de partição existente (account_id) e aplica a mesma função de janela ROW_NUMBER() que em Teradata (e menos um).

Depois dessas alterações, o Amazon Redshift SQL gera a mesma saída que o Teradata.

Épicos

Converter o RESET WHEN para Amazon Redshift SQL

Tarefa	Descrição	Habilidades necessárias
Criar sua função de janela Teradata.	Use agregados aninhados e a frase RESET WHEN de acordo com as suas necessidades.	SQL Developer
Converter o código para Amazon Redshift SQL.	Para converter seu código, siga as diretrizes na seção “Ferramentas” desse padrão.	SQL Developer
Executar o código no Amazon Redshift.	Crie sua tabela, carregue dados na tabela e execute seu código no Amazon Redshift.	SQL Developer

Recursos relacionados

Referências

- Frase RESET WHEN (documentação da Teradata)
- Explicação do RESET WHEN (estouro de pilha)
- Migre para o Amazon Redshift (site da AWS)
- Migre um banco de dados Teradata para o Amazon Redshift usando agentes de extração de dados do AWS SCT (Recomendações da AWS)
- Converta o atributo temporal Teradata NORMALIZE no Amazon Redshift SQL (Recomendações da AWS)

Ferramentas

- AWS Schema Conversion Tool (AWS SCT)

Parceiros

- Parceiros de competência em migração da AWS

Implante e gerencie um data lake de tecnologia sem servidor na Nuvem AWS usando a infraestrutura como código

Criado por Kirankumar Chandrashekar (AWS) e Abdel Jaidi (AWS)

Resumo

Aviso: CodeCommit A AWS não está mais disponível para novos clientes. Os clientes atuais da AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Este padrão descreve como usar a computação de tecnologia sem servidor e a infraestrutura como código (IaC) para implementar e administrar um data lake na Nuvem da Amazon Web Services (AWS). Esse padrão é baseado no workshop da serverless data lake framework (SDLF) (Estrutura de data lake de tecnologia sem servidor) desenvolvido pela AWS.

A SDLF é uma coleção de recursos reutilizáveis que aceleram a entrega de data lakes corporativos na Nuvem AWS e ajudam a acelerar a implantação na produção. Ela é usada para implementar a estrutura básica de um data lake seguindo as práticas recomendadas.

O SDLF implementa um processo de integração contínua/implantação contínua (CI/CD) em toda a implantação do código e da infraestrutura usando serviços da AWS, como AWS, AWS e CodePipeline AWS. CodeBuild CodeCommit

Esse padrão usa vários serviços de tecnologia sem servidor da AWS para simplificar o gerenciamento de data lake. Isso inclui o Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB para armazenamento, o AWS Lambda e o AWS Glue para computação e o Amazon Events, o Amazon Simple Queue Service (Amazon SQS) CloudWatch e o AWS Step Functions para orquestração.

A AWS CloudFormation e os serviços de código da AWS atuam como a camada de IaC para fornecer implantações rápidas e reproduzíveis com operações e administração fáceis.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI), instalada e configurada.

- Um cliente Git, instalado e configurado.
- O workshop da SDLF, aberto em uma janela do navegador da web e pronto para uso.

Arquitetura

O diagrama de arquitetura ilustra um processo orientado por eventos com as etapas a seguir.

1. Depois que um arquivo é adicionado ao bucket do S3 de dados brutos, uma notificação de evento do Amazon S3 é colocada em uma fila do SQS. Cada notificação é entregue como um arquivo JSON, que contém metadados como o nome do bucket do S3, a chave do objeto ou o timestamp.
2. Essa notificação é consumida por uma função do Lambda que roteia o evento para o processo correto de extração, transformação e carregamento (ETL) com base nos metadados. A função do Lambda também pode usar configurações contextuais armazenadas em uma tabela do Amazon DynamoDB. Essa etapa permite o desacoplamento e o escalonamento para vários aplicativos no data lake.
3. O evento é roteado para a primeira função do Lambda no processo de ETL, que transforma e move dados da área de dados brutos para a área de preparação do data lake. A primeira etapa é atualizar o catálogo abrangente. Essa é uma tabela do DynamoDB que contém todos os metadados do arquivo do data lake. Cada linha nessa tabela contém metadados operacionais sobre um único objeto armazenado no Amazon S3. Uma chamada síncrona é feita para uma função do Lambda que executa uma transformação leve, que é uma operação computacionalmente barata (como converter um arquivo de um formato para outro), no objeto S3. Como um novo objeto foi adicionado ao bucket temporário do S3, o catálogo abrangente é atualizado e uma mensagem é enviada para a fila do SQS aguardando a próxima fase no ETL.
4. Uma regra de CloudWatch eventos aciona uma função Lambda a cada 5 minutos. Essa função verifica se as mensagens foram entregues à fila SQS da fase ETL anterior. Se uma mensagem foi entregue, a função do Lambda inicia a segunda função do AWS Step Functions no processo de ETL.
5. Uma transformação intensa é então aplicada em um lote de arquivos. Essa transformação pesada é uma operação computacionalmente cara, como uma chamada síncrona para uma tarefa do AWS Glue, uma tarefa do AWS Fargate, uma etapa do Amazon EMR ou um notebook da Amazon. SageMaker Os metadados da tabela são extraídos dos arquivos de saída usando um crawler do AWS Glue, que atualiza o catálogo do AWS Glue. Os metadados do arquivo também são adicionados à tabela abrangente do catálogo no DynamoDB. Por fim, uma etapa de qualidade de dados aproveitando o Deequ também é executada.

Pilha de tecnologia

- CloudWatch Eventos da Amazon
- AWS CloudFormation
- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- Amazon DynamoDB
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SQS
- AWS Step Functions

Ferramentas

- Amazon CloudWatch Events — CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- AWS CloudFormation — CloudFormation ajuda a criar e provisionar implantações de infraestrutura da AWS de forma previsível e repetida.
- AWS CodeBuild — CodeBuild é um serviço de construção totalmente gerenciado que compila seu código-fonte, executa testes unitários e produz artefatos prontos para implantação.
- AWS CodeCommit — CodeCommit é um serviço de controle de versão hospedado pela AWS que você pode usar para armazenar e gerenciar ativos de forma privada (como código-fonte e arquivos binários).
- AWS CodePipeline — CodePipeline é um serviço de entrega contínua que você pode usar para modelar, visualizar e automatizar as etapas necessárias para liberar suas alterações de software continuamente.
- Amazon DynamoDB: o DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade.
- AWS Glue: o AWS Glue é um serviço de ETL totalmente gerenciado que facilita a preparação e o carregamento de dados para análise.

- AWS Lambda: o Lambda é compatível com a execução de código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável. O Amazon S3 pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- AWS Step Functions: o AWS Step Functions é um orquestrador de funções de tecnologia sem servidor que facilita o sequenciamento de funções do Lambda na AWS e a multiplicação dos serviços da AWS em aplicativos essenciais para os negócios.
- Amazon SQS: o Amazon Simple Queue Service (Amazon SQS) é um serviço de enfileiramento de mensagens totalmente gerenciado que ajuda você a desacoplar e escalar microsserviços, sistemas distribuídos e aplicativos de tecnologia sem servidor.
- Deequ: o Deequ é uma ferramenta que ajuda você a calcular métricas de qualidade de dados para grandes conjuntos de dados, definir e verificar restrições de qualidade de dados e se manter informado sobre mudanças na distribuição de dados.

Repositório de código

O código-fonte e os recursos do SDLF estão disponíveis no GitHub repositório do AWS Labs.

Épicos

Configure o pipeline de CI/CD para provisionar IaC

Tarefa	Descrição	Habilidades necessárias
Configure o pipeline de CI/CD para gerenciar o IaC para o data lake.	Faça login no Console de Gerenciamento da AWS e siga as etapas da seção Configuração inicial do workshop da SDLF. Isso cria os recursos iniciais de CI/CD, como CodeCommit repositór ios, CodeBuild ambientes e CodePipeline pipelines que	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	provisionam e gerenciam a IaC para o data lake.	

Controle de versão do IaC

Tarefa	Descrição	Habilidades necessárias
Clone o CodeCommit repositório em sua máquina local.	Siga as etapas da seção Deploying the foundations (Implantação dos fundamentos) do workshop da SDLF. Isso ajuda você a clonar o repositório Git que hospeda o IaC em seu ambiente local. Para obter mais informações, consulte Conexão com CodeCommit repositórios na CodeCommit documentação.	DevOps engenheiro
Modifique os CloudFormation modelos.	Use sua estação de trabalho local e um editor de código para modificar os CloudFormation modelos de acordo com seus casos de uso ou requisitos. Confirme-os no repositório Git clonado localmente. Para obter mais informações, consulte Como trabalhar com CloudFormation modelos da AWS na CloudFormation documentação da AWS.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Envie as alterações para o CodeCommit repositório.	Seu código de infraestrutura agora está sob controle de versão e as modificações em sua base de código são rastreadas. Quando você envia uma alteração para o CodeCommit repositório, a aplica CodePipeline automatic amente à sua infraestrutura e a entrega para CodeBuild. **Important** Se você usa a CLI do AWS SAM em CodeBuild, execute os comandos `sam package` e. `sam deploy` Se você usa a AWS CLI, execute os comandos `aws cloudformation package` e `aws cloudformation deploy`.	DevOps engenheiro

Recursos relacionados

Configure o pipeline de CI/CD para provisionar IaC

- Workshop SDLF: configuração inicial

Controle de versão do IaC

- Workshop da SDLF: Deploying the foundations (Implantação das fundações)
- Conectando-se a CodeCommit repositórios
- Trabalhando com CloudFormation modelos da AWS

Outros recursos

- AWS serverless data analytics pipeline reference architecture (Arquitetura de referência do pipeline de análise de dados sem servidor da AWS)
- Documentação da SDLF

Imponha a marcação dos clusters do Amazon EMR no lançamento

Criado por Priyanka Chaudhary (AWS)

Resumo

Esse padrão fornece um controle de segurança que garante que os clusters do Amazon EMR sejam marcados quando são criados.

O Amazon EMR é um serviço da Amazon Web Services (AWS) para processar e analisar grandes quantidades de dados. O Amazon EMR oferece um serviço expansível e de baixa configuração como uma alternativa mais fácil à execução da computação em cluster interna. Você pode usar tags para categorizar os recursos da AWS de diferentes formas, como por finalidade, proprietário ou ambiente. Por exemplo, você pode marcar seus clusters do Amazon EMR atribuindo metadados personalizados a cada cluster. Uma tag consiste em uma chave e um valor que você define. Recomendamos criar um conjunto consistente de tags para atender às necessidades da sua organização. Quando você adiciona uma tag a um cluster do Amazon EMR, a tag também é propagada para cada instância ativa do Amazon Elastic Compute Cloud (Amazon EC2) associada ao cluster. Da mesma forma, quando você remove uma tag de um cluster do Amazon EMR, essa tag também é removida de cada EC2 instância ativa associada.

O controle de detetives monitora as chamadas de API e inicia um evento Amazon CloudWatch Events para o RunJobFlow, AddTagsRemoveTags, e. CreateTags APIs O evento chama de AWS Lambda, que executa um script do Python. A função Python obtém o ID do cluster do Amazon EMR da entrada JSON do evento e executa as seguintes verificações:

- Verifique se o cluster do Amazon EMR está configurado com nomes de tag que você especifica.
- Caso contrário, envie uma notificação do Amazon Simple Notification Service (Amazon SNS) ao usuário com as informações relevantes: nome do cluster do Amazon EMR, detalhes da violação, região da AWS, conta da AWS e o nome do recurso da Amazon (ARN) do Lambda, de onde essa notificação foi originada.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa

- Um bucket do Amazon Simple Storage Service (Amazon S3) para carregar o código do Lambda fornecido. Ou você pode criar um bucket do S3 para essa finalidade, conforme descrito na seção Épicos .
- Um endereço de e-mail ativo no qual você deseja receber notificações de violação.
- Uma lista de tags obrigatórias que você deseja verificar.

Limitações

- Esse controle de segurança é regional. Você deve implantá-lo em cada região da AWS que você deseja monitorar.

Versões do produto

- Versão 4.8.0 e posterior do Amazon EMR.

Arquitetura

Arquitetura de fluxo de trabalho

Automação e escala

- Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

Serviços da AWS

- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em várias contas e regiões da AWS.
- Amazon CloudWatch Events — A Amazon CloudWatch Events oferece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.

- Amazon EMR: o Amazon EMR é um serviço web que simplifica a execução de estruturas de big data e o processamento eficiente de grandes quantidades de dados.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

Esse padrão inclui os seguintes anexos:

- `EMRTagValidation.zip`: o código Lambda para o controle de segurança.
- `EMRTagValidation.yml`— O CloudFormation modelo que configura o evento e a função Lambda.

Épicos

Configurar o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	No console do Amazon S3, escolha ou crie um bucket do S3 para hospedar o arquivo .zip do código Lambda. O bucket do S3 deve estar na mesma região da AWS que o cluster do Amazon EMR que você deseja monitorar. Um nome	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	de bucket do Amazon S3 é globalmente exclusivo, e o namespace é compartilhado por todas as contas da AWS. O nome do bucket do S3 não pode incluir barras iniciais.	
Fazer o upload do código do Lambda.	Faça upload do arquivo .zip do código do Lambda fornecido na seção Anexos no bucket do S3.	Arquiteto de nuvem

Implemente o CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo da AWS.	Abra o CloudFormation console da AWS na mesma região da AWS do seu bucket do S3 e implante o modelo. Para obter mais informaçõ es sobre a implantação de CloudFormation modelos da AWS, consulte Como criar uma pilha no CloudForm ation console da AWS na CloudFormation documenta ção.	Arquiteto de nuvem
Preencher os parâmetros no modelo.	Ao iniciar o modelo, você será solicitado a fornecer as seguintes informações:	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	• Bucket S3: especifique o bucket que você criou ou selecionou no primeiro épico. É onde que você fez o upload do código do Lambda anexado (arquivo .zip). • Chave do S3: especifique a localização do arquivo .zip do Lambda em seu bucket do S3 (por exemplo, nome do arquivo.zip ou controles /nome do arquivo.zip). Não inclua barras iniciais. • E-mail de notificação: Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS. • Marcação de nomes de chaves: forneça as tags que você deseja verificar em uma lista separada por vírgulas (por exemplo, `ApplicationID` , `Environment` , `Owner`). O evento CloudWatch Events monitora o cluster em busca dessas tags e envia uma notificação se elas não forem encontradas. • Nível de registro do Lambda: especifique o nível de registro e a frequência	

Tarefa	Descrição	Habilidades necessárias
	da função do Lambda. Use Informações para registrar em log mensagens informativas detalhadas sobre o progresso, Erro para eventos de erro que ainda permitiriam a continuidade da implantação e Aviso sobre situações potencialmente prejudiciais.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o CloudFormation modelo é implantado com sucesso, ele envia um e-mail de assinatura para o endereço de e-mail que você forneceu. Você deve confirmar essa assinatura de e-mail para começar a receber notificações de violação.	Arquiteto de nuvem

Recursos relacionados

- Guia do desenvolvedor do AWS Lambda
- Como colocar tags nos clusters do Amazon EMR

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Garanta que o registro do Amazon EMR no Amazon S3 esteja habilitado no lançamento

Criado por Priyanka Chaudhary (AWS)

Resumo

Esse padrão fornece um controle de segurança que monitora a configuração de log para clusters do Amazon EMR executados na Amazon Web Services (AWS).

O Amazon EMR é uma ferramenta da AWS para processamento e análise de big data. O Amazon EMR oferece o serviço expansível de baixa configuração como alternativa à execução da computação em cluster interna. O Amazon EMR fornece dois tipos de clusters EMR.

- Clusters transitórios do Amazon EMR: os clusters transitórios do Amazon EMR são desligados automaticamente e param de incorrer em custos quando o processamento é concluído.
- Clusters persistentes do Amazon EMR: os clusters persistentes do Amazon EMR continuam em execução após a conclusão do trabalho de processamento de dados.

Tanto o Amazon EMR como o Hadoop produzem arquivos de log que informam o status no cluster. Por padrão, eles são gravados no nó principal no diretório mnt/var/log//. Dependendo de como você configura o cluster ao iniciá-lo, também poderá salvar esses logs no Amazon Simple Storage Service (Amazon S3) e visualizá-los por meio da ferramenta de depuração gráfica. Observe que o registro em log do Amazon S3 só pode ser especificado quando o cluster é iniciado. Com essa configuração, os registros são enviados do nó primário para o local do Amazon S3 a cada cinco minutos. Para clusters transitórios, o registro no Amazon S3 é importante porque os clusters desaparecem quando o processamento é concluído, e esses arquivos de log podem ser usados para depurar qualquer trabalho com falha.

O padrão usa um CloudFormation modelo da AWS para implantar um controle de segurança que monitora as chamadas de API e inicia o Amazon CloudWatch Events em ""RunJobFlow. O gatilho invoca o AWS Lambda, que executa um script Python. A função do Lambda recupera o ID do cluster EMR da entrada JSON do evento e também verifica se há um URI de log do Amazon S3. Se um URI do Amazon S3 não for encontrado, a função do Lambda enviará uma notificação do Amazon Simple Notification Service (Amazon SNS) detalhando o nome do cluster do EMR, os detalhes da violação, a região da AWS, a conta da AWS e o nome do recurso da Amazon (ARN) do Lambda do qual a notificação foi originada.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket S3 para o arquivo .zip do código Lambda
- Um endereço de e-mail no qual você deseja receber a notificação de violação

Limitações

- Esse controle de detetive é regional e deve ser implantado nas regiões da AWS que você pretende monitorar.

Versões do produto

- Versão 4.8.0 e posterior do Amazon EMR

Arquitetura

Pilha de tecnologias de destino

- Evento Amazon CloudWatch Events
- Amazon EMR
- Função do Lambda
- Bucket do S3
- Amazon SNS

Arquitetura de destino

Automação e escala

- Se você estiver usando o AWS Organizations, você pode usar CloudFormation StackSets a AWS para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

Ferramentas

- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar recursos da AWS usando a infraestrutura como código.
- Eventos do AWS Cloudwatch — O AWS CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- Amazon EMR: o Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de Big Data.
- AWS Lambda: o AWS Lambda oferece suporte à execução de código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- Amazon S3: o Amazon S3 é uma interface de serviços da web que você pode usar para armazenar e recuperar qualquer quantidade de dados, a qualquer momento, em qualquer lugar da web.
- Amazon SNS: o Amazon SNS é um serviço da Web que coordena e gerencia a entrega ou o envio de mensagens entre editores e clientes, incluindo servidores da Web e endereços de e-mail.

Código

- Um arquivo .zip do projeto está disponível como anexo.

Épicos

Definir o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	Para hospedar o arquivo .zip do código Lambda, escolha ou crie um bucket do S3 com um nome exclusivo que não contenha barras iniciais. Um nome de bucket do S3 é globalmente exclusivo, e o	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	namespace é compartilhado por todas as contas da AWS. Seu bucket do S3 precisa estar na mesma região da AWS do cluster do Amazon EMR que está sendo avaliado.	

Carregar o código do Lambda para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Carregue o código do Lambda para o bucket do S3.	Faça upload do arquivo .zip do código Lambda fornecido na seção “Anexos” para o bucket do S3. O bucket do S3 deve estar na mesma região da que o cluster do Amazon EMR que está sendo avaliado.	Arquiteto de nuvem

Implemente o CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo da AWS.	No CloudFormation console da AWS, na mesma região do seu bucket do S3, implante o CloudFormation modelo da AWS que é fornecido como anexo a esse padrão. No próximo épico, forneça os valores para os parâmetros. Para obter mais informaçõ es sobre a implantação de CloudFormation modelos	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	da AWS, consulte a seção “Recursos relacionados”.	

Preencha os parâmetros no CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Dê um nome ao bucket do S3.	Em seguida, informe o nome do bucket do S3 que você criou no primeiro épico.	Arquiteto de nuvem
Forneça a chave do Amazon S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, <diretório>/<nome do arquivo>.zip).	Arquiteto de nuvem
Forneça um endereço de e-mail.	Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS.	Arquiteto de nuvem
Defina o nível de registro em log.	Defina o nível de registro e a frequência da sua função do Lambda. “Info” (Informaç ões) designa mensagens informativas detalhadas sobre o progresso do aplicativ o. “Error” (Erro) designa eventos de erro que ainda podem permitir que o aplicativ o continue em execução. “Warning” (Aviso) designa situações potencialmente prejudiciais.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail fornecido. Você deve confirmar essa assinatura de e-mail para receber notificações de violação.	Arquiteto de nuvem

Recursos relacionados

- AWS Lambda
- Registro em log no Amazon EMR
- Implantação de modelos da AWS CloudFormation

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Gerar dados de teste usando um trabalho do AWS Glue e Python

Criado por Moinul Al-Mamun (AWS)

Resumo

Este padrão mostra como gerar de forma rápida e fácil milhões de arquivos de exemplo simultaneamente criando um trabalho do AWS Glue escrito em Python. Os arquivos de exemplo são armazenados em um bucket do Amazon Simple Storage Service (Amazon S3). A capacidade de gerar rapidamente um grande número de arquivos de exemplo é importante para testar ou avaliar serviços na Nuvem AWS. Por exemplo, você pode testar o desempenho das DataBrew tarefas do AWS Glue Studio ou do AWS Glue realizando análises de dados em milhões de arquivos pequenos em um prefixo do Amazon S3.

Embora você possa usar outros serviços da AWS para gerar conjuntos de dados de exemplo, recomendamos que você use o AWS Glue. Você não precisa gerenciar nenhuma infraestrutura porque o AWS Glue é um serviço de processamento de dados com tecnologia sem servidor. Você pode simplesmente trazer seu código e executá-lo em um cluster do AWS Glue. Além disso, o AWS Glue provisiona, configura e escala os recursos necessários para executar seus trabalhos. Você paga apenas pelos recursos que o seu trabalho utilizar quando estiver sendo executado.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI), instalada e configurada para sua conta da AWS

Versões do produto

- Python 3.9
- AWS CLI versão 2

Limitações

O número máximo de trabalhos do AWS Glue por Trigger é 50. Para obter mais informações, consulte Endpoints e cotas do AWS Glue.

Arquitetura

O diagrama a seguir mostra um exemplo de arquitetura centrada em um trabalho do AWS Glue que grava sua saída (ou seja, arquivos de exemplo) em um bucket do S3.

O diagrama inclui o seguinte fluxo de trabalho:

1. Você usa a AWS CLI, o Console de gerenciamento da AWS ou uma API para iniciar o trabalho do AWS Glue. A AWS CLI ou API permite que você automatize a paralelização do trabalho invocado e reduza o runtime para gerar arquivos de exemplo.
2. O trabalho do AWS Glue gera conteúdo de arquivo aleatoriamente, converte o conteúdo em formato CSV e, em seguida, armazena o conteúdo como um objeto do Amazon S3 sob um prefixo comum. Cada arquivo tem menos de um kilobyte. O trabalho do AWS Glue aceita dois parâmetros de trabalho definidos pelo usuário: `START_RANGE` e `END_RANGE`. Você pode usar esses parâmetros para definir os nomes dos arquivos e o número de arquivos gerados no Amazon S3 por cada execução de trabalho. Você pode executar várias instâncias desse trabalho em paralelo (por exemplo, 100 instâncias).

Ferramentas

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

Práticas recomendadas

Considere as seguintes práticas recomendadas do AWS Glue ao implementar esse padrão:

- Use o tipo certo de processamento do AWS Glue para reduzir custos. Recomendamos que você entenda as diferentes propriedades dos tipos de trabalhadores e, em seguida, escolha o tipo de trabalhador certo para sua workload com base nos requisitos de CPU e memória. Para esse padrão, recomendamos que você use um trabalho de shell do Python como seu tipo de trabalho para minimizar a DPU e reduzir os custos. Para obter mais informações, consulte Adicionar trabalhos no AWS Glue, no Guia do desenvolvedor do AWS Glue.
- Use o limite correto de simultaneidade para escalar seu trabalho. Recomendamos que você baseie a simultaneidade máxima do seu trabalho no AWS Glue na sua necessidade de tempo e no número necessário de arquivos.
- Comece a gerar um pequeno número de arquivos primeiro. Para reduzir custos e economizar tempo ao criar seus trabalhos do AWS Glue, comece com um pequeno número de arquivos (como 1.000). Isso pode facilitar a solução de problemas. Se a geração de um pequeno número de arquivos for bem-sucedida, você poderá escalar para um número maior de arquivos.
- Execute localmente primeiro. Para reduzir custos e economizar tempo ao criar seus trabalhos do AWS Glue, inicie o desenvolvimento localmente e teste seu código. Para obter instruções sobre como configurar um contêiner do Docker que possa ajudar você a escrever trabalhos de extração, transformação e carregamento (ETL) do AWS Glue em um shell e em um ambiente de desenvolvimento integrado (IDE), consulte a postagem Desenvolver trabalhos de ETL do AWS Glue localmente usando um contêiner do blog AWS Big Data.

Para obter mais práticas recomendadas do AWS Glue, consulte Práticas recomendadas na documentação do AWS Glue.

Épicos

Criar um bucket do S3 e um perfil do IAM de destino

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3 para armazenar os arquivos.	Crie um bucket do S3 e um prefixo dentro dele. **Note** Esse padrão usa a `s3://{your-s3-bucket-name}/`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`small-files/` localização para fins de demonstração.	

Tarefa	Descrição	Habilidades necessárias
Criar e configurar um perfil do IAM.	Você deve criar um perfil do IAM que seu trabalho do AWS Glue possa usar para gravar em seu bucket do S3. 1. Crie um perfil do IAM (por exemplo, chamado `"AWSGlueServiceRole-smallfiles"`). 2. Escolha o AWS Glue como a entidade confiável da política. 3. Anexe uma política gerenciada pela AWS chamada `"AWSGlueServiceRole"` ao perfil. 4. Crie uma política em linha ou uma política gerenciada pelo cliente chamada `"s3-small-file-access"` com base na configuração a seguir. Substitua `"{bucket}"` pelo nome do seu bucket. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject",`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	<pre>"s3:PutObject"
	            ],
	            "Resource
	": [
	
	"arn:aws:s3:::{buc
	ket}/small-files/i
	nput/*"
	            ]
	        }
	    ]
	}</pre>
	5. Anexe sua política `"s3-small-file-access"` ao perfil.	

Criar e configurar um trabalho do AWS Glue para lidar com execuções simultâneas

Tarefa	Descrição	Habilidades necessárias
Criar um trabalho do AWS Glue.	Você deve criar um trabalho do AWS Glue que gere seu conteúdo e o armazene em um bucket do S3. Crie um trabalho do AWS Glue e, em seguida, configure seu trabalho seguindo as seguintes etapas: 1. Faça login no Console de Gerenciamento da AWS e abra o Console do AWS Glue.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	2. No painel de navegação, em Integração de dados e ETL, escolha Trabalhos. 3. Na seção Criar trabalho, escolha o editor Scripts de shell do Python. 4. Na seção Opções, selecione Criar um novo script com código clichê e escolha Criar. 5. Escolha Detalhes do trabalho. 6. Em Nome, insira create_small_files. 7. Em Perfil do IAM, selecione o perfil do IAM que você criou anteriormente. 8. Na seção Este trabalho é executado, escolha Um novo script de sua autoria. 9. Escolha Propriedades avançadas. 10. Em Simultaneidade máxima, insira 100 para fins de demonstração. Observação: a simultaneidade máxima define quantas instâncias do trabalho você pode executar paralelamente. 11. Escolha Salvar.	

Tarefa	Descrição	Habilidades necessárias

Atualizar o código do trabalho.	1. Abra o Console do AWS Glue.
	2. No painel de navegação, escolha Trabalhos.
	3. Na seção Seus trabalhos, escolha o trabalho que você criou anteriormente.
	4. Escolha a guia Script e atualize o script com base no código a seguir. Atualize as variáveis `BUCKET_NAME`, `PREFIX` e `text_str` com seus valores.
	
	`from awsglue.utils import getResolvedOptions`
	`import sys`
	`import boto3`
	`from random import randrange`
	
	`# Two arguments`
	`args = getResolvedOptions(sys.argv, ['START_RANGE', 'END_RANGE'])`
	
	`START_RANGE = int(args['START_RANGE'])`
	`END_RANGE = int(args['END_RANGE'])`
	
	`BUCKET_NAME = '{BUCKET_NAME}'`
	`PREFIX = 'small-files/input/'`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	s3 = boto3.res
	ource('s3')
	for x in range(STA
	RT_RANGE, END_RANGE
	):
	    # generate file
	 name
	    file_name =
	 f"input_{x}.txt"
	    # generate text
	    text_str =
	 str(randrange(1000
	00))+","+str(randr
	ange(100000))+", "
	 + str(randrange(1000
	0000)) + "," +
	 str(randrange(1000
	0))
	    # write in s3
	s3.Object(BUCKE
	T_NAME, PREFIX +
	 file_name).put(Bod
	y=text_str)
	5. Escolha Salvar.	

Execute o trabalho do AWS Glue na linha de comando ou no console

Tarefa	Descrição	Habilidades necessárias
Execute o trabalho do AWS Glue na linha de comando.	Para executar seu trabalho do AWS Glue a partir da AWS CLI, execute o seguinte comando usando seus valores: cmd:~$ aws glue start- job-run --job-name create_small_files	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	--arguments '{"--STAR T_RANGE":"0","--EN D_RANGE":"1000000"}' cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--STAR T_RANGE":"1000000" ,"--END_RANGE":"20 00000"}' **Note** Para obter instruções sobre como executar o trabalho do AWS Glue a partir do Console de Gerenciamento da AWS, consulte a história Executar o trabalho do AWS Glue no Console de Gerenciamento da AWS neste padrão. **Tip** Recomendamos usar a AWS CLI para executar trabalhos do AWS Glue se você quiser executar várias execuções ao mesmo tempo com parâmetro s diferentes, conforme	

Tarefa	Descrição	Habilidades necessárias

	mostrado no exemplo acima.
	
	Para gerar todos os comandos da AWS CLI necessários para obter um número definido de arquivos usando um determinado fator de paralelização, execute o seguinte código bash (usando os seus valores):
	
	`# define parameters`
	`NUMBER_OF_FILES=`
	`10000000;`
	`PARALLELIZATION=50;`
	
	`# initialize`
	`_SB=0;`
	
	`# generate commands`
	`for i in $(seq 1`
	` $PARALLELIZATION);`
	`do`
	`  echo aws glue`
	` start-job-run --`
	`job-name create_sm`
	`all_files --argumen`
	`ts "'"'{"--START_RANG`
	`E":"'$(((NUMBER_OF`
	`_FILES/PARALLELIZA`
	`TION) * (i-1) +`
	` _SB))'","--END_RAN`
	`GE":"'$(((NUMBER_O`
	`F_FILES/PARALLELIZ`
	`ATION) * (i)))'"}'"'";`
	`  _SB=1;`
	`done`	

Tarefa	Descrição	Habilidades necessárias
	Se você usar o script acima, considere o seguinte: • O script simplifica a invocação e a geração de arquivos pequenos em grande escala. • Atualize `NUMBER_OF_FILES` e `PARALLELIZATION` com os seus valores. • O script acima imprime uma lista dos comandos que você deve executar. Copie esses comandos de saída e execute-os em seu terminal. • Se você quiser executar os comandos diretamente de dentro do script, remova a instrução `echo` na linha 11. **Note** Para ver um exemplo da saída do script acima, consulte Saída do script Shell na seção Informaçõ es adicionais desse padrão.	

Tarefa	Descrição	Habilidades necessárias
Execute o trabalho do AWS Glue no Console de Gerenciamento da AWS.	1. Faça login no Console de Gerenciamento da AWS e abra o Console do AWS Glue. 2. No painel de navegação, em Integração de dados e ETL, escolha Trabalhos. 3. Na seção Seus trabalhos, selecione o seu trabalho. 4. Na seção Parâmetros (opcional), atualize os seus parâmetros. 5. Escolha Ação e selecione Executar trabalho. 6. Repita as etapas de 3 a 5 quantas vezes precisar. Por exemplo, para criar 10 milhões de arquivos, repita esse processo 10 vezes.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Verificar o status do trabalho do AWS Glue.	1. Abra o Console do AWS Glue. 2. No painel de navegação, escolha Trabalhos. 3. Na seção Seus trabalhos , escolha o trabalho que você criou anteriormente (ou seja, `create_sm all_files`). 4. Para obter informações sobre o progresso e a geração de seus arquivos, revise as colunas ID da execução, Status da execução e outras.	Desenvolvedor de aplicativos

Recursos relacionados

Referências

- Registry of Open Data on AWS
- Conjuntos de dados para análise
- Dados abertos na AWS
- Adicionar trabalhos no AWS Glue
- Conceitos básicos do AWS Glue

Guias e padrões

- Práticas recomendadas do AWS Glue
- Aplicativos de teste de carga

Mais informações

Teste de benchmarking

Esse padrão foi usado para gerar 10 milhões de arquivos usando diferentes parâmetros de paralelização como parte de um teste de benchmarking. A seguinte tabela mostra a saída do teste:

Paralelização	Número de arquivos gerados pela execução de um trabalho	Duração do trabalho	Velocidade
10	1.000.000	6 horas e 40 minutos	Muito lento
50	200.000	80 minutos	Moderada
100	100.000	40 minutos	Fast

Se quiser tornar o processo mais rápido, você pode configurar mais execuções simultâneas na configuração do seu trabalho. Você pode ajustar facilmente a configuração do trabalho com base nos seus requisitos, mas lembre-se de que há um limite de Service Quotas do AWS Glue. Para obter mais informações, consulte Endpoints e cotas do AWS Glue.

Saída de script de shell

O exemplo a seguir mostra a saída do script de shell do histórico de Execução do trabalho do AWS Glue a partir da linha de comando nesse padrão.

```
user@MUC-1234567890 MINGW64 ~
  $ # define parameters
  NUMBER_OF_FILES=10000000;
  PARALLELIZATION=50;
  # initialize
  _SB=0;

  # generate commands
  for i in $(seq 1 $PARALLELIZATION);
   do
```

```
        echo aws glue start-job-run --job-name create_small_files --arguments
 "'"'{"--START_RANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i-1) + SB))'","--
ENDRANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i)))'"}'"'";
        _SB=1;
   done

  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"0","--END_RANGE":"200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"200001","--END_RANGE":"400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"400001","--END_RANGE":"600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"600001","--END_RANGE":"800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"800001","--END_RANGE":"1000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1000001","--END_RANGE":"1200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1200001","--END_RANGE":"1400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1400001","--END_RANGE":"1600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1600001","--END_RANGE":"1800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1800001","--END_RANGE":"2000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2000001","--END_RANGE":"2200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2200001","--END_RANGE":"2400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2400001","--END_RANGE":"2600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2600001","--END_RANGE":"2800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2800001","--END_RANGE":"3000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3000001","--END_RANGE":"3200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3200001","--END_RANGE":"3400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3400001","--END_RANGE":"3600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3600001","--END_RANGE":"3800000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3800001","--END_RANGE":"4000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4000001","--END_RANGE":"4200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4200001","--END_RANGE":"4400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4400001","--END_RANGE":"4600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4600001","--END_RANGE":"4800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4800001","--END_RANGE":"5000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5000001","--END_RANGE":"5200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5200001","--END_RANGE":"5400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5400001","--END_RANGE":"5600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5600001","--END_RANGE":"5800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5800001","--END_RANGE":"6000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6000001","--END_RANGE":"6200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6200001","--END_RANGE":"6400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6400001","--END_RANGE":"6600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6600001","--END_RANGE":"6800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6800001","--END_RANGE":"7000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7000001","--END_RANGE":"7200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7200001","--END_RANGE":"7400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7400001","--END_RANGE":"7600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7600001","--END_RANGE":"7800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7800001","--END_RANGE":"8000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8000001","--END_RANGE":"8200000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8200001","--END_RANGE":"8400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8400001","--END_RANGE":"8600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8600001","--END_RANGE":"8800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8800001","--END_RANGE":"9000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9000001","--END_RANGE":"9200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9200001","--END_RANGE":"9400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9400001","--END_RANGE":"9600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9600001","--END_RANGE":"9800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9800001","--END_RANGE":"10000000"}'

  user@MUC-1234567890 MINGW64 ~
```

PERGUNTAS FREQUENTES

Quantas execuções simultâneas ou trabalhos paralelos devo usar?

O número de execuções simultâneas e trabalhos paralelos depende do tempo necessário e do número desejado de arquivos de teste. Recomendamos que você verifique o tamanho dos arquivos que estão sendo criados. Primeiro, verifique quanto tempo um trabalho do AWS Glue leva para gerar o número desejado de arquivos. Em seguida, use o número certo de execuções simultâneas para atingir suas metas. Por exemplo, se você presumir que 100.000 arquivos levam 40 minutos para concluir a execução, mas seu tempo alvo é 30 minutos, você deve aumentar a configuração de simultaneidade para o seu trabalho do AWS Glue.

Que tipo de conteúdo posso criar usando esse padrão?

Você pode criar qualquer tipo de conteúdo, como arquivos de texto com delimitadores diferentes (por exemplo, PIPE, JSON ou CSV). Esse padrão usa o Boto3 para gravar em um arquivo e depois salva o arquivo em um bucket do S3.

De que nível de permissão do IAM eu preciso no bucket do S3?

É necessário ter uma política baseada em identidade que permita o acesso `Write` a objetos em seu bucket do S3. Para obter mais informações, consulte Amazon S3: permite acesso de leitura e gravação a objetos em um bucket do S3 na documentação do Amazon S3.

Ingerir dados de IoT de forma econômica diretamente no Amazon S3 usando o AWS IoT Greengrass

Criado por Sebastian Viviani (AWS) e Rizwan Syed (AWS)

Resumo

Este padrão mostra como ingerir dados da Internet das Coisas (IoT) de forma econômica diretamente em um bucket do Amazon Simple Storage Service (Amazon S3) usando um dispositivo AWS IoT Greengrass versão 2. O dispositivo executa um componente personalizado que lê os dados da IoT e os salva em armazenamento persistente (ou seja, um disco ou volume local). Em seguida, o dispositivo compacta os dados de IoT em um arquivo Apache Parquet e carrega os dados periodicamente em um bucket do S3.

A quantidade e a velocidade dos dados de IoT que você ingere são limitadas apenas pelos recursos de hardware de borda e pela largura de banda da rede. É possível usar o Amazon Athena para analisar de forma econômica os dados ingeridos. O Athena suporta arquivos compactados do Apache Parquet e visualização de dados usando o Amazon Managed Grafana.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um gateway de borda que é executado no AWS IoT Greengrass versão 2 e coleta dados de sensores (as fontes de dados e o processo de coleta de dados estão além do escopo desse padrão, mas você pode usar praticamente qualquer tipo de dados de sensor. Esse padrão usa um corretor MQTThttps://mqtt.org/ local com sensores ou gateways que publicam dados localmente.)
- Componentes, funções e dependências do SDK do AWS IoT Greengrass
- Um componente do gerenciador de fluxo para carregar os dados no bucket do S3
- AWS SDK para Java, AWS SDK para ou AWS SDK JavaScript para Python (Boto3) SDK for Python (Boto3) para executar o APIs

Limitações

- Os dados nesse padrão não são enviados em tempo real para o bucket do S3. Há um período de atraso e você pode configurar esse período. Os dados são armazenados temporariamente no dispositivo de borda e, em seguida, carregados quando o período expira.
- O SDK está disponível apenas em Java, Node.js e Python.

Arquitetura

Pilha de tecnologias de destino

- Amazon S3
- AWS IoT Greengrass
- Operador MQTT
- Componente gerenciador de fluxo

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura projetada para ingerir dados de sensores de IoT e armazená-los em um bucket do S3.

O diagrama mostra o seguinte fluxo de trabalho:

1. Várias atualizações de sensores (por exemplo, temperatura e válvula) são publicadas em um corretor MQTT local.
2. O compressor de arquivos Parquet que está inscrito nesses sensores atualiza os tópicos e recebe essas atualizações.
3. O compressor de arquivos Parquet armazena as atualizações localmente.
4. Após o término do período, os arquivos armazenados são compactados em arquivos Parquet e transmitidos ao gerenciador de fluxo para serem carregados no bucket do S3 especificado.
5. O gerenciador de fluxo carrega os arquivos Parquet para o bucket do S3.

> **Note**
>
> O gerenciador de fluxo (`StreamManager`) é um componente gerenciado. Para obter exemplos de como exportar dados para o Amazon S3, consulte Gerenciador de fluxo na

documentação do AWS IoT Greengrass. Você pode usar um corretor MQTT local como componente ou outro corretor como o Eclipse Mosquitto.

Ferramentas

Ferramentas da AWS

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS IoT Greengrass é um serviço de nuvem e runtime de borda da IoT de código aberto que ajuda você a criar, implantar e gerenciar aplicativos de IoT em seus dispositivos.

Outras ferramentas

- O Apache Parquet é um formato de arquivos de dados orientados por colunas de código aberto projetado para armazenamento e recuperação.
- O MQTT (Message Queuing Telemetry Transport) é um protocolo de mensagens leve projetado para dispositivos restritos.

Práticas recomendadas

Use o formato de partição correto para dados carregados

Não há requisitos específicos para os nomes do prefixo raiz no bucket do S3 (por exemplo, `"myAwesomeDataSet/"` ou`"dataFromSource"`), mas recomendamos que você use uma partição e um prefixo significativos para facilitar a compreensão da finalidade do conjunto de dados.

Também recomendamos que você use o particionamento correto no Amazon S3 para que as consultas sejam executadas de maneira ideal no conjunto de dados. No exemplo a seguir, os dados são particionados no formato HIVE para que a quantidade de dados digitalizados por cada consulta do Athena seja otimizada. Isso melhora o desempenho e reduz os custos.

```
s3://<ingestionBucket>/<rootPrefix>/year=YY/month=MM/day=DD/
HHMM_<suffix>.parquet
```

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	1. Criar um bucket do S3 ou use um bucket existente. 2. Crie um prefixo significativo para o bucket do S3 em que você deseja ingerir os dados de IoT (por exemplo, `s3:\\<bucket>\<prefix>`). 3. Anote o seu prefixo para uso posterior.	Desenvolvedor de aplicativos
Adicionar permissões do IAM para o bucket do S3.	Para conceder aos usuários acesso de gravação ao bucket e ao prefixo do S3 que você criou anteriormente, adicione a seguinte política do IAM à sua função do AWS IoT Greengrass: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "S3DataUpload", "Effect": "Allow", "Action": [ "s3:List*", "s3:Put*"`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`], "Resource": [ "arn:aws:s3:::<ingestionBucket>", "arn:aws:s3:::<ingestionBucket>/<prefix>/*" ] } ] }` Para obter mais informações, consulte Criar uma política do IAM para acessar recursos do Amazon S3 na documentação do Aurora. Em seguida, atualize a política de recursos (se necessário) do bucket do S3 para permitir o acesso de gravação com as entidades principais corretas da AWS.	

Criar e implantar o componente AWS IoT Greengrass

Tarefa	Descrição	Habilidades necessárias
Atualizar os componentes da fórmula.	Atualize a configuração do componente ao criar uma implantação com base no exemplo a seguir:	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	  "region": "<region>",
	  "parquet_period":
	 <period>,
	  "s3_bucket":
	 "<s3Bucket>",
	  "s3_key_prefix":
	 "<s3prefix>"
	}</pre>
	Substitua `<region>` por sua região da AWS, `<period>` por seu intervalo periódico, `<s3Bucket>` por seu bucket do S3 e `<s3prefix>` por seu prefixo.	

Tarefa	Descrição	Habilidades necessárias
Criar o componente.	Execute um destes procedimentos: • Criar o componente. • Adicione o componente ao pipeline de CI/CD (se houver). Certifique-se de copiar o artefato do repositório de artefatos para o bucket de artefatos do AWS IoT Greengrass. Em seguida, crie ou atualize seu componente do AWS IoT Greengrass. • **Note** Adicione o corretor MQTT como um componente e ou adicione-o manualmente posteriormente. : essa decisão afeta o esquema de autenticação que você pode usar com o broker. A adição manual de um corretor separa o corretor do AWS IoT Greengrass e habilita qualquer esquema de autenticação	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	compatível do corretor. Os componentes do corretor fornecidos pela AWS têm esquemas de autenticação predefinidos. Para obter mais informações, consulte Corretor MQTT 3.1.1 (Moquette) e Corretor MQTT 5 (EMQX).	
Atualize o cliente MQTT.	O código de amostra não usa autenticação porque o componente se conecta localmente ao corretor. Se seu cenário for diferente, atualize a seção do cliente MQTT conforme necessário. Além disso, faça o seguinte: 1. Atualize os tópicos do MQTT na assinatura. 2. Atualize o analisador de mensagens MQTT conforme necessário, pois as mensagens de cada fonte podem ser diferentes.	Desenvolvedor de aplicativos

Adicione o componente ao dispositivo principal do AWS IoT Greengrass versão 2

Tarefa	Descrição	Habilidades necessárias
Atualize a implantação do dispositivo principal.	Se a implantação do dispositivo principal do AWS IoT Greengrass versão 2 já existir, revise a implantação. Se a implantação não existir, crie uma nova implantação. Para dar ao componente o nome correto, atualize a configuração do gerenciador de logs para o novo componente (se necessário) com base no seguinte: `{ "logsUploaderConfiguration": { "systemLogsConfiguration": { ... }, "componentLogsConfigurationMap": { "<com.iot.ingest.parquet>": { "minimumLogLevel": "INFO", "diskSpaceLimit": "20", "diskSpaceLimitUnit": "MB", "deleteLogFileAfterCloudUpload": "false" } ... }`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	<pre> }, "periodicUploadInterval Sec": "300" }</pre> Por fim, conclua a revisão da implantação do seu dispositivo principal do AWS IoT Greengrass.	

Verificar a ingestão de dados no bucket do S3

Tarefa	Descrição	Habilidades necessárias
Verificar os registros do volume do AWS IoT Greengrass.	Verifique o seguinte: • O cliente MQTT foi conectado com sucesso ao corretor MQTT local. • O cliente MQTT está inscrito nos tópicos corretos. • As mensagens de atualização do sensor estão chegando ao corretor sobre os tópicos do MQTT. • A compressão do Parquet ocorre em todos os intervalos periódicos.	Desenvolvedor de aplicativos
Verificar o bucket do S3.	Verifique se os dados estão sendo carregados para o bucket do S3. Você pode ver os arquivos sendo enviados em cada período.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Você também pode verificar se os dados foram carregados no bucket do S3 ao consultar os dados na próxima seção.	

Configurar a consulta do Athena

Tarefa	Descrição	Habilidades necessárias
Criar banco de dados e tabela.	1. Crie um banco de dados AWS Glue (se necessário). 2. Crie uma tabela no AWS Glue manualmente ou executando um crawler no AWS Glue.	Desenvolvedor de aplicativos
Conceda ao Athena o acesso aos dados.	1. Atualize as permissões para permitir que o Athena acesse o bucket do S3. Para obter mais informaçõ es, consulte Acesso refinado a bancos de dados e tabelas no catálogo de dados do AWS Glue na documentação do Athena. 2. Consulte a tabela em seu banco de dados.	Desenvolvedor de aplicativos

Solução de problemas

Problema	Solução
O cliente MQTT não consegue se conectar	• Valide as permissões no corretor MQTT. Se você tiver um corretor MQTT da AWS, consulte o corretor MQTT3.1.1 (Moquette) e o corretor MQTT 5 (EMQX). • Valide as credenciais no cliente MQTT. Se você tiver um corretor MQTT da AWS, consulte o corretor MQTT3.1.1 (Moquette) e o corretor MQTT 5 (EMQX).
O cliente MQTT não consegue se inscrever	Valide as permissões no corretor MQTT. Se você tiver um corretor MQTT da AWS, consulte o corretor MQTT 3.1.1 (Moquette) e o corretor MQTT 5 (EMQX).
Os arquivos Parquet não são criados	• Verifique se os tópicos do MQTT estão corretos. • Verifique se as mensagens de MQTT dos sensores estão no formato correto.
Os objetos não são carregados no bucket do S3	• Verifique se você tem conectividade com a Internet e com o endpoint. • Verifique se a política de recursos do seu bucket do S3 está correta. • Verifique as permissões para a função de dispositivo principal do AWS IoT Greengrass versão 2.

Recursos relacionados

- DataFrame(Documentação do Pandas)
- Documentação do Apache Parquet (documentação do Parquet)

- Desenvolva componentes do AWS IoT Greengrass (Guia do desenvolvedor do AWS IoT Greengrass, versão 2)
- Implante componentes do AWS IoT Greengrass em dispositivos (Guia do desenvolvedor do AWS IoT Greengrass, versão 2)
- Interaja com dispositivos de IoT locais (Guia do desenvolvedor do AWS IoT Greengrass, versão 2)
- Corretor MQTT 3.1.1 (Moquette) (Guia do desenvolvedor do AWS IoT Greengrass, versão 2)
- Corretor MQTT 5 (EMQX) (Guia do desenvolvedor do AWS IoT Greengrass, versão 2)

Mais informações

Análise de custos

O cenário de análise de custos a seguir demonstra como a abordagem de ingestão de dados abordada nesse padrão pode impactar os custos de ingestão de dados na Nuvem AWS. Os exemplos de preços nesse cenário são baseados nos preços no momento da publicação. Os preços estão sujeitos a alterações. Além disso, seus custos podem variar dependendo da sua região da AWS, das Service Quotas da AWS e de outros fatores relacionados ao seu ambiente de nuvem.

Conjunto de sinais de entrada

Essa análise usa o seguinte conjunto de sinais de entrada como base para comparar os custos de ingestão de IoT com outras alternativas disponíveis.

Número de sinais	Frequência	Dados por sinal
125	25 Hz	8 bytes

Nesse cenário, o sistema recebe 125 sinais. Cada sinal tem 8 bytes e ocorre a cada 40 milissegundos (25 Hz). Esses sinais podem vir individualmente ou agrupados em um payload comum. Você tem a opção de dividir e empacotar esses sinais com base em suas necessidades. Você também pode determinar a latência. A latência consiste no período de tempo para receber, acumular e ingerir os dados.

Para fins de comparação, a operação de ingestão para esse cenário é baseada na `us-east-1`região da AWS. A comparação de custos se aplica somente aos serviços da AWS. Outros custos, como hardware ou conectividade, não são considerados na análise.

Comparações de custos

A tabela a seguir mostra o custo mensal em dólares americanos (USD) para cada método de ingestão.

Método	Custo mensal
AWS IoT * SiteWise	USD 331,77
AWS IoT SiteWise Edge com pacote de processamento de dados (mantendo todos os dados na borda)	USD 200
Regras do AWS IoT Core e do Amazon S3 para acessar dados brutos	USD 84,54
Compressão de arquivos Parquet na borda e upload para o Amazon S3	USD 0,50

*Os dados devem ser reduzidos para cumprir as Service Quotas. Isso significa que há alguma perda de dados com esse método.

Métodos alternativos

Esta seção mostra os custos equivalentes dos seguintes métodos alternativos:

- AWS IoT SiteWise — Cada sinal deve ser carregado em uma mensagem individual. Portanto, o número total de mensagens por mês é 125 × 25 × 3600 × 24 × 30, ou 8,1 bilhões de mensagens por mês. No entanto, o AWS IoT SiteWise pode lidar com apenas 10 pontos de dados por segundo por propriedade. Supondo que a resolução dos dados seja reduzida para 10 Hz, o número de mensagens por mês é reduzido para 125 × 10 × 3600 × 24 × 30, ou 3,24 bilhões. Se você usar o componente de publicador que agrupa as medidas em grupos de 10 (a USD 1 por milhão de mensagens), obterá um custo mensal de USD 324 por mês. Supondo que cada mensagem tenha 8 bytes (1 Kb/125), são 25,92 Gb de armazenamento de dados. Isso adiciona um custo mensal de USD 7,77 por mês. O custo total do primeiro mês é de USD 331,77 e aumenta em USD 7,77 a cada mês.
- AWS IoT SiteWise Edge com pacote de processamento de dados, incluindo todos os modelos e sinais totalmente processados na borda (ou seja, sem ingestão de nuvem) — Você pode usar

o pacote de processamento de dados como alternativa para reduzir custos e configurar todos os modelos que são calculados na borda. Isso pode funcionar apenas para armazenamento e visualização, mesmo que nenhum cálculo real seja realizado. Nesse caso, é necessário usar um hardware poderoso para o gateway de borda. Há um custo fixo de USD 200 por mês.

- Ingestão direta no AWS IoT Core pelo MQTT e uma regra de IoT para armazenar os dados brutos no Amazon S3: supondo que todos os sinais sejam publicados em uma payload comum, o número total de mensagens publicadas no AWS IoT Core é de 25 × 3600 × 24 × 30, ou 64,8 milhões por mês. Com USD 1 por milhão de mensagens, esse é um custo mensal de USD 64,8 por mês. Com USD 0,15 por milhão de ativações de regras e com uma regra por mensagem, isso adiciona um custo mensal de USD 19,44 por mês. Com um custo de USD 0,023 por Gb de armazenamento no Amazon S3, isso adiciona mais USD 1,50 por mês (aumentando a cada mês para refletir os novos dados). O custo total do primeiro mês é de USD 84,54 e aumenta em USD 1,50 a cada mês.
- Compressão de dados na borda de um arquivo Parquet e upload para o Amazon S3 (método proposto): a taxa de compactação depende do tipo de dados. Com os mesmos dados industriais testados para o MQTT, o total de dados de saída de um mês inteiro é de 1,2 Gb. Isso custa USD 0,03 por mês. As taxas de compressão (usando dados aleatórios) descritas em outros benchmarks são da ordem de 66 por cento (mais próximas do pior cenário). O total de dados é de 21 Gb e custa USD 0,50 por mês.

Gerador de arquivos Parquet

O exemplo de código a seguir mostra a estrutura de um gerador de arquivos Parquet escrito em Python. O exemplo de código serve apenas para fins ilustrativos e não funcionará se for colado em seu ambiente.

```
import queue
import paho.mqtt.client as mqtt
import pandas as pd

#queue for decoupling the MQTT thread
messageQueue = queue.Queue()
client = mqtt.Client()
streammanager = StreamManagerClient()

def feederListener(topic, message):
    payload = {
        "topic" : topic,
        "payload" : message,
    }
```

```
    messageQueue.put_nowait(payload)

def on_connect(client_instance, userdata, flags, rc):
    client.subscribe("#",qos=0)

def on_message(client, userdata, message):
    feederListener(topic=str(message.topic),
 message=str(message.payload.decode("utf-8")))


filename = "tempfile.parquet"
streamname = "mystream"
destination_bucket= "amzn-s3-demo-bucket"
keyname="mykey"
period= 60

client.on_connect = on_connect
client.on_message = on_message
streammanager.create_message_stream(
            MessageStreamDefinition(name=streamname,
 strategy_on_full=StrategyOnFull.OverwriteOldestData)
        )


while True:
   try:
       message = messageQueue.get(timeout=myArgs.mqtt_timeout)
   except (queue.Empty):
       logger.warning("MQTT message reception timed out")

   currentTimestamp = getCurrentTime()
   if currentTimestamp >= nextUploadTimestamp:
       df = pd.DataFrame.from_dict(accumulator)
       df.to_parquet(filename)
       s3_export_task_definition = S3ExportTaskDefinition(input_url=filename,
 bucket=destination_bucket, key=key_name)
       streammanager.append_message(streamname,
 Util.validate_and_serialize_to_json_bytes(s3_export_task_definition))
       accumulator = {}
       nextUploadTimestamp += period
   else:
        accumulator.append(message)
```

Executar uma tarefa do Spark em um cluster EMR transitório usando uma função do Lambda

Criado por Dhrubajyoti Mukherjee (AWS)

Resumo

Esse padrão usa a ação da RunJobFlow API do Amazon EMR para iniciar um cluster transitório para executar um trabalho do Spark a partir de uma função Lambda. Um cluster EMR transitório foi projetado para encerrar assim que a tarefa for concluída ou se ocorrer algum erro. Um cluster transitório proporciona economia de custos porque é executado somente durante o tempo de computação e fornece escalabilidade e flexibilidade em um ambiente de nuvem.

O cluster EMR transitório é executado usando a API Boto3 e a linguagem de programação Python em uma função do Lambda. A função do Lambda, escrita em Python, oferece a flexibilidade adicional de executar o cluster quando necessário.

Para demonstrar um exemplo de computação em lote e resultado, esse padrão executará uma tarefa do Spark em um cluster EMR a partir de uma função do Lambda e realizará um cálculo em lote com base em exemplos de dados de vendas de uma empresa fictícia. O resultado da tarefa do Spark será um arquivo com valores separados por vírgula (CSV) no Amazon Simple Storage Service (Amazon S3). O arquivo de dados de entrada, o arquivo.jar do Spark, um trecho de código e um CloudFormation modelo da AWS para uma nuvem privada virtual (VPC) e as funções do AWS Identity and Access Management (IAM) para executar a computação são fornecidos como anexo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa

Limitações

- Somente uma tarefa do Spark por vez pode ser executada a partir do código.

Versões do produto

- Testado no Amazon EMR 6.0.0

Arquitetura

Pilha de tecnologias de destino

- Amazon EMR
- AWS Lambda
- Amazon S3
- Apache Spark

Arquitetura de destino

Automação e escala

Para automatizar a computação em lote do Spark-EMR, é possível usar uma das opções a seguir.

- Implemente uma EventBridge regra da Amazon que possa iniciar a função Lambda em um cronograma cron. Para obter mais informações, consulte Tutorial: Programar funções do AWS Lambda usando o. EventBridge
- Configure notificações de eventos do Amazon S3 para executar a função do Lambda na chegada do arquivo.
- Transmita os parâmetros de entrada para a função do AWS Lambda por meio do corpo do evento e das variáveis de ambiente do Lambda.

Ferramentas

Serviços da AWS

- O Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de big data no AWS para processar e analisar grandes volumes de dados.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- O Apache Spark é um mecanismo de análise de várias linguagens para processamento de dados em grande escala.

Épicos

Criar os perfis do IAM do Amazon EMR e do Lambda, além da VPC

Tarefa	Descrição	Habilidades necessárias
Criar os perfis do IAM e a VPC.	Se você já tiver os perfis do IAM do AWS Lambda e do Amazon EMR, além de uma VPC, poderá ignorar essa etapa. Para executar o código, tanto o cluster EMR quanto a função do Lambda exigem perfis do IAM. O cluster EMR também exige uma VPC com uma sub-rede pública ou uma sub-rede privada com um gateway NAT. Para criar automatic amente todas as funções do IAM e uma VPC, implante o CloudFormation modelo da AWS anexado como está, ou você pode criar as funções e a VPC manualmen te, conforme especificado na seção Informações adicionais.	Arquiteto de nuvem
Observe as chaves CloudFormation de saída do modelo AWS.	Depois que o CloudFormation modelo for implantado com sucesso, navegue até a guia Saídas no console da AWS	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	CloudFormation . Anote as cinco chaves resultantes: • `S3Bucket` • `LambdaExecutionRole` • `ServiceRole` • `JobFlowRole` • `Ec2SubnetId` Você usará os valores dessas chaves ao criar a função do Lambda.	

Fazer upload do arquivo .jar do Spark

Tarefa	Descrição	Habilidades necessárias
Fazer upload do arquivo .jar do Spark.	Faça upload do arquivo Spark .jar no bucket do S3 que a pilha da AWS CloudFormation criou. O nome do bucket é o mesmo que a chave resultante `S3Bucket`.	AWS geral

Criar a função do Lambda para executar o cluster EMR

Tarefa	Descrição	Habilidades necessárias
Crie uma função do Lambda.	No console do Lambda, crie uma função do Lambda do Python 3.9+ com uma função de execução. A política da função de execução	Engenheiro de dados, engenheiro de nuvem

Tarefa	Descrição	Habilidades necessárias
	deve permitir que o Lambda execute um cluster EMR. (Veja o CloudFormation modelo da AWS em anexo.)	
Copie e cole o código.	Substitua o código no arquivo `lambda_function.py` pelo código da seção Informações adicionais deste padrão.	Engenheiro de dados, engenheiro de nuvem
Altere os parâmetros no código.	Siga os comentários no código para alterar os valores de parâmetro a fim de correspon der à sua conta da AWS.	Engenheiro de dados, engenheiro de nuvem
Execute a função para iniciar o cluster.	Execute a função para iniciar a criação de um cluster EMR transitório com o arquivo .jar do Spark fornecido. Ele executará a tarefa do Spark e será encerrado automatic amente quando a tarefa for concluída.	Engenheiro de dados, engenheiro de nuvem
Verifique o status do cluster EMR.	Depois que o cluster EMR é iniciado, ele aparece no console do Amazon EMR, na guia Clusters. Eventuais erros ocorridos ao executar o cluster ou a tarefa podem ser verificados de maneira apropriada.	Engenheiro de dados, engenheiro de nuvem

Configurar e executar a demonstração

Tarefa	Descrição	Habilidades necessárias
Fazer upload do arquivo .jar do Spark.	Baixe o arquivo .jar do Spark da seção Anexos e faça o upload para o bucket do S3.	Engenheiro de dados, engenheiro de nuvem
Faça upload do conjunto de dados de entrada.	Faça upload do arquivo `fake_sales_data.csv` no bucket do S3.	Engenheiro de dados, engenheiro de nuvem
Cole o código do Lambda e altere os parâmetros.	Copie o código da seção Ferramentas e cole-o em uma função do Lambda, substituindo o arquivo `lambda_function.py` do código. Altere os valores de parâmetro para corresponder à sua conta.	Engenheiro de dados, engenheiro de nuvem
Execute a função e verifique o resultado.	Depois que a função do Lambda executa o cluster com a tarefa fornecida do Spark, ela gera um arquivo .csv no bucket do S3.	Engenheiro de dados, engenheiro de nuvem

Recursos relacionados

- Desenvolvimento do Spark
- Apache Spark e Amazon EMR
- Documentação run_job_flow do Boto3 Docs
- Informações e documentação do Apache Spark

Mais informações

Código

```
"""
Copy paste the following code in your Lambda function. Make sure to change the
 following key parameters for the API as per your account

-Name (Name of Spark cluster)
-LogUri (S3 bucket to store EMR logs)
-Ec2SubnetId (The subnet to launch the cluster into)
-JobFlowRole (Service role for EC2)
-ServiceRole (Service role for Amazon EMR)

The following parameters are additional parameters for the Spark job itself. Change the
 bucket name and prefix for the Spark job (located at the bottom).

-s3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar (Spark jar file)
-s3://your-bucket-name/prefix/fake_sales_data.csv (Input data file in S3)
-s3://your-bucket-name/prefix/outputs/report_1/ (Output location in S3)
"""
import boto3

client = boto3.client('emr')


def lambda_handler(event, context):
    response = client.run_job_flow(
        Name='spark_job_cluster',
        LogUri='s3://your-bucket-name/prefix/logs',
        ReleaseLabel='emr-6.0.0',
        Instances={
            'MasterInstanceType': 'm5.xlarge',
            'SlaveInstanceType': 'm5.large',
            'InstanceCount': 1,
            'KeepJobFlowAliveWhenNoSteps': False,
            'TerminationProtected': False,
            'Ec2SubnetId': 'subnet-XXXXXXXXXXXXXX'
        },
        Applications=[{'Name': 'Spark'}],
        Configurations=[
            {'Classification': 'spark-hive-site',
             'Properties': {
```

```
                'hive.metastore.client.factory.class':
'com.amazonaws.glue.catalog.metastore.AWSGlueDataCatalogHiveClientFactory'}
            }
        ],
        VisibleToAllUsers=True,
        JobFlowRole='EMRLambda-EMREC2InstanceProfile-XXXXXXXXX',
        ServiceRole='EMRLambda-EMRRole-XXXXXXXXX',
        Steps=[
            {
                'Name': 'flow-log-analysis',
                'ActionOnFailure': 'TERMINATE_CLUSTER',
                'HadoopJarStep': {
                    'Jar': 'command-runner.jar',
                    'Args': [
                        'spark-submit',
                        '--deploy-mode', 'cluster',
                        '--executor-memory', '6G',
                        '--num-executors', '1',
                        '--executor-cores', '2',
                        '--class', 'com.aws.emr.ProfitCalc',
                        's3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar',
                        's3://your-bucket-name/prefix/fake_sales_data.csv',
                        's3://your-bucket-name/prefix/outputs/report_1/'
                    ]
                }
            }
        ]
    )
```

Criação de perfis do IAM e de VPC

Para executar o cluster EMR em uma função do Lambda, exige-se VPC e perfis do IAM. Você pode configurar as funções de VPC e IAM usando o CloudFormation modelo da AWS na seção Anexos desse padrão ou pode criá-las manualmente usando os links a seguir.

Os perfis do IAM a seguir são necessários para executar o Lambda e o Amazon EMR.

Função de execução do Lambda

A função de execução de uma função do Lambda concede a ela permissão para acessar recursos e serviços da AWS.

Perfis de serviço para o Amazon EMR

A função do Amazon EMR define as ações permitidas para o Amazon EMR ao provisionar recursos e realizar tarefas de nível de serviço que não são executadas no contexto de uma instância do Amazon Elastic Compute Cloud (Amazon) executada em um cluster. EC2 Por exemplo, a função de serviço é usada para provisionar EC2 instâncias quando um cluster é iniciado.

Função de serviço para EC2 instâncias

A função de serviço para EC2 instâncias de cluster (também chamada de perfil de EC2 instância para Amazon EMR) é um tipo especial de função de serviço que é atribuída a cada EC2 instância em um cluster do Amazon EMR quando a instância é executada. Os processos de aplicativos que são executados no Apache Hadoop assumem essa função para que as permissões interajam com outros serviços da AWS.

Criação de VPC e sub-rede

Você pode criar um VPC a partir do console VPC.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre cargas de trabalho do Apache Cassandra para o Amazon Keyspaces usando o AWS Glue

Criado por Nikolai Kolesnikov (AWS), Karthiga Priya Chandran (AWS) e Samir Patel (AWS)

Resumo

Esse padrão mostra como migrar suas cargas de trabalho existentes do Apache Cassandra para o Amazon Keyspaces (para Apache Cassandra) usando o AWS Glue. CQLReplicator Você pode usar o CQLReplicator AWS Glue para minimizar o atraso de replicação da migração de suas cargas de trabalho em questão de minutos. Você também aprende a usar um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar dados necessários para a migração, incluindo arquivos, arquivos de configuração e scripts do Apache Parquet. Esse padrão pressupõe que suas cargas de trabalho do Cassandra estejam hospedadas em instâncias do Amazon Elastic Compute Cloud (EC2Amazon) em uma nuvem privada virtual (VPC).

Pré-requisitos e limitações

Pré-requisitos

- Cluster Cassandra com uma tabela de origem
- Tabela de destino no Amazon Keyspaces para replicar a workload
- Bucket do S3 para armazenar arquivos intermediários do Parquet que contêm alterações incrementais de dados
- Bucket do S3 para armazenar scripts e arquivos de configuração do trabalho

Limitações

- CQLReplicator no AWS Glue, é necessário algum tempo para provisionar unidades de processamento de dados (DPUs) para as cargas de trabalho do Cassandra. O atraso de replicação entre o cluster do Cassandra e o keyspace e a tabela de destino no Amazon Keyspaces provavelmente durará apenas alguns minutos.

Arquitetura

Pilha de tecnologia de origem

- Apache Cassandra
- DataStax Servidor
- ScyllaDB

Pilha de tecnologias de destino

- Amazon Keyspaces

Arquitetura de migração

O diagrama a seguir mostra um exemplo de arquitetura em que um cluster do Cassandra é hospedado em EC2 instâncias e distribuído por três zonas de disponibilidade. Os nós do Cassandra encontram-se hospedados em sub-redes privadas.

O diagrama mostra o seguinte fluxo de trabalho:

1. Uma função de serviço personalizada fornece acesso ao Amazon Keyspaces e ao bucket do S3.
2. Um trabalho do AWS Glue lê a configuração e os scripts do trabalho no bucket do S3.
3. O trabalho do AWS Glue se conecta pela porta 9042 para ler dados do cluster Cassandra.
4. O trabalho do AWS Glue se conecta por meio da porta 9142 para gravar dados no Amazon Keyspaces.

Ferramentas

Ferramentas e serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- CloudShellA AWS é um shell baseado em navegador que você pode usar para gerenciar serviços da AWS usando a AWS Command Line Interface (AWS CLI) e uma variedade de ferramentas de desenvolvimento pré-instaladas.
- O AWS Glue é um serviço de ETL totalmente gerenciado que ajuda você a categorizar, limpar, enriquecer e mover dados de forma confiável entre armazenamentos de dados e fluxos de dados.
- O Amazon Keyspaces (para Apache Cassandra) é um serviço de banco de dados gerenciado que ajuda você a migrar, executar e escalar suas workloads do Cassandra na nuvem AWS.

Código

O código desse padrão está disponível no GitHub CQLReplicatorrepositório.

Práticas recomendadas

- Para determinar os recursos necessários do AWS Glue para a migração, estime o número de linhas na tabela de origem do Cassandra. Por exemplo, 250 K linhas por 0,25 DPU (2 vCPUs, 4 GB de memória) com disco de 84 GB.
- Pré-aqueça as tabelas do Amazon Keyspaces antes de executá-las. CQLReplicator Por exemplo, oito CQLReplicator blocos (trabalhos do AWS Glue) podem gravar até 22 K WCUs por segundo, portanto, o alvo deve ser pré-aquecido até 25 a 30 K WCUs por segundo.
- Para permitir a comunicação entre os componentes do AWS Glue, use uma regra de entrada de autorreferência para todas as portas TCP do seu grupo de segurança.
- Use a estratégia de tráfego incremental para distribuir a carga de trabalho de migração ao longo do tempo.

Épicos

Implantar CQLReplicator

Tarefa	Descrição	Habilidades necessárias
Crie um espaço de teclas e uma tabela de destino.	1. Crie um keyspace e uma tabela no Amazon Keyspaces. Para obter mais informaçõ es sobre a capacidade de gravação, consulte Cálculos de unidades de gravação na seção Informações adicionais desse padrão. Você também pode criar um keyspace usando a Cassandra Query	Proprietário do aplicativo, administrador da AWS, DBA, desenvolvedor do aplicativo

Tarefa	Descrição	Habilidades necessárias
	Language (CQL). Para obter mais informações, consulte Criar um keyspace usando CQL na seção Informações adicionais desse padrão. **Note** Depois de criar a tabela, considere mudar a tabela para o modo de capacidade sob demanda para evitar cobranças desnecessárias. 2. Para atualizar para o modo de throughput execute o script a seguir: `ALTER TABLE target_keyspace.target_table WITH CUSTOM_PROPERTIES = { 'capacity_mode': { 'throughput_mode': 'PAY_PER_REQUEST'} }`	

Tarefa	Descrição	Habilidades necessárias
Configure o driver do Cassandra para conectar-se ao Cassandra.	Use o seguinte script de configuração: `Datastax-java-driver { basic.request.consistency = “LOCAL_QUORUM” basic.contact-points = [“127.0.0.1:9042”] advanced.reconnect-on-init = true basic.load-balancing-policy { local-datacenter = “datacenter1” } advanced.auth-provider = { class = PlainTextAuthProvider username = “user-at-sample” password = “S@MPLE=PASSWORD=” } }` **Note** O script anterior usa o conector Spark Cassandra. Para obter mais informações, consulte a configuração de referência do Cassandra.	DBA

Tarefa	Descrição	Habilidades necessárias
Configure o driver do Cassandra para se conectar ao Amazon Keyspaces.	Use o seguinte script de configuração: `datastax-java-driver { basic { load-balancing-pol icy { local-datacenter = us-west-2 } contact-points = ["cassandr a.us-west-2.amazon aws.com:9142"] request { page-size = 2500 timeout = 360 seconds consistency = LOCAL_QUORUM } } advanced { control-connection { timeout = 360 seconds } session-leak.thres hold = 6 connection { connect-timeout = 360 seconds init-query-timeout = 360 seconds warn-on-init-error = false } auth-provider = { class = software. aws.mcs.auth.SigV4 AuthProvider`	DBA

Tarefa	Descrição	Habilidades necessárias

	<pre> aws-region = us-
	west-2
	 }
	
	 ssl-engine-factory {
	  class = DefaultSs
	lEngineFactory
	  }
	  }
	}</pre>
	Note
	O script anterior usa o conector Spark Cassandra. Para obter mais informações, consulte a configuração de referência do Cassandra.	

Tarefa	Descrição	Habilidades necessárias
Crie um perfil do IAM para o trabalho do AWS Glue.	Crie uma nova função de serviço da AWS nomeada `glue-cassandra-migration` com o AWS Glue como uma entidade confiável. **Note** Eles `glue-cassandra-migration` devem fornecer acesso de leitura e gravação ao bucket do S3 e ao Amazon Keyspaces. O bucket do S3 contém os arquivos. jar, os arquivos de configuração do Amazon Keyspaces e do Cassandra e os arquivos intermediários do Parquet. Por exemplo, ele contém `AWSGlueServiceRole` as políticas `AmazonKeyspacesFullAccess` gerenciadas `AmazonS3FullAccess`, e.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Faça o download CQLReplicator na AWS CloudShell.	Baixe o projeto para sua pasta pessoal executando o seguinte comando:
	`git clone https://github.com/aws-samples/cql-replicator .git`
	`cd cql-replicator/glue`
	`# Only for AWS CloudShell, the bc package includes bc and dc. Bc is an arbitrary precision numeric processing arithmetic language`
	`sudo yum install bc -y`	

Modifique os arquivos de configuração de referência.	Copie `Cassandra Connector.conf` e `KeyspacesConnector.conf` para o `../glue/conf` diretório na pasta do projeto.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Inicie o processo de migração.	O comando a seguir inicializa o CQLReplicator ambiente. A inicialização envolve copiar artefatos.jar e criar um conector AWS Glue, um bucket S3, uma tarefa do AWS Glue, o keyspace e a `migration` tabela: `ledger`
	
	`cd cql-replicator/glue/bin`
	`./cqlreplicator --state init --sg '"sg-1","sg-2"' \ --subnet "subnet-XXXXXXXXXXXX" \ --az us-west-2a --region us-west-2 \ --glue-iam-role glue-cassandra-migration \ --landing-zone s3://cql-replicator-1234567890-us-west-2`
	
	O comando inclui os seguintes parâmetros:
	
	• `--sg`— Os grupos de segurança que permitem acesso ao cluster Cassandra a partir do AWS Glue e incluem a regra de entrada de autorreferência para todo o tráfego
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• `--subnet`— A sub-rede à qual o cluster Cassandra pertence • `--az`— A zona de disponibilidade da sub-rede • `--region`— A região da AWS onde o cluster Cassandra está implantado • `--glue-iam-role` — As permissões de função do IAM que o AWS Glue pode assumir ao chamar o Amazon Keyspaces e o Amazon S3 em seu nome • `--landing zone`— Um parâmetro opcional para reutilizar um bucket do S3 (se você não fornecer um valor para o `--landing zone` parâmetro, o `init` processo tentará criar um novo bucket para armazenar os arquivos de configuração, artefatos.jar e arquivos intermediários.)	

Tarefa	Descrição	Habilidades necessárias
Valide a implantação.	Depois de executar o comando anterior, a conta da AWS deve conter o seguinte: • O trabalho do CQLReplicator AWS Glue e o conector do AWS Glue no AWS Glue • O bucket S3 que armazena os artefatos • O keyspace de destino `migration` e a `ledger` tabela no Amazon Keyspaces	AWS DevOps

Corra CQLReplicator

Tarefa	Descrição	Habilidades necessárias
Inicie o processo de migração.	Para operar CQLReplicator no AWS Glue, você precisa usar o `--state run` comando, seguido por uma série de parâmetros. A configuração precisa desses parâmetros é determinada principalmente por seus requisitos exclusivos de migração. Por exemplo, essas configurações podem variar se você optar por replicar valores e atualizações de tempo de vida (TTL) ou se você transferir objetos que excedam 1 MB para o Amazon S3.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Para replicar a carga de trabalho do cluster Cassandra para o Amazon Keyspaces, execute o seguinte comando: `./cqlreplicator --state run --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace \ --src-table source_table \ --trg-keyspace taget_keyspace \ --writetime-column column_name \ --trg-table target_table --inc-traffic` Seu espaço de chave e tabela de origem estão `source_keyspace.source_table` no cluster Cassandra. Seu keyspace e sua tabela de destino estão `target_keyspace.target_table` no Amazon Keyspaces. O parâmetro `--inc-traffic`	

Tarefa	Descrição	Habilidades necessárias
	ajuda a evitar que o tráfego incremental sobrecarregue o cluster Cassandra e o Amazon Keyspaces com um grande número de solicitações. Para replicar atualizaç ões, adicione `--writeti me-column regular_c olumn_name` à sua linha de comando. A coluna normal será usada como fonte do carimbo de data/hora de gravação.	

Monitore o processo de migração

Tarefa	Descrição	Habilidades necessárias
Valide as linhas migradas do Cassandra durante a fase histórica de migração.	Para obter o número de linhas replicadas durante a fase de preenchimento, execute o seguinte comando: `./cqlreplicator --state stats \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --src-keyspace source_keyspace --src-table source_table --region us-west-2`	AWS DevOps

Pare o processo de migração

Tarefa	Descrição	Habilidades necessárias
Use o `cqlreplicator` comando ou o console do AWS Glue.	Para interromper o processo de migração normalmente, execute o seguinte comando: `./cqlreplicator --state request-stop --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace --src-table source_table` Para interromper o processo de migração imediatamente, use o console do AWS Glue.	AWS DevOps

Limpeza

Tarefa	Descrição	Habilidades necessárias
Exclua os recursos implantados.	O comando a seguir excluirá o trabalho, o conector, o bucket do S3 e a tabela `ledger` Keyspaces do AWS Glue: `./cqlreplicator --state cleanup --landing-zone`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`s3://cql-replicator-1234567890-us-west-2`	

Solução de problemas

Problema	Solução
Os trabalhos do AWS Glue falharam e retornaram um erro de falta de memória (OOM).	1. Altere o tipo de trabalhador (aumente a escala). Por exemplo, `G0.25X` mude para `G.1X` ou `G.1X` para`G.2X`. Como alternativa, aumente o número de DPUs por trabalho do AWS Glue (escalabilidade horizontal) em CQLReplicator. 2. Inicie o processo de migração a partir do ponto em que foi interrompido. Para reiniciar CQLReplicator trabalhos com falha, execute novamente o `--state run` comando com os mesmos parâmetros.

Recursos relacionados

- CQLReplicator com o AWS Glue README.MD
- Documentação do AWS Glue
- Documentação do Amazon Keyspaces
- Apache Cassandra

Mais informações

Considerações sobre a migração

Você pode usar o AWS Glue para migrar seu workload do Cassandra para o Amazon Keyspaces, mantendo seus bancos de dados de origem do Cassandra completamente funcionais durante

o processo de migração. Após a conclusão da replicação, você pode optar por transferir seus aplicativos para o Amazon Keyspaces com um atraso mínimo de replicação (menos de minutos) entre o cluster Cassandra e o Amazon Keyspaces. Para manter a consistência de dados, você também pode usar um pipeline similar para replicar os dados de volta para o cluster Cassandra a partir do Amazon Keyspaces.

Grave cálculos unitários

Como exemplo, considere que você pretende escrever 500.000.000 com o tamanho da linha 1 KiB durante uma hora. O número total de unidades de gravação (WCUs) do Amazon Keyspaces que você precisa é baseado neste cálculo:

`(number of rows/60 mins 60s) 1 WCU per row = (500,000,000/(60*60s) * 1 WCU) = 69,444 WCUs required`

69.444 WCUs por segundo é a taxa de 1 hora, mas você pode adicionar um pouco de amortecimento para despesas gerais. Por exemplo, `69,444 * 1.10 = 76,388 WCUs` tem 10% de sobrecarga.

Crie um keyspace usando CQL

Para criar um keyspace usando CQL, execute os seguintes comandos:

```
CREATE KEYSPACE target_keyspace WITH replication = {'class': 'SingleRegionStrategy'}
CREATE TABLE target_keyspace.target_table ( userid uuid, level text, gameid int,
 description text, nickname text, zip text, email text, updatetime text, PRIMARY KEY
 (userid, level, gameid) ) WITH default_time_to_live = 0 AND CUSTOM_PROPERTIES =
 {'capacity_mode':{ 'throughput_mode':'PROVISIONED', 'write_capacity_units':76388,
 'read_capacity_units':3612 }} AND CLUSTERING ORDER BY (level ASC, gameid ASC)
```

Migre dados do Hadoop para o Amazon S3 usando o Migrator WANdisco LiveData

Criado por Tony Velcich

Resumo

Esse padrão descreve o processo de migração de dados do Apache Hadoop de um Sistema de Arquivos Distribuído do Hadoop (HDFS) para o Amazon Simple Storage Service (Amazon S3). Ele usa o WANdisco LiveData Migrator para automatizar o processo de migração de dados.

Pré-requisitos e limitações

Pré-requisitos

- Nó de borda do cluster Hadoop onde o LiveData Migrator será instalado. O nó deve atender aos seguintes requisitos:
  - Especificação mínima: 4 CPUs, 16 GB de RAM, 100 GB de armazenamento.
  - Rede mínima de 2 Gbps.
  - Porta 8081 acessível em seu nó de borda para acessar a WANdisco interface do usuário.
  - Java 1.8 de 64 bits.
  - Bibliotecas de cliente do Hadoop instaladas no nó periférico.
  - Capacidade de se autenticar como superusuário do HDFS (por exemplo, “hdfs”).
  - Se o Kerberos estiver habilitado em seu cluster do Hadoop, um keytab válido que contenha uma entidade principal adequada para o superusuário do HDFS deverá estar disponível no nó de borda.
- Uma conta ativa da AWS com acesso a um bucket do S3.
- Um link do AWS Direct Connect estabelecido entre seu cluster do Hadoop on-premises (especificamente o nó de borda) e a AWS.

Versões do produto

- LiveData Migrador 1.8.6
- WANdisco Interface do usuário (OneUI) 5.8.0

Arquitetura

Pilha de tecnologia de origem

- Cluster Hadoop on-premises

Pilha de tecnologias de destino

- Amazon S3

Arquitetura

O diagrama a seguir mostra a arquitetura da solução LiveData Migrator.

O fluxo de trabalho consiste em quatro componentes principais para a migração de dados do HDFS on-premises para o Amazon S3.

- LiveData Migrador — automatiza a migração de dados do HDFS para o Amazon S3 e reside em um nó periférico do cluster Hadoop.
- HDFS: um sistema de arquivos distribuído que fornece acesso de alto throughput dos dados do aplicativo.
- Amazon S3: um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e performance líderes do setor.
- AWS Direct Connect: um serviço que estabelece uma conexão de rede dedicada entre seus datacenters on-premises e a AWS.

Automação e escala

Normalmente, você cria várias migrações para poder selecionar conteúdo específico do sistema de arquivos de origem por caminho ou diretório. Você também pode migrar dados para vários sistemas de arquivos independentes ao mesmo tempo definindo vários recursos de migração.

Épicos

Configure o armazenamento do Amazon S3 em sua conta da AWS

Tarefa	Descrição	Habilidades necessárias
Faça login na sua conta da AWS.	Faça login no AWS Management Console e abra o console do Amazon S3 em. https://console.aws.amazon.com/s3/	Experiência da AWS
Criar um bucket do S3.	Se você ainda não tiver um bucket do S3 existente para usar como armazenamento de destino, selecione a opção “Criar um bucket” no console do Amazon S3 e especifique o nome do bucket, a região da AWS e as configurações do bucket para bloquear o acesso público. A AWS WANdisco recomenda que você habilite as opções de bloqueio de acesso público para o bucket S3 e configure as políticas de acesso ao bucket e de permissão de usuário para atender aos requisitos da sua organização. Um exemplo da AWS é fornecido em https://docs.aws.amazon.com/AmazonS3/ latest/dev/ example - walkthroughs-managing-access-example 1.html.	Experiência da AWS

Instale o LiveData Migrator

Tarefa	Descrição	Habilidades necessárias
Baixe o LiveData instalador do Migrator.	Faça o download do LiveData instalador do Migrator e carregue-o no nó de borda do Hadoop. Você pode baixar uma versão de avaliação gratuita do LiveData Migrator em https://www2.wandisco.com/ldm-trial. You can also obtain access to LiveData Migrator from AWS Marketplace, at https:/ /aws.amazon. com/marketplace/pp/B07B8SZND9.	Administrador do Hadoop, proprietário do aplicativo
Instale o LiveData Migrator.	Use o instalador baixado e instale o LiveData Migrator como superusuário do HDFS em um nó periférico em seu cluster Hadoop. Consulte a seção “Informações adicionais” para ver os comandos de instalação.	Administrador do Hadoop, proprietário do aplicativo
Verifique o status do LiveData Migrator e de outros serviços.	Verifique o status do LiveData Migrator, do Hive migrator e da WANdisco UI usando os comandos fornecidos na seção “Informações adicionais”.	Administrador do Hadoop, proprietário do aplicativo

Configurar o armazenamento por meio da WANdisco interface

Tarefa	Descrição	Habilidades necessárias
Registre sua conta do LiveData Migrator.	Faça login na WANdisco interface do usuário por meio de um navegador da Web na porta 8081 (no nó de borda do Hadoop) e forneça seus detalhes para registro. Por exemplo, se você estiver executando o LiveData Migrator em um host chamado myldmhost.example.com, a URL seria: http://myldmhost.example.com:8081	Proprietário do aplicativo
Configure seu armazenamento do HDFS de origem.	Forneça os detalhes de configuração necessários para seu armazenamento do HDFS de origem. Isso incluirá o valor “fs.defaultFS” e um nome de armazenamento definido pelo usuário. Se o Kerberos estiver habilitado, forneça o local principal e o keytab para o LiveData Migrator usar. Se o NameNode HA estiver habilitado no cluster, forneça um caminho para os arquivos core-site.xml e hdfs-site.xml no nó de borda.	Administrador do Hadoop, proprietário do aplicativo
Configure seu armazenamento do Amazon S3 de destino.	Adicione seu armazenamento de destino como o tipo S3a. Forneça o nome de armazenamento definido	AWS, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	pelo usuário e o nome do bucket do S3. Insira “org.apache.hadoop.fs.s3a.SimpleAWSCredentials Provider” na opção Credentials Provider e forneça as chaves secretas e de acesso da AWS para o bucket do S3. Propriedades adicionais do S3a também serão necessárias. Para obter detalhes, consulte a seção “Propriedades do S3a” na documentação do LiveData Migrator em docs/command-reference/# 3a https://docs.wandisco.com/live-data-migrator/. filesystem-add-s	

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Adicione exclusões (se necessário).	Se quiser excluir conjuntos de dados específicos da migração, adicione exclusões para o armazenamento de origem do HDFS. Essas exclusões podem ser baseadas no tamanho do arquivo, nos nomes dos arquivos (com base nos padrões regex) e na data de modificação.	Administrador do Hadoop, proprietário do aplicativo

Crie e inicie a migração

Tarefa	Descrição	Habilidades necessárias
Crie e configure a migração.	Crie uma migração no painel da WANdisco interface do usuário. Selecione sua origem (HDFS) e destino (o bucket S3). Adicione as novas exclusões que você definiu na etapa anterior. Selecione a opção “Substitu ir” ou “Ignorar se o tamanho for correspondente”. Crie a migração quando todos os campos estiverem preenchid os.	Administrador do Hadoop, proprietário do aplicativo
Inicie a migração.	No painel, selecione a migração que você criou. Clique para iniciar a migração. Você também pode iniciar uma migração automatic amente escolhendo a opção de início automático ao criar a migração.	Proprietário do aplicativo

Gerencie a largura de banda (opcional)

Tarefa	Descrição	Habilidades necessárias
Defina um limite de largura de banda da rede entre a origem e o destino.	Na lista Armazenamentos no painel, selecione seu armazenamento de origem e selecione “Gerenciamento de largura de banda” na lista	Proprietário do aplicativo, Rede

Tarefa	Descrição	Habilidades necessárias
	de agrupamento. Limpe a opção ilimitada e defina o limite máximo de largura de banda e a unidade. Escolha “Aplicar”.	

Monitore e gerencie migrações

Tarefa	Descrição	Habilidades necessárias
Visualize as informações de migração usando a WANdisco interface do usuário.	Use a WANdisco interface do usuário para visualizar as informações de licença, largura de banda, armazenamento e migração. A interface do usuário também fornece um sistema de notificação para que você possa receber notificações sobre erros, avisos ou marcos importantes em seu uso.	Administrador do Hadoop, proprietário do aplicativo
Suspenda, retome e exclua migrações.	Você pode impedir que uma migração transfira conteúdo para seu destino colocando-a no estado INTERROMPIDO. Migrações suspensas podem ser retomadas. As migrações no estado INTERROMPIDO também podem ser excluídas.	Administrador do Hadoop, proprietário do aplicativo

Recursos relacionados

- LiveData Documentação do migrador

- LiveData Migrador no AWS Marketplace
- WANdisco LiveData Demonstração do Migrator (vídeo)

Mais informações

Instalando o LiveData Migrator

Você pode usar os seguintes comandos para instalar o LiveData Migrator, supondo que o instalador esteja dentro do seu diretório de trabalho:

```
su - hdfs
chmod +x livedata-migrator.sh && sudo ./livedata-migrator.sh
```

Verificando o status do LiveData Migrator e de outros serviços após a instalação

Use os comandos a seguir para verificar o status do LiveData Migrator, do Hive migrator e da UI: WANdisco

```
service livedata-migrator status
service hivemigrator status
service livedata-ui status
```

Migrar o Oracle Business Intelligence 12c para a Nuvem AWS a partir de servidores on-premises

Criado por Lanre (Lan-Ray) showunmi (AWS) e Patrick Huang (AWS)

Resumo

Esse padrão mostra como migrar o Oracle Business Intelligence Enterprise Edition 12c de servidores locais para a Nuvem AWS usando a AWS. CloudFormation Também descreve como você pode usar outros serviços da AWS para implementar componentes do Oracle BI 12c que oferecem alta disponibilidade, segurança, flexibilidade e a capacidade de escalar dinamicamente.

Para obter uma lista das práticas recomendadas relacionadas à migração do Oracle BI 12c para a Nuvem AWS, consulte a seção Informações adicionais desse padrão.

> **Note**
>
> É uma prática recomendada executar várias migrações de teste antes de transferir seus dados existentes do Oracle BI 12c para a nuvem. Esses testes ajudam você a ajustar sua abordagem de migração, identificar e corrigir possíveis problemas e estimar os requisitos de tempo de inatividade com mais precisão.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Conectividade de rede segura entre servidores on-premises e a AWS por meio dos serviços da Rede Privada Virtual da AWS (AWS VPN) ou do AWS Direct Connect
- Licenças de software para seu sistema operacional Oracle, Oracle BI 12c, Oracle Database, Oracle WebLogic Server e Oracle HTTP Server

Limitações

Para obter informações sobre limites de tamanho de armazenamento, consulte a documentação do Amazon Relational Database Service (Amazon RDS) para Oracle.

Versões do produto

- Oracle Business Intelligence Enterprise, edição 12c
- WebLogic Servidor Oracle 12c
- Oracle HTTP Server 12c
- Banco de dados Oracle 12c (ou mais recente)
- Oracle Java SE 8

Arquitetura

O diagrama a seguir mostra um exemplo de arquitetura para executar componentes do Oracle BI 12c na Nuvem AWS:

O diagrama a seguir mostra a arquitetura:

1. O Amazon Route 53 fornece configuração de serviço de nome de domínio (DNS).
2. O Elastic Load Balancing (ELB) distribui o tráfego de rede para melhorar a escalabilidade e a disponibilidade dos componentes do Oracle BI 12c em várias zonas de disponibilidade.
3. Os grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling hospedam os Oracle HTTP Servers, o servidor Weblogic Admin e os servidores de BI gerenciados em várias zonas de disponibilidade.
4. O Amazon Relational Database Service (Amazon RDS) para banco de dados Oracle armazena metadados do BI Server em várias zonas de disponibilidade.
5. O Amazon Elastic File System (Amazon EFS) é montado em cada componente do Oracle BI 12c para armazenamento compartilhado de arquivos.

Pilha de tecnologia

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon RDS para Oracle

- AWS Certificate Manager (ACM)
- Elastic Load Balancing (ELB)
- Oracle BI 12c
- WebLogic Servidor Oracle 12c
- Oracle HTTP Server (OHS)

Ferramentas

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- O AWS Certificate Manager (ACM) ajuda você a criar, armazenar e renovar chaves e certificados X.509 SSL/TLS públicos e privados que protegem seus sites e aplicativos da AWS.
- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon EC2 Auto Scaling ajuda você a manter a disponibilidade do aplicativo e permite que você adicione ou remova automaticamente EC2 instâncias da Amazon de acordo com as condições definidas por você.
- O Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS.
- O Elastic Load Balancing distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

- O Oracle Data Pump ajuda você a mover dados e metadados de um banco de dados para outro em alta velocidade.
- O Oracle Fusion Middleware é um conjunto de ferramentas de desenvolvimento de aplicativos e soluções de integração para gerenciamento de identidade, colaboração e relatórios de business intelligence.
- GoldenGateA Oracle ajuda você a projetar, executar, orquestrar e monitorar suas soluções de replicação de dados e streaming de processamento de dados na Oracle Cloud Infrastructure.
- O Oracle WebLogic Scripting Tool (WLST) fornece uma interface de linha de comando que ajuda você a escalar horizontalmente seus clusters. WebLogic

Épicos

Avaliar o ambiente de origem

Tarefa	Descrição	Habilidades necessárias
Reunir informações de inventário de software.	Identifique versões e níveis de patch para cada um dos componentes de software da sua pilha de tecnologia de origem, incluindo o seguinte: • Sistema operacional do Oracle • Oracle Database • Oracle BI 12c • WebLogic Servidor Oracle • Oracle HTTP Server • Java	Arquiteto de migração, arquiteto de soluções, proprietário do aplicativo, administrador do Oracle BI
Reunir informações de inventário de computação e armazenamento.	Em seu ambiente de origem, analise as métricas de utilização atuais e históricas para o seguinte: • Uso da CPU	Arquiteto de migração, arquiteto de soluções, proprietário do aplicativo, administrador do Oracle BI, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
	• Uso de memória • Uso de armazenamento ⚠ Important Certifique-se de considerar os picos históricos de uso.	
Reunir informações sobre a arquitetura do ambiente de origem e seus requisitos.	Obtenha uma compreensão completa da arquitetura do seu ambiente de origem e de seus requisitos, incluindo o conhecimento do seguinte: • Configuração de domínio WebLogic do Oracle Server • Agrupamento em clusters • Balanceamento de carga • Conectividade • Disponibilidade • Requisitos de recuperação de desastres	Arquiteto de migração, arquiteto de soluções, proprietário do aplicativo, administrador do Oracle BI
Identificar fontes de dados de Java Database Connectivity (JDBC).	Reúna informações sobre as fontes de dados e drivers do JDBC do seu ambiente de origem para cada mecanismo de banco de dados que ele usa.	Arquiteto de migração, proprietário do aplicativo, administrador do Oracle BI, engenheiro ou administrador de banco de dados

Tarefa	Descrição	Habilidades necessárias
Reunir informações sobre configurações específicas do ambiente.	Colete informações sobre definições e configurações específicas do seu ambiente de origem, incluindo o seguinte: • Scripts personalizados de startup e desligamento • Java e outras variáveis de ambiente • Certificados	Arquiteto de migração, arquiteto de soluções, proprietário do aplicativo, administrador do Oracle BI
Identificar quaisquer dependências em outros aplicativos.	Colete informações sobre integrações em seu ambiente de origem que criam dependências com outros aplicativos. **Important** Certifique-se de identificar todas as integrações do Lightweight Directory Access Protocol (LDAP) e outros requisitos de rede.	Arquiteto de migração, arquiteto de soluções, proprietário do aplicativo, administrador do Oracle BI

Projetar seu ambiente de destino

Tarefa	Descrição	Habilidades necessárias
Criar um documento de projeto de alto nível.	Crie um documento de projeto de arquitetura de	Arquiteto de soluções, arquiteto de aplicativos,

Tarefa	Descrição	Habilidades necessárias
	destino. Certifique-se de usar as informações coletadas ao avaliar seu ambiente de origem para compor o documento do projeto.	engenheiro de banco de dados, arquiteto de migração
Obter aprovação para o documento do projeto.	Revise o documento do projeto com as partes interessadas e obtenha as aprovações necessárias.	Proprietário do aplicativo ou serviço, arquiteto de soluções, arquiteto de aplicativos

Implantar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Prepare o código de infraestrutura em CloudFormation.	Crie CloudFormation modelos para provisionar sua infraestrutura Oracle BI 12c na Nuvem AWS. Para obter mais informações, consulte Como trabalhar com CloudFormation modelos da AWS no Guia CloudFormation do usuário da AWS. **Note** É uma prática recomendada criar CloudFormation modelos modulares para cada camada do Oracle BI 12c, em vez de um modelo	Arquiteto de infraestrutura de nuvem, arquiteto de soluções, arquiteto de aplicativos

Tarefa	Descrição	Habilidades necessárias
	grande para todos os seus recursos. Para obter mais informações sobre as CloudFormation melhores práticas, consulte 8 melhores práticas ao automatizar suas implantações com a AWS CloudFormation no blog da AWS.	
Download do software necessário.	DDownload o seguinte software junto com as versões e os patches necessários do site da Oracle: • Java JDK8 • WebLogic Servidor Oracle 12c • Oracle BI 12c	Arquiteto de migração, engenheiro de banco de dados, arquiteto de aplicativos

Tarefa	Descrição	Habilidades necessárias
Preparar os scripts de instalação.	Crie scripts de instalação de software que executem uma instalação silenciosa. Esses scripts simplificam a automação da implantação. Para obter mais informaçõ es, consulte OBIEE 12c: Como realizar uma instalação silenciosa? no site do Oracle Support. Você precisa de uma conta do Oracle Support para ver os documentos.	Arquiteto de migração, engenheiro de banco de dados, arquiteto de aplicativos

Tarefa	Descrição	Habilidades necessárias
Criar uma AMI do Linux baseada no Amazon EBS para seus níveis de web e aplicativos.	1. Implante e configure EC2 instâncias da Amazon para seus níveis de web e aplicativos. Certifique-se de que as instâncias atendam aos pré-requisitos para executar o seguinte: • Configuração do ambiente do sistema operacional do Oracle • Configuração da conta de usuário do sistema operacional Oracle • Instalação de softwares em Java 2. Crie Amazon Machine Images (AMIs) das instâncias e salve cópias para uso futuro. Para obter instruções, consulte Criar uma AMI Linux baseada no Amazon EBS no Guia EC2 do usuário da Amazon para instâncias Linux.	Arquiteto de migração, engenheiro de banco de dados, arquiteto de aplicativos

Tarefa	Descrição	Habilidades necessárias
Inicie sua infraestrutura da AWS usando CloudFormation.	Implante suas camadas web e de aplicativos do Oracle BI 12c em módulos usando os CloudFormation modelos que você criou. Para obter instruções, consulte Conceitos básicos da AWS CloudFormation no Guia CloudFormation do usuário da AWS.	Arquiteto de infraestrutura de nuvem, arquiteto de soluções, arquiteto de aplicativos

Migrar o Oracle BI 12c para a AWS usando uma nova instalação

Tarefa	Descrição	Habilidades necessárias
Preparar o software necessário.	Organize o software necessário em um local acessível às EC2 instâncias da Amazon. Por exemplo, você pode configurar o software no Amazon S3 ou em outra EC2 instância da Amazon que estaria acessível aos seus servidores web e de aplicativos.	Arquiteto de migração, arquiteto do Oracle BI, infraestrutura de nuvem, arquiteto de soluções, arquiteto de aplicativos
Preparar seu banco de dados do repositório para a instalação do Oracle BI 12c.	Crie esquemas do Oracle BI 12c executando o Oracle Repository Creation Utility (RCU) em uma nova instância de banco de dados do Amazon RDS para Oracle.	Arquiteto de infraestrutura de nuvem, arquiteto de soluções, arquiteto de aplicativos, arquiteto de migração, arquiteto do Oracle BI

Tarefa	Descrição	Habilidades necessárias
Instalar o Oracle Fusion Middleware 12c e o Oracle BI 12c.	1. Começando com uma EC2 instância da Amazon, instale a infraestrutura Oracle Fusion Middlewar e 12c e o OBIEE 12c. Para obter mais informaçõ es, consulte as seguintes seções do Guia de Implantação Corporativa do Oracle Fusion Middlewar e para Oracle Business Intelligence: • Iniciando o instalado r de infraestrutura em BIHOST1 • Instalar o Oracle Business Intelligence em preparação para uma implantação corporativa **Note** Use o Amazon EFS para hospedar diretórios que serão compartilhados entre os nós do cluster Oracle BI 12c. 2. Aplique todos os patches necessários à instalação.	Arquiteto de migração, arquiteto do Oracle BI

Tarefa	Descrição	Habilidades necessárias
	3. Crie AMIs as instâncias e salve as cópias para uso futuro.	
Configure seu domínio WebLogic do Oracle Server para o Oracle BI 12c.	Configure seu domínio Oracle BI 12c como uma implantação sem cluster. Para obter mais informaçõ es, consulte Configurar o domínio de BI no Guia de Implantação Corporativa do Oracle Fusion Middleware para Oracle Business Intellige nce.	Arquiteto de migração, arquiteto do Oracle BI
Aumentar a escala horizonta lmente do Oracle BI 12c.	Aumente a escala horizonta lmente de um único nó até o número desejado de nós. Para obter mais informações, consulte Aumentar a escala horizontalmente do Oracle Business Intelligence no Guia de Implantação Corporativa do Oracle Fusion Middleware para Oracle Business Intellige nce.	Arquiteto de migração, arquiteto do Oracle BI

Tarefa	Descrição	Habilidades necessárias
Instalar o Oracle HTTP Server 12c.	1. Instale o Oracle HTTP Server 12c nas EC2 instâncias da Amazon de nível web da Oracle. Para obter instruções, consulte Instalar o Oracle HTTP Server 12c em Instalar e configurar o Oracle HTTP Server para Oracle Access Management 12c. 2. Aplique todos os patches necessários à instalação. 3. Crie AMIs as instâncias e salve as cópias para uso futuro.	Arquiteto de migração, arquiteto do Oracle BI
Configurar balanceadores de carga para terminação SSL.	1. Crie ou importe um certificado no ACM. 2. Associe os certificados SSL ao ELB.	Arquiteto de infraestrutura de nuvem, arquiteto de migração

Tarefa	Descrição	Habilidades necessárias
Migrar artefatos de metadados de inteligência de negócios para a AWS.	1. Exporte arquivos do Oracle Business Intelligence Application Archive (BAR) da instalação on-premises do Oracle BI 12c. Para exportar os arquivos BAR, use a Ferramenta WebLogic de Scripting (WLST) para executar o exportServiceInstancecomando. 2. Importe os arquivos BAR on-premises para a instalação do AWS Oracle BI 12c. Para importar os arquivos BAR, execute o comando importServiceInstanceWLST.	Arquiteto de migração, arquiteto do Oracle BI

Tarefa	Descrição	Habilidades necessárias
Executar tarefas pós-migração.	Depois de importar os arquivos BAR, faça o seguinte: • Configure qualquer fonte de dados JDBC adicional. • Instale drivers para outras fontes de dados, como PostgreSQL ou Amazon Redshift. • Configure Oracle LDAP, SSL, single sign-on (SSO) e armazenamento de segurança. WebLogic • Configuração de políticas do AWS Identity and Access Management (IAM). • Ative o rastreamento de uso. • Configure integrações com outros sistemas. • Migre qualquer script personalizado.	Arquiteto de migração, arquiteto do Oracle BI

Testar o novo ambiente

Tarefa	Descrição	Habilidades necessárias
Testar o novo ambiente Oracle BI 12c.	Realize end-to-end testes no novo ambiente Oracle BI 12c. Use a automação o máximo possível.	Arquiteto de migração, arquiteto de soluções, proprietário do aplicativo, administrador do Oracle BI

Tarefa	Descrição	Habilidades necessárias
	Exemplos de atividades de teste incluem: • Validando painéis, relatórios e URLs • Teste de aceitação do usuário (UAT) • Teste de aceitação operacional (OAT) **Note** Realize testes e validações adicionais conforme necessário.	

Transferir para o novo ambiente

Tarefa	Descrição	Habilidades necessárias
Desconectar o tráfego do ambiente Oracle BI 12c on-premises.	Na janela de substituição indicada, interrompa todo o tráfego para o ambiente on-premises do Oracle BI 12c.	Arquiteto de migração, arquiteto de soluções, proprietário do aplicativo, administrador do Oracle BI
Ressincronizar o novo banco de dados do repositório Oracle BI 12c com o banco de dados de origem.	Ressincronize o banco de dados do repositório Amazon RDS Oracle BI 12c com o banco de dados on-premises. Para sincronizar os bancos de dados, você pode usar uma atualização do Oracle Data Pump ou uma captura de	Administrador do Oracle BI, engenheiro/administrador de banco de dados

Tarefa	Descrição	Habilidades necessárias
	dados de alteração (CDC) do AWS DMS.	
Mude seu Oracle BI 12c URLs para apontar para o novo ambiente da AWS.	Atualize o Oracle BI 12c URLs em seus servidores DNS internos para que eles apontem para a nova instalaçã o da AWS.	Arquiteto de migração, arquiteto de soluções, proprietário do aplicativo, administrador do Oracle BI
Monitorar o novo ambiente.	Monitore o novo ambiente Oracle BI 12c usando qualquer uma das seguintes ferramentas: • Amazon CloudWatch • Insights de Performance do Amazon RDS • Oracle Enterprise Manager	Administrador do Oracle BI, engenheiro/administrador de banco de dados, Administr ador do Aplicativo
Obter a aprovação do projeto.	Analise os resultados dos testes com as partes interessa das e obtenha as aprovaçõe s necessárias para concluir a migração.	Proprietário do aplicativ o, proprietário do serviço, arquiteto de infraestrutura de nuvem, arquiteto de migração, arquiteto do Oracle BI

Recursos relacionados

- Usar o Oracle Repository Creation Utility no Amazon RDS para Oracle (Guia do usuário do Amazon RDS)
- Oracle no Amazon RDS (Guia do usuário do Amazon RDS)
- Oracle WebLogic Server 12c na AWS (whitepaper da AWS)
- Implantar o Oracle Business Intelligence para alta disponibilidade (Oracle Help Center)
- Oracle Business Intelligence Application Archive (BAR) (central de ajuda da Oracle)
- Como migrar o OBI 12c entre ambientes (suporte do Oracle)

Mais informações

A seguir está uma lista das práticas recomendadas relacionadas à migração do Oracle BI 12c para a Nuvem AWS.

Bancos de dados do repositório

É uma prática recomendada hospedar esquemas de banco de dados Oracle BI 12c em uma instância do Amazon RDS para Oracle. Esse tipo de instância fornece capacidade econômica e redimensionável enquanto automatiza tarefas administrativas, como provisionamento de hardware, configuração de banco de dados, aplicativo de patches e backups.

Para obter mais informações, consulte Usar o Oracle Repository Creation Utility no Amazon RDS para Oracle no Guia do usuário do Amazon RDS.

Níveis da Web e do aplicativo

EC2 As instâncias Amazon otimizadas para memória geralmente são adequadas para servidores Oracle BI 12c. Seja qual for o tipo de instância escolhido, certifique-se de que as instâncias que você provisiona atendam aos requisitos de uso de memória do seu sistema. Além disso, certifique-se de configurar um tamanho de pilha de WebLogic Java Virtual Machine (JVM) suficiente com base na memória disponível da sua EC2 instância Amazon.

Armazenamento local

A E/S desempenha um papel importante no desempenho geral do seu aplicativo Oracle BI 12c. O Amazon Elastic Block Store (Amazon EBS) oferece classes de armazenamento diferentes que são otimizadas para padrões de workload diferentes. Certifique-se de escolher um tipo de volume do Amazon EBS adequado ao seu caso de uso.

Para obter mais informações sobre tipos de volumes de EBS, consulte Atributos do Amazon EBS na documentação do Amazon EBS.

Armazenamento compartilhado

Um domínio em cluster do Oracle BI 12c requer armazenamento compartilhado para os seguintes recursos:

- Arquivos de configuração
- Diretório de dados singleton (SDD) Oracle BI 12c

- Cache global da Oracle
- Scripts do Oracle BI Scheduler
- Binários WebLogic do Oracle Server

Você pode atender a esse requisito de armazenamento compartilhado usando o Amazon EFS, que fornece um sistema de arquivos elástico de rede (NFS) escalável e totalmente gerenciado.

Ajuste fino do desempenho do armazenamento compartilhado

O Amazon EFS tem dois modos de throughput: provisionado e intermitente. O serviço também tem dois modos de desempenho: Uso geral e E/S máxima.

Para ajustar o desempenho, comece testando suas workloads no modo de desempenho de objetivo geral e no modo de throughput provisionada. A realização desses testes ajudará você a determinar se esses modos de linha de base são suficientes para atender aos níveis de serviço desejados.

Para obter mais informações, consulte o Desempenho do Amazon EFS no Guia do usuário do Amazon EFS.

Alta disponibilidade e recuperação de desastres

É uma prática recomendada implantar componentes do Oracle BI 12c em várias zonas de disponibilidade para proteger esses recursos no caso de uma falha na zona de disponibilidade. A seguir está uma lista das práticas recomendadas de disponibilidade e recuperação de desastres para recursos específicos do Oracle BI 12c hospedados na Nuvem AWS:

- Bancos de dados do repositório Oracle BI 12c: implante uma instância de banco de dados Amazon RDS multi-AZ em seu banco de dados do repositório Oracle BI 12c. Em uma implantação multi-AZ, o Amazon RDS automaticamente provisiona e mantém uma réplica em espera síncrona em outra AZ. Executar uma instância de banco de dados do repositório do Oracle BI 12c em zonas de disponibilidade (AZ) pode aumentar a disponibilidade durante a manutenção planejada do sistema e ajudar a proteger seus bancos de dados contra falhas na instância e na zona de disponibilidade.
- Servidores gerenciados Oracle BI 12c: Para obter tolerância a falhas, é uma prática recomendada implantar componentes do sistema Oracle BI 12c em servidores gerenciados em um grupo Amazon Auto EC2 Scaling configurado para abranger várias zonas de disponibilidade. O Auto Scaling substitui instâncias defeituosas com base nas verificações de saúde da Amazon. EC2 No caso de uma falha em uma zona de disponibilidade, os Servidores HTTP Oracle continuam direcionando o tráfego para os servidores gerenciados na zona de disponibilidade em

funcionamento. Em seguida, o ajuste de escala automático inicia instâncias para atender aos requisitos de contagem de hosts. É recomendável habilitar a replicação do estado da sessão HTTP para ajudar a garantir que haja um failover tranquilo das sessões existentes para os servidores gerenciados em funcionamento.

- Servidores de Administração Oracle BI 12c: Para garantir que seu Servidor de Administração tenha alta disponibilidade, hospede-o em um grupo do Amazon EC2 Auto Scaling configurado para abranger várias zonas de disponibilidade. Em seguida, defina o tamanho mínimo e máximo do grupo definido como 1. Se ocorrer uma falha na zona de disponibilidade, o Amazon EC2 Auto Scaling iniciará um servidor de administração substituto em uma zona de disponibilidade alternativa. Para recuperar qualquer host subjacente com falha na mesma zona de disponibilidade, você pode ativar o Amazon EC2 Auto Recovery.
- Servidores Oracle Web Tier: É uma prática recomendada associar seu Oracle HTTP Server ao seu domínio Oracle WebLogic Server. Para obter alta disponibilidade, implante seu Oracle HTTP Server em um grupo Amazon EC2 Auto Scaling configurado para aspen em várias zonas de disponibilidade. Em seguida, coloque o servidor atrás de um balanceador de carga elástico ELB. Para fornecer proteção adicional contra falhas no host, você pode ativar o Amazon EC2 Auto Recovery.

Escalabilidade

A elasticidade da Nuvem AWS ajuda você a escalar aplicativos horizontal ou verticalmente em resposta aos requisitos de workload.

Escala vertical

Para escalar verticalmente seu aplicativo, você pode alterar o tamanho e o tipo das EC2 instâncias da Amazon que estão executando seus componentes do Oracle BI 12c. Você não precisa provisionar instâncias em excesso no início da implantação e incorrer em custos desnecessários.

Escalabilidade horizontal

O Amazon EC2 Auto Scaling ajuda você a escalar horizontalmente seu aplicativo adicionando ou removendo automaticamente servidores gerenciados com base nos requisitos de carga de trabalho.

> **Note**
>
> A escalabilidade horizontal com o Amazon EC2 Auto Scaling requer habilidades de script e testes completos para ser implementada.

Backup e recuperação

A seguir está uma lista das práticas recomendadas de backup e recuperação para recursos específicos do Oracle BI 12c hospedados na Nuvem AWS:

- Repositórios de metadados do Oracle Business Intelligence: o Amazon RDS cria e salva automaticamente backups de suas instâncias de banco de dados. Esses backups são mantidos por um período especificado por você. Certifique-se de definir as configurações de duração e retenção do backup do Amazon RDS com base nos requisitos de proteção de dados. Para obter mais informações, consulte Backup e restauração do Amazon RDS.
- Servidores gerenciados, servidores de administração e servidores de nível web: certifique-se de configurar os snapshots do Amazon EBS com base em seus requisitos de proteção e retenção de dados.
- Armazenamento compartilhado: você pode gerenciar o backup e a recuperação de arquivos armazenados no Amazon EFS usando o AWS Backup. O serviço AWS Backup também pode ser implantado para gerenciar centralmente o backup e a recuperação de outros serviços, incluindo Amazon, EC2 Amazon EBS e Amazon RDS. Para obter mais informações, consulte O que é o AWS Backup? No Guia do desenvolvedor do AWS Backup.

Segurança e conformidade

A seguir está uma lista das práticas recomendadas de segurança e dos serviços da AWS que podem ajudar você a proteger seus aplicativos Oracle BI 12c na Nuvem AWS:

- Criptografia em repouso: Amazon RDS, Amazon EFS e Amazon EBS oferecem suporte a algoritmos de criptografia padrão do setor. Você pode usar o AWS Key Management Service (AWS KMS) para criar e gerenciar chaves criptográficas e controlar seu uso nos serviços da AWS e em seus aplicativos. Você também pode configurar o Oracle Transparent Data Encryption (TDE) na instância de banco de dados Amazon RDS para Oracle que hospeda seu banco de dados do repositório Oracle BI 12c.
- Criptografia em trânsito: é uma prática recomendada habilitar os protocolos SSL ou TLS para proteger os dados em trânsito entre as várias camadas da instalação do Oracle BI 12c. Você pode usar o AWS Certificate Manager (ACM) para provisionar, gerenciar e implantar certificados SSL e TLS públicos e privados para os recursos do Oracle BI 12c.
- Segurança de rede: certifique-se de implantar seus recursos do Oracle BI 12c em uma Amazon VPC que tenha os controles de acesso apropriados configurados para seu caso de uso. Configure seus grupos de segurança para filtrar o tráfego de entrada e saída das EC2 instâncias da Amazon

que estão executando sua instalação. Além disso, certifique-se de configurar as Listas de Controle de Acesso à Rede (NACLs) que permitem ou negam tráfego com base em regras definidas.

- Monitoramento e registro: você pode usar CloudTrail a AWS para rastrear chamadas de API para sua infraestrutura da AWS, incluindo seus recursos do Oracle BI 12c. Essa funcionalidade é útil ao rastrear alterações na infraestrutura ou ao realizar uma análise de segurança. Você também pode usar CloudWatch a Amazon para visualizar dados operacionais que podem fornecer uma visão prática sobre o desempenho e a integridade do seu aplicativo Oracle BI 12c. Você também pode configurar alarmes e realizar ações automatizadas com base nesses alarmes. O Amazon RDS fornece ferramentas adicionais de monitoramento, incluindo monitoramento aprimorado e Performance Insights.

Migre um cluster Apache Kafka local para o Amazon MSK usando MirrorMaker

Criado por Han Zhang (AWS) e Tanner Pratt (AWS)

Resumo

Esse padrão fornece orientação para migrar um cluster do Apache Kafka on-premises, autogerenciado ou hospedado para o Amazon Managed Streaming for Apache Kafka (Amazon MSK). Você também pode usar esse padrão para migrar de um cluster do Amazon MSK para outro.

O Apache Kafka inclui o MirrorMaker recurso, que replica dados entre dois clusters do Kafka. MirrorMaker consiste em uma coleção de consumidores, que fazem parte de um grupo de consumidores. Os consumidores leem os dados dos tópicos no cluster de origem e, em seguida, passam esses dados aos produtores, que gravam os dados no cluster de destino.

A documentação do Amazon MSK contém uma visão geral de alto nível do processo de uso da MirrorMaker versão 1.0 para migrar clusters Kafka locais para o Amazon MSK. Esse padrão complementa essas informações oferecendo step-by-step instruções abrangentes para o uso da MirrorMaker versão 2.0.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um cluster de origem do Kafka que é um dos seguintes:
  - Em um datacenter on-premises
  - Autogerenciado na nuvem
  - Hospedado por meio de um parceiro

Limitações

- Para usar a MirrorMaker versão 2.0, o cluster de origem deve estar operando o Apache Kafka versão 2.4.0 ou posterior. Para versões anteriores, consulte as instruções na documentação do Amazon MSK para usar a MirrorMaker versão 1.0.

Versões do produto

- MirrorMaker versão 2.0
- Apache Kafka versão 2.4.0 ou superior. Para obter mais informações sobre as versões do Apache Kafka suportadas pelo Amazon MSK, consulte Versões suportadas do Apache Kafka.

Arquitetura

Pilha de tecnologia de origem

- Cluster Kafka on-premises ou autogerenciado

Pilha de tecnologias de destino

- Cluster do Amazon MSK

Arquitetura de destino

O diagrama mostra o seguinte processo:

1. MirrorMaker lê os dados dos tópicos e grupos de consumidores no cluster Kafka de origem.
2. MirrorMaker replica os dados e as informações do consumidor para o cluster Amazon MSK de destino.

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Managed Streaming for Apache Kafka (Amazon MSK) é um serviço totalmente gerenciado que ajuda você a criar e executar aplicações que usam o Apache Kafka para processar dados em streaming.

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- Apache Kafka é uma plataforma de streaming de eventos de código aberto. Nesse padrão, você usa o MirrorMakerrecurso do Kafka para realizar a migração entre clusters.

Práticas recomendadas

Você pode executá-lo MirrorMaker nos ambientes de origem ou de destino, mas é recomendável executá-lo o mais próximo possível do cluster de destino. Para obter mais informações, consulte Boas práticas: consumir do remoto, produzir ao local na documentação do Apache Kafka.

Épicos

Criar a VPC e visar a um cluster do Amazon MSK

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	1. Crie uma VPC na conta de destino da AWS. Para obter instruções, consulte Criar uma VPC. 2. Crie três sub-redes privadas em zonas de disponibilidade diferentes na nova VPC. Para obter instruções, consulte Criar uma sub-rede. O uso de zonas de disponibilidade diferentes fornece alta disponibilidade e tolerância a falhas.	Administrador de sistemas da AWS, DevOps engenheiro, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Note Se você estiver usando uma conexão pública de internet para migrar o cluster Kafka, crie sub-redes públicas e habilite o acesso público ao cluster Amazon MSK.	
Crie o cluster do Amazon MSK.	Crie um cluster do Amazon MSK. Para obter instruções, consulte Criar um cluster usando o Console de Gerenciamento da AWS ou Criar um cluster usando a AWS CLI. Configure o cluster para usar a VPC e as sub-redes que você criou anteriormente.	Administrador de sistemas da AWS, DevOps engenheiro, administrador de nuvem

Configurar MirrorMaker

Tarefa	Descrição	Habilidades necessárias
Instalar MirrorMaker.	1. Execute uma EC2 instância. 2. Conecte-se à sua EC2 instância. 3. Na EC2 instância, baixe e extraia a versão mais	Administrador de sistemas da AWS, administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	recente do Kafka. Para obter instruções, consulte Início rápido (document ação do Kafka). **Note** Nesse padrão, você instala MirrorMaker 2.0 como um MirrorMaker cluster dedicado em uma EC2 instância da Amazon. Essa opção é aceitável para ambientes de desenvolvimento e é a abordagem usada nesse padrão. Para obter mais informações sobre outras opções de implantação para MirrorMaker 2.0, consulte a seção Informações adicionais desse padrão.	

Tarefa	Descrição	Habilidades necessárias
Especifique as informações do cluster Kafka.	Na pasta `bin` de instalação do cliente Kafka, crie um arquivo mm2.properties e configure-o para seu cluster do Kafka de origem. Para obter instruções, consulte Como executar um MirrorMaker cluster dedicado (documentação do Kafka).	Administrador de sistemas da AWS, administrador de nuvem, DevOps engenheiro
Começar MirrorMaker.	Digite o comando a seguir para iniciar MirrorMaker e passar o arquivo mm2.properties. `$ ./bin/connect-mirror-maker.sh mm2.properties`	Administrador de sistemas da AWS, administrador de nuvem, DevOps engenheiro
Monitorar o andamento.	Verifique o progresso inspecionando o intervalo entre o último deslocamento de cada tópico e o deslocamento atual do tópico que está sendo consumido. MirrorMaker Para obter instruções, consulte Monitoramento da replicação geográfica na documentação do Kafka.	Administrador de sistemas da AWS, administrador de nuvem, DevOps engenheiro

Substituir

Tarefa	Descrição	Habilidades necessárias
Interrompa os aplicativos de consumo.	Interrompa todos os aplicativos de consumo que	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	consomem dados do cluster de origem.	
Inicie os aplicativos de consumo.	Altere a configuração de bootstrap dos aplicativos para apontar para o cluster de destino. Em seguida, comece a consumir no cluster de destino.	Desenvolvedor de aplicativos
Encerre todos os produtores no cluster de origem.	Quando os aplicativos do consumidor estiverem sendo consumidos com sucesso no cluster de destino, interromp a os produtores no cluster de origem.	Desenvolvedor de aplicativos
Iniciar os produtores no cluster de destino.	Altere a configuração dos servidores bootstrap do produtor e aponte para o cluster de destino. Aguarde MirrorMaker a conclusão do espelhamento de todos os dados do cluster de origem antes de iniciar os produtores.	Desenvolvedor de aplicativos
Pare MirrorMaker.	Depois que os produtores mudarem para o cluster de destino, pare MirrorMaker.	Administrador de sistemas da AWS, administrador de nuvem, DevOps engenheiro

Recursos relacionados

Recursos da AWS

- Migração de clusters usando MirrorMaker (documentação do Amazon MSK)
- Laboratórios de migração do Amazon MSK (AWS Workshop Studio)

Outros recursos

- MirrorMaker 2.0 (Propostas de melhoria do Apache Kafka)
- Replicação geográfica: espelhamento de dados entre clusters (documentação do Apache Kafka)

Mais informações

Esse padrão é executado na MirrorMaker versão 2.0 como um MirrorMaker cluster dedicado na Amazon EC2. Esta opção é aceitável para ambientes de desenvolvimento. Embora isso não seja discutido nesse padrão, você também pode executar a MirrorMaker versão 2.0 em um cluster do Kafka Connect. Essa opção de implantação usa uma estrutura dentro do ecossistema Kafka que melhora o dimensionamento e a manutenção. Você implanta o conector em um cluster do Kafka Connect com a configuração associada para executar o aplicativo. O conector pode ser executado no modo autônomo para desenvolvimento ou teste ou no modo distribuído para produção. Para obter mais informações, consulte Executando MirrorMaker em um cluster Connect (documentação do Apache Kafka). Para obter mais informações sobre outras opções de implantação MirrorMaker 2.0, consulte Passo a passo: Executando MirrorMaker 2.0 (documentação do Kafka).

Migre um pilha ELK para a Nuvem Elastic na AWS

Criado por Battulga Purevragchaa (AWS), Juday reddy e Antony Prasad Thevaraj (AWS)

Resumo

Elastic fornece serviços há muitos anos, com seus usuários e clientes normalmente gerenciando a própria Elastic on-premises. Nuvem Elastic, o serviço gerenciado do Elasticsearch, fornece uma forma de consumir o Elastic Stack (ELK Stack) e soluções para pesquisa corporativa, observabilidade e segurança. Você pode acessar as soluções da Elastic com aplicativos como Logs, Metrics, APM (monitoramento de desempenho de aplicativos) e SIEM (gerenciamento de eventos e informações de segurança). Você pode usar atributos integrados, como machine learning, gerenciamento do ciclo de vida do índice e Kibana Lens (para visualizações de arrastar e soltar).

Quando você migra do Elasticsearch autogerenciado para a Nuvem Elastic, o serviço Elasticsearch cuida do seguinte:

- Provisionamento e gerenciamento da infraestrutura subjacente
- Criação e gerenciamento de clusters do Elasticsearch
- Aumentando e diminuindo a escala de clusters
- Atualizações, patches e snapshots

Isso lhe dá mais tempo para se concentrar na solução de outros desafios.

Esse padrão define como migrar o Elasticsearch 7.13 on-premises para o Elasticsearch na Nuvem Elastic na Amazon Web Services (AWS). Outras versões podem exigir pequenas modificações nos processos descritos nesse padrão. Para obter mais informações, entre em contato com o representante da Elastic.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da AWS com acesso ao Amazon Simple Storage Service (Amazon S3) para snapshots
- Um link privado seguro e com largura de banda suficientemente alta para copiar arquivos de dados de snapshots para o Amazon S3

- Amazon S3 Transfer Acceleration
- Políticas do Elastic Snapshot para garantir que a ingestão de dados seja arquivada regularmente, seja em um armazenamento de dados local suficientemente grande ou em um armazenamento remoto (Amazon S3)

Você deve entender o tamanho dos seus snapshots e das políticas de ciclo de vida dos índices que os acompanham on-premises antes de iniciar a migração. Para obter mais informações, entre em contato com a Elastic.

Funções e habilidades

O processo de migração também exige as funções e a experiência descritas na tabela a seguir.

Função	Experiência	Responsabilidades
Suporte de aplicativos	Familiaridade com a Nuvem Elastic e o Elastic on premises	Todas as tarefas relacionadas à Elastic
Administrador de sistemas ou DBA	Conhecimento profundo do ambiente da Elastic on-premises e de sua configuração	Capacidade de provisionar armazenamento, instalar e usar a interface da linha de AWS Command Line Interface (AWS CLI) e identificar todas as fontes de dados que alimentam a Elastic on-premises
Administrador de rede	Conhecimento da conectividade, segurança e desempenho da rede on-premises com a AWS	Estabelecimento de links de rede on-premises para o Amazon S3, com uma compreensão da largura de banda de conectividade

Limitações

- O Elasticsearch na Nuvem Elastic está disponível somente nas regiões compatíveis da AWS (setembro de 2021).

Versões do produto

- Elasticsearch 7.13

Arquitetura

Pilha de tecnologia de origem

Elasticsearch 7.13 on-premises ou superior:

- Snapshots do cluster
- Snapshots de índices
- Configurações do Beats

Arquitetura de tecnologia de origem

O diagrama a seguir mostra uma arquitetura on-premises típica com diferentes métodos de ingestão, tipos de nós e Kibana. Os diferentes tipos de nós refletem as funções de cluster, autenticação e visualização do Elasticsearch.

1. Ingestão do Beats para o Logstash
2. Ingestão da fila de mensagens do Beats para o Apache Kafka
3. Ingestão do Filebeat para o Logstash
4. Ingestão da fila de mensagens do Apache Kafka para o Logstash
5. Ingestão do Logstash para um cluster do Elasticsearch
6. Cluster do Elasticsearch
7. Nó de autenticação e notificação
8. Kibana e nós blob

Pilha de tecnologias de destino

A Nuvem Elastic é implantada em sua conta de software como serviço (SaaS) em várias regiões da AWS com replicação entre clusters.

- Snapshots do cluster

- Snapshots de índices
- Configurações do Beats
- Nuvem Elastic
- Network Load Balancer
- Amazon Route 53
- Amazon S3

Arquitetura de destino

A infraestrutura gerenciada da Nuvem Elastic é:

- Altamente disponível, estando presente em várias zonas de disponibilidade e várias regiões da AWS.
- Região tolerante a falhas porque os dados (índices e snapshots) são replicados usando a replicação entre clusters (CCR) da Nuvem Elastic.
- Arquivamento, porque os snapshots são arquivados no Amazon S3
- Partição de rede tolerante por meio de uma combinação de Network Load Balancers e Route 53
- Ingestão de dados originada (mas não limitada a) Elastic APM, Beats, Logstash

Etapas de migração de alto nível

A Elastic desenvolveu sua própria metodologia prescritiva para migrar o Elastic Cluster on-premises para a Nuvem Elastic. A metodologia da Elastic está diretamente alinhada e complementa a orientação e as melhores práticas de migração da AWS, incluindo o Well-Architected Framework e e o Programa de Aceleração da Migração (MAP). Normalmente, as três fases de migração para a AWS são as seguintes:

- Avaliar
- Mobilizar
- Migrar e modernizar

A Elastic segue fases de migração semelhantes com terminologia complementar:

- Iniciar

- Planejar
- Implementar
- Entregar
- Fechar

A Elastic usa a Metodologia de Implementação da Elastic para facilitar a entrega dos resultados do projeto. Isso é inclusivo por design para garantir que a Elastic, as equipes de consultoria e as equipes de clientes trabalhem juntas com clareza para fornecer conjuntamente os resultados pretendidos.

A metodologia Elastic combina o faseamento tradicional em cascata com o Scrum na fase de implementação. As configurações dos requisitos técnicos são fornecidas iterativamente de forma colaborativa, minimizando os riscos.

Ferramentas

Serviços da AWS

- Amazon Route 53: o Amazon Route 53 é um web service do Sistema de Nomes de Domínio (DNS) altamente disponível e dimensionável. Você pode usar o Route 53 para executar três funções principais em qualquer combinação: registro de domínios, roteamento de DNS e verificação de integridade.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web. Esse padrão usa um bucket do S3 e o Amazon S3 Transfer Acceleration.
- Elastic Load Balancing — O Elastic Load Balancing distribui automaticamente seu tráfego de entrada em vários destinos, EC2 como instâncias, contêineres e endereços IP, em uma ou mais zonas de disponibilidade.

Outras ferramentas

- Beats: o Beats envia dados do Logstash ou do Elasticsearch
- Nuvem Elastic: a Nuvem Elastic é um serviço gerenciado para hospedar o Elasticsearch.

- Elasticsearch: o Elasticsearch é um mecanismo de pesquisa e análise que usa o Elastic Stack para armazenar centralmente seus dados para pesquisas e análises escaláveis. Esse padrão também usa a criação de snapshots e a replicação entre clusters.
- Logstash: o Logstash é um pipeline de processamento de dados do lado do servidor que ingere dados de várias origens, os transforma e os envia para seu armazenamento de dados.

Épicos

Preparar-se para a migração

Tarefa	Descrição	Habilidades necessárias
Identifique os servidores que executam a solução on-premises da Elastic.	Confirme se a migração da Elastic é compatível.	Proprietário do App
Entenda a configuração do servidor on-premises.	Para entender a configuração do servidor necessária para conduzir cargas de trabalho on-premises com êxito, encontre o espaço ocupado pelo hardware do servidor, a configuração da rede e as características de armazenamento que estão em uso atualmente	Suporte de aplicativos
Reúna informações da conta do usuário e do aplicativo.	Identifique os nomes de usuário e nomes de aplicativos que são usados pelo ambiente on-premises da Elastic.	Administrador de sistemas, suporte de aplicativos
Document Beats e configuração do remetente de dados.	Para documentar as configurações, veja as fontes de dados e coletores existentes. Para obter mais informações,	Suporte de aplicativos

Tarefa	Descrição	Habilidades necessárias
	consulte a documentação do Elastic.	
Determine a velocidade e o volume dos dados.	Estabeleça uma linha de base para a quantidade de dados que o cluster está manipulando.	Administrador de sistemas, suporte de aplicativos
Documente cenários de RPO e RTO.	Documente os cenários de objetivo de ponto de recuperação (RPO) e objetivo de tempo de recuperação (RTO) em termos de interrupções e contratos de nível de serviço ()SLAs.	Proprietário do aplicativo, administrador de sistemas, suporte de aplicativos
Determine as configurações ideais do ciclo de vida do snapshot.	Defina com que frequência os dados precisam ser protegidos usando snapshots da Elastic durante e após a migração.	Proprietário do aplicativo, administrador de sistemas, suporte de aplicativos
Defina as expectativas de desempenho pós-migração.	Gere métricas sobre a atualização de tela atual e esperada, os tempos de execução de consultas e os comportamentos da interface do usuário.	Administrador de sistemas, suporte de aplicativos
Documente os requisitos de transporte, largura de banda e disponibilidade do acesso à Internet.	Verifique a velocidade, a latência e a resiliência das conexões de internet para copiar snapshots para o Amazon S3.	Administrador de rede

Tarefa	Descrição	Habilidades necessárias
Documente os custos atuais do runtime on-premises da Elastic.	Garanta que o dimension amento do ambiente de destino da AWS seja projetado para ser de alto desempenho e econômico.	DBA, administrador de sistemas, suporte de aplicativ os
Identifique as necessidades de autenticação e autorização.	Os atributos de segurança do Elastic Stack fornecem domínios integrados, como Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML) e OpenID Connect (OIDC).	DBA, administrador de sistemas, suporte de aplicativ os
Entenda os requisitos regulatórios específicos com base na localização geográfic a.	Garanta que os dados sejam exportados e criptografados de acordo com seus requisito s e com quaisquer requisitos nacionais relevantes.	DBA, administrador de sistemas, suporte de aplicativ os

Implementar a migração

Tarefa	Descrição	Habilidades necessárias
Prepare a área de preparação no Amazon S3.	Para receber snapshots no Amazon S3, crie um bucket do S3e um perfil temporário do AWS Identity and Access Management (IAM) com acesso total ao bucket recém-criado. Para obter mais informações, consulte Criar uma função para delegar permissões a um usuário do	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	IAM. Ou você pode usar o AWS Security Token Service para solicitar credenciais de segurança temporárias. Mantenha o ID da chave de acesso, a chave de acesso secreta e o token da sessão em segurança. Habilitar o Transfer Acceleration do Amazon S3 no bucket.	
Instale a AWS CLI e o plug-in Amazon S3 on-premises.	Em cada nó do Elasticsearch, execute o comando a seguir. `sudo bin/elasticsearch-plugin install repository-s3` Em seguida, reinicie o nó.	Administrador da AWS

Configurar o acesso ao cliente Amazon S3.	Adicione as chaves criadas anteriormente executando os comandos a seguir.
	
	`elasticsearch-keystore add s3.client.default.access_key`
	
	`elasticsearch-keystore add s3.client.default.secret_key`
	
	`elasticsearch-keystore add s3.client.default.session_token`
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Registre um repositório de snapshots para dados da Elastic	Use as ferramentas de desenvolvimento do Kibana para informar ao cluster on-premises local em qual bucket remoto do S3 gravar.	Administrador da AWS
Configure a política de snapshot.	Para configurar o gerenciamento do ciclo de vida de snapshots, na guia Políticas do Kibana, escolha a política SLM e defina quais horários, fluxos de dados ou índices devem ser incluídos e quais nomes usar. Configure uma política que tire snapshots frequentes. Os snapshots são incrementais e fazem uso eficiente do armazenamento. Combine a sua decisão de avaliação de prontidão. Uma política também pode especificar uma política de retenção e excluir snapshots automaticamente quando eles não forem mais necessários.	Suporte de aplicativos
Verifique se os snapshots funcionam.	Nas Ferramentas de desenvolvimento do Kibana, execute o comando a seguir. `GET _snapshot/<your_repo_name>/_all`	Administrador da AWS, Suporte de aplicativos,

Tarefa	Descrição	Habilidades necessárias
Implante um novo cluster na Nuvem Elastic.	Faça login No campo Elastic e escolha um cluster para “observabilidade, pesquisa ou segurança” derivado das descobertas de sua empresa na avaliação de prontidão.	Administrador da AWS, Suporte de aplicativos
Configure o acesso ao armazenamento de chaves do cluster.	O novo cluster precisa acessar o bucket do S3 que armazenará os snapshots . No Elasticsearch Service Console, escolha Segurança e insira as chaves secretas e de acesso do IAM que você criou anteriormente.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Configurar o cluster hospedado da Nuvem Elastic para acessar o Amazon S3.	Configure um novo acesso de cluster ao repositório de snapshots criado anteriormente no Amazon S3. Usando o Kibana, faça o seguinte: 1. Escolha Stack Management, Snapshot Settings,. RegisterRepo 2. No campo Alias, insira o nome do repositório. 3. Para o nome do cliente S3, escolha secundário. 4. Adicione ao repositório o bucket do S3 criado anteriormente. 5. Escolha Comprimir snapshot. 6. Para as configurações de criptografia, mantenha os valores padrão.	Administrador da AWS, Suporte de aplicativos
Verifique o novo repositório do Amazon S3.	Garanta que você possa acessar seu novo repositório hospedado no cluster da Nuvem Elastic.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Inicialize o cluster de serviços do Elasticsearch.	No Elasticsearch Service Console, inicialize o cluster de serviços Elasticsearch a partir do snapshot do S3.
	
	Execute um dos seguintes comandos como POSTAR.
	
	`*/_close?expand_wildcards=all`
	
	`/_snapshot/<your-repo-name>/ <your-snapshot-name>/_restore`
	
	`*/_open?expand_wildcards=all`
		Suporte de aplicativos

Concluir a migração

Tarefa	Descrição	Habilidades necessárias
Verifique se a restauração do snapshot foi bem-sucedida.	Usando o Kibana Dev Tools, execute o comando a seguir. `GET _cat/indices`	Suporte de aplicativos
Implemente serviços de ingestão.	Conecte os endpoints do Beats e do Logstash ao novo endpoint do serviço Elasticsearch.	Suporte de aplicativos

Teste o ambiente de cluster e limpe

Tarefa	Descrição	Habilidades necessárias
Valide o ambiente de cluster.	Depois que o ambiente de cluster Elastic on-premises for migrado para a AWS, você poderá se conectar a ele e usar suas próprias ferrament as de teste de aceitação do usuário (UAT) para validar o novo ambiente.	Suporte de aplicativos
Limpe os recursos.	Depois de validar se o cluster foi migrado com êxito, remova o bucket do S3 e o perfil do IAM usada para a migração.	Administrador da AWS

Recursos relacionados

Referência da Elastic

- Nuvem Elastic
- Elasticsearch e Kibana gerenciados na AWS
- Pesquisa corporativa Elastic
- Integrações Elastic
- Observabilidade Elastic
- Segurança Elastic
- Batidas
- APM Elastic
- Migre para o gerenciamento do ciclo de vida do índice
- Assinaturas da Elastic
- Entre em contato com a Elastic

Postagens de blog da Elastic

- Como migrar do Elasticsearch autogerenciado para a Nuvem Elastic na AWS (post no blog)
- Migração para a Nuvem Elastic (publicação no blog)

Documentação da Elastic

- Tutorial: Automatize os backups com o SLM
- ILM: gerencie o ciclo de vida do índice
- Logstash
- Replicação entre clusters (CCR)
- Ingestão de pipelines
- Execute solicitações da API Elasticsearch
- Retenção de snapshots

Vídeo e webinar Elastic

- Migração para a nuvem Elastic
- Nuvem Elastic: Por que os clientes estão migrando (webinar)

Referências da AWS

- Nuvem Elastic no AWS Marketplace
- Interface de linha de comando da AWS
- AWS Direct Connect
- Programa de Aceleração da Migração da AWS
- Network Load Balancers
- Regiões e zonas de disponibilidade
- Amazon Route 53
- Amazon Simple Storage Service
- Amazon S3 Transfer Acceleration
- Conexões da VPN
- Well-Architected Framework

Mais informações

Se você planeja migrar cargas de trabalho complexas, contrate a Elastic Consulting Services. Se você tiver dúvidas básicas relacionadas a configurações e serviços, entre em contato com a equipe de Suporte da Elastic.

Migre dados para o Nuvem AWS usando o Starburst

Criado por Antony Prasad Thevaraj (AWS), Shaun Van Staden e Suresh Veeragoni (AWS)

Resumo

O Starburst ajuda a acelerar sua jornada de migração de dados para a Amazon Web Services (AWS) fornecendo um mecanismo de consulta empresarial que reúne as fontes de dados existentes em um único ponto de acesso. Você pode executar análises em várias fontes de dados para obter informações valiosas antes de finalizar qualquer plano de migração. Sem interromper a business-as-usual análise, você pode migrar os dados usando o mecanismo Starburst ou um aplicativo dedicado de extração, transformação e carregamento (ETL).

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Uma nuvem privada virtual (VPC).
- Amazon Elastic Kubernetes Service (Amazon EKS): cluster
- Um grupo de Auto Scaling da Amazon Elastic Compute Cloud (Amazon EC2)
- Uma lista das workloads atuais do sistema que precisem ser migradas
- Conectividade de rede AWS com seu ambiente local

Arquitetura

Arquitetura de referência

O diagrama de arquitetura de alto nível a seguir mostra a implantação típica do Starburst Enterprise no: Nuvem AWS

1. O cluster Starburst Enterprise é executado dentro do seu. Conta da AWS
2. Um usuário se autentica usando o Lightweight Directory Access Protocol (LDAP) ou Open Authorization (OAuth) e interage diretamente com o cluster Starburst.
3. O Starburst pode se conectar a várias fontes de AWS dados, como AWS Glue Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS) e Amazon

Redshift. O Starburst fornece recursos de consulta federada em todas as fontes de dados no local ou em outros ambientes de nuvem. Nuvem AWS

4. Você inicia o Starburst Enterprise em um cluster Amazon EKS usando chart do Helm.
5. A Starburst Enterprise usa grupos do Amazon Auto EC2 Scaling e EC2 Amazon Spot Instances para otimizar a infraestrutura.
6. O Starburst Enterprise se conecta diretamente às suas fontes de dados on-premises existentes para ler dados em tempo real. Além disso, se você tiver uma implantação do Starburst Enterprise existente nesse ambiente, poderá conectar diretamente seu novo cluster Starburst no Nuvem AWS a esse cluster existente.

Observe o seguinte:

- O Starburst não é uma plataforma de virtualização de dados. É um mecanismo de consulta de processamento paralelo massivo (MPP) baseado em SQL que forma a base de uma estratégia geral de data mesh para análise.
- Quando o Starburst é implantado como parte de uma migração, ele tem conectividade direta com a infraestrutura on-premises existente.
- O Starburst fornece vários conectores corporativos e de código aberto integrados que facilitam a conectividade com uma variedade de sistemas herdados. Para obter uma lista completa dos conectores e seus recursos, consulte Conectores no guia do usuário do Starburst Enterprise.
- O Starburst pode consultar dados em tempo real a partir de fontes de dados on-premises. Isso evita interrupções nas operações comerciais regulares durante a migração dos dados.
- Se você estiver migrando de uma implantação local existente do Starburst Enterprise, poderá usar um conector especial, o Starburst Stargate, para conectar seu cluster Starburst Enterprise diretamente ao seu cluster local. AWS Isso fornece benefícios adicionais de desempenho quando usuários corporativos e analistas de dados estão federando consultas do Nuvem AWS para seu ambiente local.

Visão geral do processo de alto nível

Você pode acelerar os projetos de migração de dados usando o Starburst porque o Starburst permite insights sobre todos os seus dados, antes de migrá-los. A imagem a seguir mostra o processo típico de migração de dados usando o Starburst.

Funções

Normalmente, as seguintes funções são necessárias para concluir uma migração usando o Starburst:

- Administrador de nuvem: responsável por disponibilizar recursos de nuvem para executar o aplicativo Starburst Enterprise
- Administrador do Starburst: responsável pela instalação, configuração, gerenciamento e suporte do aplicativo Starburst
- Engenheiro de dados: responsável por:
  - Migração do bancos de dados Oracle para a nuvem
  - Criando visualizações semânticas para apoiar a análise
- Proprietário da solução ou do sistema: responsável pela implementação geral da solução

Ferramentas

Serviços da AWS

- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.

Outras ferramentas

- Helm: o Helm é um gerenciador de pacotes Helm para o Kubernetes ajuda a instalar e gerenciar aplicações em seu cluster do Kubernetes.
- Starburst Enterprise: o Starburst Enterprise é um mecanismo de consulta de processamento paralelo massivo (MPP) baseado em SQL que forma a base de uma estratégia geral de data mesh para análise.
- Starburst Stargate — Starburst Stargate vincula catálogos e fontes de dados em um ambiente Starburst Enterprise, como um cluster em um data center local, aos catálogos e fontes de dados em outro ambiente Starburst Enterprise, como um cluster no. Nuvem AWS

Épicos

Avaliar os dados

Tarefa	Descrição	Habilidades necessárias
Identifique e priorize seus dados.	Identifique os dados que você deseja mover. Grandes sistemas herdados on-premises podem incluir dados essenciais que você deseja migrar junto com dados que você não quer mover ou não pode ser movido por motivos de conformidade. Começar com um inventário de dados ajuda a priorizar quais dados você deve segmentar primeiro. Para obter mais informações, consulte Conceitos básicos do portfólio automatizado.	Engenheiro de dados, DBA
Explore, faça o inventário e faça backup de seus dados.	Valide a qualidade, a quantidade e a relevância dos dados para seu caso de uso. Faça backup ou crie um instantâneo dos dados conforme necessário e finalize o ambiente de destino para os dados.	Engenheiro de dados, DBA

Configurar o ambiente Starburst Enterprise

Tarefa	Descrição	Habilidades necessárias
Configure o Starburst Enterprise no. Nuvem AWS	Enquanto os dados estão sendo catalogados, configure o Starburst Enterprise em um cluster gerenciado do Amazon EKS. Para obter mais informações, consulte Implantação com o Kubernetes na documentação de referência do Starburst Enterprise. Isso permite business-as-usual análises enquanto a migração de dados está em andamento.	Administrador da AWS, desenvolvedor de aplicativos
Conecte o Starburst às fontes de dados.	Depois de identificar os dados e configurar o Starburst Enterprise, conecte o Starburst às fontes de dados. O Starburst lê dados diretamente da fonte de dados como uma consulta SQL. Para obter mais informações, consulte a documentação de referência do Starburst Enterprise.	Administrador da AWS, desenvolvedor de aplicativos

Migrar os dados

Tarefa	Descrição	Habilidades necessárias
Criar e executar pipelines de ETL.	Iniciar o processo de migração de dados. Essa atividade pode	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	ocorrer ao mesmo tempo que a business-as-usual análise. Para a migração, você pode usar um produto de terceiros ou Starburst. O Starburst tem a capacidade de ler e gravar dados em diferentes fontes. Para obter mais informaçõ es, consulte a documentação de referência do Starburst Enterprise.	
Valide os dados.	Depois que os dados forem migrados, valide os dados para garantir que todos os dados necessários tenham sido movidos e estejam intactos.	Engenheiro de dados, DevOps engenheiro

Substituir

Tarefa	Descrição	Habilidades necessárias
Substitua os dados.	Depois que a migração e a validação dos dados estiverem concluídas, você poderá recortar os dados. Isso envolve a alteração dos links de conexão de dados no Starburst. Em vez de apontar para as fontes on-premises, você aponta para as novas fontes na nuvem e atualiza as visualizações semântica s. Para obter mais informaçõ	Engenheiro de dados, líder de substituição

Tarefa	Descrição	Habilidades necessárias
	es, consulte Conectores na documentação de referência do Starburst Enterprise.	
Implemente para os usuários.	Os consumidores de dados começam a trabalhar com as fontes de dados migradas. Esse processo é invisível para os usuários finais de análise.	Líder de substituição, engenheiro de dados

Recursos relacionados

AWS Marketplace

- Galáxia Starburst
- Empresa Starburst
- Dados Starburst JumpStart
- Starburst Enterprise com Graviton

Documentação do Starburst

- Guia do usuário do Starburst Enterprise
- Documentação de referência do Starburst Enterprise

Outra AWS documentação

- Comece com a descoberta automatizada de portfólio (AWS orientação prescritiva)
- Otimizando o custo e o desempenho da infraestrutura em nuvem com o Starburst em AWS(postagem no blog)AWS

Otimize a ingestão de ETL do tamanho do arquivo de entrada na AWS

Criado por Apoorva Patrikar (AWS)

Resumo

Esse padrão mostra como otimizar a etapa de ingestão do processo de extração, transformação e carregamento (ETL) para big data e cargas de trabalho do Apache Spark no AWS Glue otimizando o tamanho do arquivo antes de processar seus dados. Use esse padrão para evitar ou resolver o problema de arquivos pequenos. Ou seja, quando um grande número de arquivos pequenos retarda o processamento de dados devido ao tamanho agregado dos arquivos. Por exemplo, centenas de arquivos com apenas algumas centenas de kilobites cada podem reduzir significativamente as velocidades de processamento de dados para suas tarefas do AWS Glue. Isso ocorre porque o AWS Glue deve executar funções de lista internas no Amazon Simple Storage Service (Amazon S3) e o YARN (Yet Another Resource Negotiator) deve armazenar uma grande quantidade de metadados. Para melhorar a velocidade de processamento de dados, você pode usar o agrupamento para permitir que suas tarefas de ETL leiam um grupo de arquivos de entrada em uma única partição na memória. A partição agrupa automaticamente arquivos menores. Como alternativa, você pode usar código personalizado para adicionar lógica de lote aos seus arquivos existentes.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um ou mais trabalhos da AWS Glue
- Uma ou mais cargas de trabalho de big data ou Apache Spark
- Um bucket do S3

Arquitetura

O padrão a seguir mostra como os dados em diferentes formatos são processados por uma tarefa do AWS Glue e, em seguida, armazenados em um bucket do S3 para obter visibilidade da performance.

O diagrama mostra o seguinte fluxo de trabalho:

1.
> **Note**
>
> Uma tarefa do AWS Glue converte arquivos pequenos nos formatos CSV, JSON e Parquet em quadros dinâmicos. : o tamanho do arquivo de entrada tem o impacto mais significativo no desempenho do trabalho do AWS Glue.

2. A tarefa do AWS Glue executa funções de lista internas em um bucket do S3.

Ferramentas

- O AWS Glue é um serviço de ETL totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Épicos

Use o agrupamento para otimizar a ingestão de ETL durante a leitura

Tarefa	Descrição	Habilidades necessárias
Especifique o tamanho do grupo.	Se você tiver mais de 50.000 arquivos, o agrupamento é feito por padrão. No entanto, você também pode usar o agrupamento para menos de 50.000 arquivos especificando o tamanho do grupo no parâmetro `connectionOptions` . O parâmetro `connectionOptions` está no método `create_dynamic_frame.from_options` .	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
Escreva o código de agrupamento.	Use o método `create_dynamic_frame` para criar um quadro dinâmico. Por exemplo: `S3bucket_node1 = glueContext.create_dynamic_frame.from_options(format_options={"multiline": False}, connection_type="s3", format="json", connection_options={ "paths": ["s3://bucket/prefix/file.json"], "recurse": True, "groupFiles": 'inPartition', "groupSize": 1048576 }, transformation_ctx="S3bucket_node1",)`  **Note** Use `groupFiles` para agrupar arquivos em um grupo de partições do Amazon S3. Use `groupSize` para	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	definir o tamanho alvo do grupo a ser lido na memória. Especifiq ue `groupSize` em bytes (1048576 = 1 MB).	
Adicione o código ao fluxo de trabalho.	Adicione o código de agrupamento ao seu fluxo de trabalho no AWS Glue.	Engenheiro de dados

Use a lógica personalizada para otimizar a ingestão de ETL

Tarefa	Descrição	Habilidades necessárias
Escolha o idioma e a plataforma de processamento.	Escolha a linguagem de script e a plataforma de processam ento adaptadas ao seu caso de uso.	Arquiteto de nuvem
Escrever o código	Escreva a lógica personali zada para agrupar seus arquivos.	Arquiteto de nuvem
Adicione o código ao fluxo de trabalho.	Adicione o código ao seu fluxo de trabalho no AWS Glue. Isso permite que sua lógica personalizada seja aplicada sempre que a tarefa for executada.	Engenheiro de dados

Repartição ao gravar dados após a transformação

Tarefa	Descrição	Habilidades necessárias
Analise os padrões de consumo.	Descubra como os aplicativos downstream usarão os dados que você grava. Por exemplo, se eles consultam dados todos os dias e você só particiona dados por região ou tem arquivos de saída muito pequenos, como 2,5 KB por arquivo, isso não é ideal para consumo.	DBA
Reparticione os dados antes da gravação.	Repartição com base em junções ou consultas durante o processamento (com base na lógica de processamento) e após o processamento (com base no consumo). Por exemplo, repartição com base no tamanho do byte, como `.repartition(100000)` , ou repartição com base em colunas, como. `.repartition("column_name")`	Engenheiro de dados

Recursos relacionados

- Ler arquivos de entrada em grupos maiores
- Monitoramento do AWS Glue
- Monitoramento do AWS Glue usando CloudWatch métricas da Amazon
- Monitoramento e depuração de trabalho

- Comece a usar o ETL com tecnologia sem servidor no AWS Glue

Mais informações

Determinando o tamanho do arquivo

Não há uma maneira simples de determinar se o tamanho do arquivo é muito grande ou muito pequeno. O impacto do tamanho do arquivo no desempenho do processamento depende da configuração do seu cluster. No núcleo do Hadoop, recomendamos que você use arquivos de 128 MB ou 256 MB para aproveitar ao máximo o tamanho do bloco.

Para a maioria das workloads de arquivos de texto no AWS Glue, recomendamos um tamanho de arquivo entre 100 MB e 1 GB para um cluster de 5 a 10 DPU. Para descobrir o melhor tamanho dos arquivos de entrada, monitore a seção de pré-processamento da sua tarefa do AWS Glue e, em seguida, verifique a utilização da CPU e da memória da tarefa.

Considerações adicionais

Se o desempenho nos estágios iniciais do ETL for um gargalo, considere agrupar ou mesclar os arquivos de dados antes do processamento. Se você tiver controle total sobre o processo de geração de arquivos, pode ser ainda mais eficiente agregar pontos de dados no próprio sistema de origem antes que os dados brutos sejam enviados para a AWS.

Orquestre um pipeline de ETL com validação, transformação e particionamento usando o AWS Step Functions

Criado por Sandip Gangapadhyay (AWS)

Resumo

Esse padrão descreve como criar um pipeline de extração, transformação e carregamento (ETL) com tecnologia sem servidor para validar, transformar, compactar e particionar um grande conjunto de dados CSV para otimizar o desempenho e os custos. O pipeline é orquestrado pelo AWS Step Functions e inclui atributos de repetição automatizados, tratamento de erros e notificação de usuários.

Quando um arquivo CSV é carregado em uma pasta de origem do bucket do Amazon Simple Storage Service (Amazon S3), o pipeline de ETL começa a ser executado. O pipeline valida o conteúdo e o esquema do arquivo CSV de origem, transforma o arquivo CSV em um formato Apache Parquet compactado, particiona o conjunto de dados por ano, mês e dia e o armazena em uma pasta separada para que as ferramentas de análise possam processá-lo.

O código que automatiza esse padrão está disponível no repositório GitHub ETL Pipeline com AWS Step Functions.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- A AWS Command Line Interface (AWS CLI) foi instalada e configurada com sua conta da AWS, para que você possa criar recursos da AWS implantando uma CloudFormation pilha da AWS. A versão 2 da AWS CLI é recomendada. Para obter instruções de instalação, consulte Instalar, atualizar e desinstalar a AWS CLI versão 2 na documentação da AWS CLI. Para obter instruções de configuração da AWS CLI, consulte Configurações do arquivo de Configurações e credenciais na documentação da AWS CLI.
- Um bucket do Amazon S3.
- Um conjunto de dados CSV com o esquema correto. (O repositório de código incluído nesse padrão fornece um arquivo CSV de amostra com o esquema e o tipo de dados corretos que você pode usar.)

- Um navegador da web compatível com o Console de Gerenciamento da AWS. (Consulte a lista de navegadores compatíveis.)
- Acesso ao console do AWS Glue.
- Acesso ao console do AWS Step Functions.

Limitações

- No AWS Step Functions, o limite máximo para manter registros históricos é de 90 dias. Para obter mais informações, consulte Quotas e Quotas para fluxos de trabalho padrão na documentação do AWS Step Functions.

Versões do produto

- Python 3.11 para AWS Lambda
- AWS Glue versão 2.0

Arquitetura

O fluxo de trabalho ilustrado no diagrama consiste nestas etapas de alto nível:

1. O usuário carrega um arquivo CSV na pasta de origem no Amazon S3.
2. Um evento de notificação do Amazon S3 inicia uma função do AWS Lambda que inicia a máquina de estado Step Functions.
3. A função do Lambda valida o esquema e o tipo de dados do arquivo CSV bruto.
4. Dependendo dos resultados da validação:
   a. Se a validação do arquivo de origem for bem-sucedida, o arquivo será movido para a pasta de estágio para processamento adicional.
   b. Se a validação falhar, o arquivo será movido para a pasta de erro e uma notificação de erro será enviada por meio do Amazon Simple Notification Service (Amazon SNS) (Amazon SNS).
5. Um crawler do AWS Glue cria o esquema do arquivo bruto a partir da pasta de estágio no Amazon S3.
6. Um trabalho do AWS Glue transforma, compacta e particiona o arquivo bruto no formato Parquet.
7. O trabalho do AWS Glue também move o arquivo para a pasta de transformação no Amazon S3.

8. O AWS Glue Crawler cria o esquema a partir do arquivo transformado. O esquema resultante pode ser usado por qualquer trabalho de análise. Você pode usar o Amazon Athena para realizar consultas ad-hoc.
9. Se o pipeline for concluído sem erros, o arquivo do esquema será movido para a pasta de arquivamento. Se algum erro for encontrado, o arquivo será movido para a pasta de erros.
10. O Amazon SNS envia uma notificação que indica sucesso ou falha com base no status de conclusão do pipeline.

Todos os recursos da AWS usados nesse padrão têm tecnologia sem servidor. Não há servidores para gerenciar.

Ferramentas

Serviços da AWS

- AWS Glue: o AWS Glue é um serviço de ETL totalmente gerenciado que facilita para os clientes preparar e carregar seus dados para análise.
- AWS Step Functions: o AWS Step Functions é um serviço de orquestração de tecnologia sem servidor que permite combinar funções do AWS Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios. A partir do console gráfico do AWS Step Functions, você vê o fluxo de trabalho do seu aplicativo como uma série de etapas orientadas por eventos.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade líder do setor, disponibilidade de dados, segurança e performance.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço de mensagens pub/sub altamente disponível, durável, seguro e totalmente gerenciado que permite dissociar microsserviços, sistemas distribuídos e aplicativos com tecnologia sem servidor.
- AWS Lambda: o AWS Lambda é um serviço de computação com tecnologia que pode ser usado para executar código sem provisionamento ou gerenciamento de servidores. O AWS Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia a milhares por segundo.

Código

O código desse padrão está disponível no GitHub repositório ETL Pipeline with AWS Step Functions. O repositório de código contém os seguintes arquivos e pastas:

- `template.yml`— CloudFormation Modelo da AWS para criar o pipeline de ETL com o AWS Step Functions.
- `parameter.json`: contém todos os parâmetros e valores de parâmetros. Você atualiza esse arquivo para alterar os valores dos parâmetros, conforme descrito na seção Épicos.
- A pasta `myLayer/python`: contém os pacotes Python necessários para criar a camada necessária do AWS Lambda para esse projeto.
- A pasta `lambda`: contém as seguintes funções do Lambda:
  - `move_file.py`: move o conjunto de dados de origem para a pasta de arquivamento, transformação ou erro.
  - `check_crawler.py`: verifica o status do crawler do AWS Glue quantas vezes for configurado pela variável de ambiente `RETRYLIMIT` , antes de enviar uma mensagem de falha.
  - `start_crawler.py`: inicia o crawler do AWS Glue.
  - `start_step_function.py`: inicia o AWS Step Functions.
  - `start_codebuild.py`— Inicia o CodeBuild projeto da AWS.
  - `validation.py`: valida o conjunto de dados brutos de entrada.
  - `s3object.py`: cria a estrutura de diretórios necessária dentro do bucket do S3.
  - `notification.py`: envia notificações de sucesso ou erro no final do pipeline.

Para usar o código de amostra, siga as instruções na seção Épicos.

Épicos

Preparar os arquivos de origem

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de código de amostra.	1. Abra o pipeline de ETL com o repositório AWS Step Functions. 2. Escolha Código na página principal do repositório, acima da lista de arquivos, e copie o URL listado em Clonar com HTTPS.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	3. Altere seu diretório de trabalho para o local em que você deseja armazenar os arquivos de amostra. 4. Em um terminal ou prompt de comando, digite o comando: `git clone <repoURL>` onde `<repoURL>` se refere ao URL que você copiou na etapa 2.	

Tarefa	Descrição	Habilidades necessárias
Atualizar valores de parâmetro .	Na sua cópia local do repositório, edite o arquivo `parameter.json` e atualize os valores dos parâmetros padrão da seguinte forma: • `pS3BucketName` — O nome do bucket do S3 para armazenar os conjuntos de dados. O modelo criará esse bucket para você. O nome do bucket deve ser exclusivo globalmente. • `pSourceFolder` — O nome da pasta dentro do bucket do S3 que será usada para carregar o arquivo CSV de origem. • `pStageFolder` — O nome da pasta dentro do bucket do S3 que será usada como área de armazenamento durante o processo. • `pTransformFolder` — O nome da pasta dentro do bucket do S3 que será usada para armazenar conjuntos de dados transformados e particion ados. • `pErrorFolder` — A pasta dentro do bucket do S3 para a qual o arquivo CSV de	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	origem será movido se não puder ser validado. • `pArchiveFolder` — O nome da pasta dentro do bucket do S3 que será usada para arquivar o arquivo CSV de origem. • `pEmailforNotification` — Um endereço de e-mail válido para receber notificações de sucesso/erro. • `pPrefix` — Uma string de prefixo que será usada no nome do rastreador do AWS Glue. • `pDatasetSchema` — O esquema do conjunto de dados com o qual o arquivo de origem será validado. O pacote Cerberus Python é usado para validação do conjunto de dados de origem. Para obter mais informações, consulte o site da Cerberus.	

Tarefa	Descrição	Habilidades necessárias
Carregue o código-fonte no bucket do S3.	Antes de implantar o CloudFormation modelo que automatiza o pipeline de ETL, você deve empacotar os arquivos de origem do CloudFormation modelo e carregá-los em um bucket do S3. Para fazer isso, execute o seguinte comando da CLI da AWS com seu perfil pré-confi gurado: `aws cloudformation package --template-file template.yml --s3-bucket <bucket_name> --output-template-file packaged.template --profile <profile_name>` em que: • `<bucket_name>` é o nome de um bucket do S3 existente na região da AWS em que você deseja implantar a pilha. Esse bucket é usado para armazenar o pacote de código-fonte do CloudForm ation modelo. • `<profile_name>` é um perfil válido da AWS CLI	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	que você pré-configurou ao configurar a AWS CLI.	

Crie a pilha.

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	Para implantar o CloudFormation modelo, execute o seguinte comando da AWS CLI: `aws cloudformation deploy --stack-name <stack_name> --template-file packaged.template --parameter-overrides file://parameter.json --capabilities CAPABILITY_IAM --profile <profile_name>` em que: • `<stack_name>` é um identificador exclusivo para a CloudFormation pilha. • `<profile-name>` é o seu perfil pré-configurado da AWS CLI.	Desenvolvedor
Verifique o andamento.	No CloudFormation console da AWS, verifique o progresso do desenvolvimento da pilha. Quando o status for	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`CREATE_COMPLETE` , a pilha foi implantada com sucesso.	
Observe o nome do banco de dados AWS Glue.	A guia Saídas da pilha exibe o nome do banco de dados do AWS Glue. O nome da chave é `GlueDBOutput` .	Desenvolvedor

Teste o pipeline

Tarefa	Descrição	Habilidades necessárias
Inicie o pipeline de ETL.	1. Navegue até a pasta de origem (`source`ou o nome da pasta que você definiu no arquivo `parameter .json`) dentro do bucket do S3. 2. Faça upload de um arquivo CSV de amostra para essa pasta. (O repositório de código fornece um arquivo de amostra chamado `Sample_Bank_Transa ction_Raw_Dataset. csv` que você pode usar.) O upload do arquivo iniciará o pipeline de ETL por meio de Step Functions. 3. No console Step Functions , verifique o status do pipeline de ETL.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Verifique o conjunto de dados particionado.	Quando o pipeline de ETL for concluído, verifique se o conjunto de dados particionado está disponível na pasta de transformação do Amazon S3 (`transform` , ou no nome da pasta que você definiu no arquivo `parameter.json`).	Desenvolvedor
Verifique o banco de dados AWS Glue particionado.	1. No console do AWS Glue, selecione o banco de dados AWS Glue criado pela pilha (esse é o banco de dados que você observou no épico anterior). 2. Verifique se a tabela particionada está disponível no Catálogo de dados do AWS Glue.	Desenvolvedor
Executar consultas.	(Opcional) Use o Amazon Athena para executar consultas ad-hoc no banco de dados particionado e transformado. Para obter instruções, consulte Como executar consultas SQL usando o Amazon Athena na documentação da AWS.	Analista de banco de dados

Solução de problemas

Problema	Solução
Permissões do AWS Identity and Access Management (IAM) para o trabalho e o rastreador do AWS Glue	Se você personalizar ainda mais a tarefa do AWS Glue ou o rastreador, certifique-se de conceder as permissões apropriadas do IAM na função do IAM usada pela tarefa do AWS Glue ou fornecer permissões de dados ao AWS Lake Formation. Para obter mais informações, consulte a documentação da AWS.

Recursos relacionados

Documentação do serviço da AWS

- AWS Step Functions
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SNS

Mais informações

O diagrama a seguir mostra o fluxo de trabalho do AWS Step Functions para um pipeline de ETL bem-sucedido, a partir do painel Step Functions Inspector.

O diagrama a seguir mostra o fluxo de trabalho do AWS Step Functions para um pipeline de ETL que falha devido a um erro de validação de entrada, no painel Step Functions Inspector.

Execute análises avançadas usando o Amazon Redshift ML

Criado por Po Hong (AWS) e Chyanna Antonio (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), você pode usar o machine learning do Amazon Redshift (Amazon Redshift ML) para realizar análises de ML em dados armazenados em um cluster do Amazon Redshift ou no Amazon Simple Storage Service (Amazon S3). O Amazon Redshift ML oferece suporte ao aprendizado supervisionado, que normalmente é usado para análises avançadas. Os casos de uso do Amazon Redshift ML incluem previsão de receita, detecção de fraudes em cartões de crédito e valor da vida útil do cliente (CLV, Customer Lifetime Value) ou previsões de rotatividade de clientes.

O Amazon Redshift ML facilita a criação, o treinamento e a implantação de modelos de Machine Learning usando comandos SQL padrões. O Amazon Redshift ML usa o Amazon SageMaker Autopilot para treinar e ajustar automaticamente os melhores modelos de ML para classificação ou regressão com base em seus dados, enquanto você mantém o controle e a visibilidade.

Todas as interações entre o Amazon Redshift, o Amazon S3 e a SageMaker Amazon são abstraídas e automatizadas. Depois que o modelo de ML é treinado e implantado, ele fica disponível como uma função definida pelo usuário (UDF) no Amazon Redshift e pode ser usado em consultas SQL.

Esse padrão complementa o tutorial Criar, treinar e implantar modelos de ML no Amazon Redshift usando SQL com Amazon Redshift ML do blog da AWS e o tutorial Criar, treinar e implantar um modelo de ML com a SageMaker Amazon do Getting Started Resource Center.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Dados existentes em uma tabela do Amazon Redshift

Habilidades

- Familiaridade com termos e conceitos usados pelo Amazon Redshift ML, incluindo machine learning , treinamento, e previsão. Para obter mais informações sobre isso, consulte Modelos de treinamento de ML na documentação do Amazon Machine Learning (Amazon ML).

- Experiência com configuração de usuários, gerenciamento de acesso e sintaxe SQL padrão do Amazon Redshift. Para obter mais informações sobre isso, consulte Conceitos básicos do Amazon Redshift na documentação do Amazon Redshift.
- Conhecimento e experiência com o Amazon S3 e o AWS Identity and Access Management (IAM).
- A experiência na execução de comandos na AWS Command Line Interface (AWS CLI) também é vantajosa, mas não obrigatória.

Limitações

- O cluster do Amazon Redshift e o bucket do Amazon S3 devem estar na mesma região da Região da AWS.
- A abordagem desse padrão oferece suporte apenas a modelos de aprendizado supervisionado, como regressão, classificação binária e classificação multiclasse.

Arquitetura

As etapas a seguir explicam como o Amazon Redshift ML funciona SageMaker para criar, treinar e implantar um modelo de ML:

1. O Amazon Redshift exporta dados de treinamento para um bucket do S3.
2. SageMaker O piloto automático pré-processa automaticamente os dados de treinamento.
3. Depois que a `CREATE MODEL` declaração é invocada, o Amazon Redshift ML SageMaker usa para treinamento.
4. SageMaker O Autopilot pesquisa e recomenda o algoritmo de ML e os hiperparâmetros ideais que otimizam as métricas de avaliação.
5. O Amazon Redshift ML registra a função de previsão como uma função SQL no cluster do Amazon Redshift.
6. A função do modelo de ML pode ser usada em uma instrução do SQL.

Pilha de tecnologia

- Amazon Redshift
- SageMaker

- Amazon S3

Ferramentas

- Amazon Redshift: o Amazon Redshift é um serviço de data warehousing em escala de petabytes e em nível empresarial totalmente gerenciado.
- Amazon Redshift ML: o Amazon Redshift Machine Learning (Amazon Redshift ML) é um serviço robusto baseado em nuvem que ajuda analistas e cientistas de dados de todos os níveis de qualificação a usarem a tecnologia de Machine Learning.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet.
- Amazon SageMaker — SageMaker é um serviço de ML totalmente gerenciado.
- Amazon SageMaker Autopilot — O SageMaker Autopilot é um conjunto de recursos que automatiza as principais tarefas de um processo automático de aprendizado de máquina (AutoML).

Código

Você pode criar um modelo de ML supervisionado no Amazon Redshift usando o seguinte código:

```
“CREATE MODEL customer_churn_auto_model
FROM (SELECT state,
             account_length,
             area_code,
             total_charge/account_length AS average_daily_spend,
             cust_serv_calls/account_length AS average_daily_cases,
             churn
      FROM customer_activity
      WHERE  record_date < '2020-01-01'
     )
TARGET churn
FUNCTION ml_fn_customer_churn_auto
IAM_ROLE 'arn:aws:iam::XXXXXXXXXXXX:role/Redshift-ML'
SETTINGS (
  S3_BUCKET 'your-bucket'
);”)
```

> **Note**
>
> O `SELECT` estado pode se referir às tabelas regulares do Amazon Redshift, às tabelas externas do Amazon Redshift Spectrum ou a ambas.

Épicos

Prepare um conjunto de dados de treinamento e teste

Tarefa	Descrição	Habilidades necessárias
Prepare um conjunto de dados de treinamento e teste.	Faça login no AWS Management Console e abra o SageMaker console da Amazon. Siga as instruções do tutorial Criar, treinar e implantar um modelo de machine learning para criar um arquivo.csv ou Apache Parquet que tenha uma coluna de rótulo(treinamento supervisionado) e nenhum cabeçalho. **Note** Recomendamos que você misture e divida o conjunto de dados brutos em um conjunto de treinamento para o treinamento do modelo (70 por cento) e um conjunto de testes para a avaliação	Cientista de dados

Tarefa	Descrição	Habilidades necessárias
	de desempenho do modelo (30 por cento).	

Prepare e configure a pilha de tecnologia

Tarefa	Descrição	Habilidades necessárias
Crie e configure um cluster do Amazon Redshift.	No console do Amazon Redshift, crie um cluster de acordo com os requisitos. Para obter mais informações sobre isso, consulte Criar um cluster na documentação do Amazon Redshift. **Important** Os clusters do Amazon Redshift devem ser criados com a trilha de `SQL_PREVIEW` manutenção. Para obter mais informaçõ es, consulte Escolher trilhas de manutençã o do cluster na documentação do Amazon Redshift.	DBA, Arquiteto de nuvem
Crie um bucket do S3 para armazenar dados de	No console do Amazon S3, crie um bucket do S3 para os dados de treinamento e teste.	DBA, Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
treinamento e artefatos do modelo.	Para obter mais informações sobre como criar um bucket do S3, consulte Criar um bucket do Amazon S3 do Início rápido do AWS. **⚠ Important** Certifique-se de que o cluster do Amazon Redshift e o bucket do S3 estejam na mesma região.	
Crie e anexe uma política do IAM ao cluster do Amazon Redshift.	Crie uma política do IAM para permitir que o cluster do Amazon Redshift acesse SageMaker o Amazon S3. Para obter instruções e etapas, consulte Configuração de cluster para usar o Amazon Redshift ML na documentação do Amazon Redshift.	DBA, Arquiteto de nuvem
Permita que usuários e grupos do Amazon Redshift acessem esquemas e tabelas.	Conceda permissões para permitir que usuários e grupos no Amazon Redshift acessem esquemas e tabelas internos e externos. Para ver as etapas e instruções, consulte Gerenciamento de permissões e propriedade na documentação do Amazon Redshift.	DBA

Crie e treine o modelo de ML no Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Crie e treine o modelo de ML no Amazon Redshift.	Crie e treine seu modelo de ML no Amazon Redshift ML. Para obter mais informações, consulte a declaração `CREATE MODEL` na documentação do Amazon Redshift.	Desenvolvedor, Cientista de dados

Execute inferência e previsão em lote no Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Faça inferência usando a função de modelo de ML gerada.	Para obter mais informações sobre como realizar inferências usando a função de modelo de ML gerada, consulte Previsões na documentação do Amazon Redshift.	Cientista de dados, usuário de inteligência de negócios

Recursos relacionados

Prepare um conjunto de dados de treinamento e teste

- Construindo, treinando e implantando um modelo de aprendizado de máquina com a Amazon SageMaker

Prepare e configure a pilha de tecnologia

- Criar um cluster do Amazon Redshift
- Escolhendo faixas de manutenção de clusters do Amazon Redshift
- Criar um bucket do S3
- Configurar um cluster do Amazon Redshift para o Amazon Redshift ML

- Gerenciamento de permissões e propriedade no Amazon Redshift

Crie e treine o modelo de ML no Amazon Redshift

- Declaração CRIAR MODELO no Amazon Redshift

Execute inferência e previsão em lote no Amazon Redshift

- Previsão no Amazon Redshift

Outros recursos

- Conceitos básicos do Amazon Redshift ML
- Criação, treinamento e implantação de modelos de ML no Amazon Redshift usando SQL com o Amazon Redshift ML
- Parâmetros do Amazon Redshift
- Parceiros de competência em machine learning da AWS

Consulte tabelas do Amazon DynamoDB com SQL usando o Amazon Athena

Criado por Gavin Perrie (AWS), Ajit Ambike (AWS) e Brad Yates (AWS)

Resumo

Se seus dados incluírem fontes diferentes do Amazon Simple Storage Service (Amazon S3), você poderá usar consultas federadas para acessar essas fontes de dados relacionais, não relacionais, de objetos ou personalizadas. Esse padrão mostra como configurar o acesso de consultas federadas por meio do Amazon Athena ao Amazon DynamoDB usando um conector de fonte de dados SQL.

Usando esse padrão, você pode fazer o seguinte:

- Consulte tabelas do DynamoDB usando SQL.
- Execute consultas SQL federadas no Athena e junte tabelas do DynamoDB a outras fontes de dados compatíveis.

Pré-requisitos e limitações

Pré-requisitos

- Uma tabela do DynamoDB.
- Um grupo de trabalho do Athena configurado para usar o motor Athena versão 2. Para obter instruções, consulte a documentação do Athena.
- Um bucket do S3 em que a `AthenaDynamoDBConnector` AWS Lambda função pode divulgar os dados. O bucket do S3 e a função Lambda devem estar na mesma região da AWS.

Se for a primeira vez que você acessa o Athena, você precisará de um bucket S3 adicional para usar como local do resultado da consulta. Para obter instruções, consulte a documentação do Athena.

Limitações

- Operações de gravação como INSERT INTO não são suportadas.

Versões do produto

- Athena Query Federation é lançado em GitHub

Arquitetura

Arquitetura de destino

O diagrama a seguir mostra o fluxo de conexão após o padrão ser estabelecido. O usuário se conecta ao Amazon Athena para fornecer a consulta. O Athena passa a consulta e o destino para a função Lambda do conector de fonte de dados do DynamoDB, que recupera e retorna os dados para o Athena. Se grandes quantidades de dados forem retornadas, o Athena armazena os resultados temporários no balde de derramamento antes de empacotar e devolver o conjunto de dados completo.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que ajuda a análise de dados diretamente no Amazon Simple Storage Service (Amazon S3) usando SQL padrão. Esse padrão usa o Amazon Athena DynamoDB Connector, uma ferramenta criada usando o Amazon Athena Query Federation SDK e instalada como um aplicativo por meio do. AWS Lambda AWS Serverless Application Repository
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Repositório de código

O código desse padrão está disponível no repositório da GitHub Athena Query Federation.

Épicos

Configurar e testar o conector da fonte de dados do DynamoDB

Tarefa	Descrição	Habilidades necessárias
Implante o AthenaDynamoDBConnector aplicativo.	Para implantar AthenaDynamoDBConnecter, faça o seguinte: 1. Faça login no e escolha o AWS Management Console Região da AWS que você está usando para a tabela do DynamoDB e o balde de derramamento. 2. Abra o Serverless Application Repository em. https://console.aws.amazon.com/serverlessrepo/ 3. No painel de navegação, escolha Aplicativos disponíveis. 4. Para acesso AWS Identity and Access Management (IAM), na barra de pesquisa, marque a caixa de seleção Mostrar aplicativos que criam funções personalizadas do IAM ou políticas de recursos. 5. Pesquise AthenaDynamoDBConnector, selecione e certifique-se de que o autor listado seja a Amazon Athena Federation.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	6. Em Configurações do aplicativo, insira os seguintes valores: • SpillBucket– Local para o qual a função pode transferir dados. • AthenaCatalogName– O nome da função Lambda que será criada. O nome também será usado como o nome da fonte de dados no Athena. 7. Marque a caixa de seleção para reconhecer a criação de funções e políticas do IAM. 8. Escolha Implantar.	

Tarefa	Descrição	Habilidades necessárias
Crie uma fonte de dados para Athena.	Para criar a fonte de dados, faça o seguinte: 1. Abra o console Athena em https://console.aws.amazon.com/athena/. 2. Expanda o painel de navegação e escolha Fontes de dados. 3. Escolha Criar fonte de dados. 4. Escolha Amazon DynamoDB. 5. Insira o nome da fonte de dados. 6. Selecione a função Lambda que você criou. 7. Revise os detalhes e escolha Criar fonte de dados.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Use o Athena para consultar a tabela do DynamoDB.	Para consultar a tabela do DynamoDB, faça o seguinte: 1. No console do Athena, expanda o painel de navegação e escolha Editor de consultas. 2. Na lista suspensa Fonte de dados, escolha a fonte de dados que você criou. 3. Confirme se as tabelas do DynamoDB estão listadas em Tabelas. 4. Executar a consulta.	Desenvolvedor de aplicativos

Solução de problemas

Problema	Solução
A consulta falha com `GENERIC_INTERNAL_ERROR: The bucket is in this region: <region>`.	Certifique-se de que o balde de derramamento do Athena e a função Lambda sejam criados no mesmo. Região da AWS
A fonte de dados recém-criada não está visível no console do Athena.	Os catálogos de dados do Athena são regionais. Verifique `AthenaDynamoDBConnector` se o foi implantado na região em que você está tentando usar o Athena.
Você não consegue executar a consulta na fonte de dados recém-criada.	Verifique se o local do resultado da consulta foi definido.

Recursos relacionados

- Conector Amazon Athena DynamoDB
- Consulta federada do Amazon Athena

Acesse, consulte e una tabelas do Amazon DynamoDB usando o Athena

Criado por Moinul Al-Mamun (AWS)

Resumo

Este padrão mostra como configurar uma conexão entre o Amazon Athena e o Amazon DynamoDB usando o conector Amazon Athena DynamoDB. O conector usa uma função do AWS Lambda para consultar os dados no DynamoDB. Não é necessário escrever nenhum código para configurar a conexão. Depois que a conexão for estabelecida, você poderá acessar e analisar rapidamente as tabelas do DynamoDB usando o Athena Federated Query para executar comandos SQL do Athena. Você também pode unir uma ou mais tabelas do DynamoDB entre si ou com outras fontes de dados, como Amazon Redshift ou Amazon Aurora.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa AWS com permissões para gerenciar tabelas do DynamoDB, fontes de dados do Athena, Lambda e perfis do AWS Identity and Access Management (IAM)
- Um bucket do Amazon Simple Storage Service (Amazon S3) no qual o Athena poderá armazenar resultados de consultas
- Um bucket do S3 em que o Athena DynamoDB Connector pode salvar os dados no curto prazo
- Uma região da AWS que fornece suporte à versão 2 do mecanismo Athena
- Permissões do IAM para acessar o Athena e os buckets do S3 necessários
- Conector do DynamoDB no Amazon Athena, instalado

Limitações

Há um custo para consultar tabelas do DynamoDB. Tamanhos de tabela superiores a alguns gigabytes (GBs) podem gerar um alto custo. Recomendamos que você considere o custo antes de realizar qualquer operação de VERIFICAÇÃO de tabela completa. Para obter mais informações, consulte a Definição de preço do Amazon DynamoDB. Para reduzir custos e alcançar alto desempenho, recomendamos que você sempre use LIMIT em sua consulta (por exemplo, `SELECT * FROM table1 LIMIT 10`). Além disso, antes de realizar uma consulta JOIN ou GROUP BY em um

ambiente de produção, considere o tamanho de suas tabelas. Se suas tabelas forem muito grandes, considere opções alternativas, como migrar a tabela para o Amazon S3.

Arquitetura

O diagrama a seguir mostra como um usuário pode executar uma consulta SQL em uma tabela do DynamoDB do Athena.

O diagrama mostra o seguinte fluxo de trabalho:

1. Para consultar uma tabela do DynamoDB, um usuário executa uma consulta SQL do Athena.
2. O Athena inicia uma função do Lambda.
3. A função do Lambda consulta os dados solicitados na tabela do DynamoDB.
4. O DynamoDB retorna os dados solicitados para a função do Lambda. Em seguida, a função transfere os resultados da consulta para o usuário por meio do Athena.
5. A função do Lambda armazena dados no bucket do S3.

Pilha de tecnologia

- Amazon Athena
- Amazon DynamoDB
- Amazon S3
- AWS Lambda

Ferramentas

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão.
- O Amazon Athena DynamoDB Connector é uma ferramenta da AWS que permite que o Athena se conecte ao DynamoDB e acesse suas tabelas usando consultas SQL.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando

necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Épicos

Criar exemplos de tabelas do DynamoDB

Tarefa	Descrição	Habilidades necessárias
Crie a primeira tabela de exemplo.	1. Faça login no Console de Gerenciamento da AWS e abra o console do DynamoDB. 2. Escolha Create table. 3. Em Nome da tabela, insira dydbtable1. 4. Em Chave de partição, digite PK1. 5. Em Chave de classificação, insira SK1. 6. Na seção Configurações da tabela, selecione Personalizar configurações. 7. Na seção Classe de tabela, escolha DynamoDB Standard. 8. Na seção Configurações de capacidade de leitura/gravação, para Modo de capacidade, escolha Sob demanda. 9. Na seção Criptografia em repouso, escolha Propriedade do Amazon DynamoDB.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	10 Escolha Create table.	

Insira dados de exemplo na primeira tabela.	1. Abra o console do DynamoDB.
	2. No painel de navegação, selecione Tabela e selecione sua tabela na coluna Nome.
	3. Escolha Ações e, em seguida, Criar item.
	4. Escolha Visualização JSON.
	5. Na barra de título do editor Attributes, desative Visualizar DynamoDB JSON.
	6. No editor Atributos, insira os seguintes dados de exemplo, um por um:
	
	`{ "PK1": "1234", "SK1": "info", "Salary": "5000" }`
	
	`{ "PK1": "1235", "SK1": "info", "Salary": "5200" }`
		Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Crie a segunda tabela de exemplo.	1. Abra o console do DynamoDB. 2. Escolha Create table. 3. Em Nome da tabela, insira dydbtable2. 4. Em Partition key, (Chave de partição), insira PK2. 5. Em Chave de classificação, insira SK2. 6. Na seção Configurações da tabela, selecione Personalizar configurações. 7. Na seção Classe de tabela, escolha DynamoDB Standard. 8. Na seção Configurações de capacidade de leitura/gravação, para Modo de capacidade, escolha Sob demanda. 9. Na seção Criptografia em repouso, escolha Propriedade do Amazon DynamoDB. 10. Escolha Create table.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias

Insira dados de exemplo na segunda tabela.	1. Abra o console do DynamoDB.
	2. No painel de navegação, selecione Tabela e selecione sua tabela na coluna Nome.
	3. Escolha Ações e, em seguida, Criar item.
	4. Na barra de título do editor Attributes, desative Visualizar DynamoDB JSON.
	5. No editor Atributos, insira os seguintes dados de exemplo, um por um:
	
	`{ "PK2": "1234", "SK2": "bonus", "Bonus": "500" }`
	
	`{ "PK2": "1235", "SK2": "bonus", "Bonus": "1000" }`
		Desenvolvedor

Crie uma fonte de dados no Athena para DynamoDB

Tarefa	Descrição	Habilidades necessárias
Configure o conector da fonte de dados.	Crie uma fonte de dados para o DynamoDB e, em seguida, uma função do Lambda para se conectar a essa fonte de dados. 1. Faça login no Console de Gerenciamento da AWS e abra o console do Athena. 2. No painel de navegação, escolha Fontes de dados e, em seguida, Criar fonte de dados. 3. Escolha a fonte de dados do Amazon DynamoDB e, em seguida, Avançar. 4. Na seção Detalhes da fonte de dados, em Nome da fonte de dados, insira testDynamoDB. 5. Na seção Detalhes da conexão, selecione uma função do Lambda que já esteja implantada ou escolha Criar função do Lambda se você não tiver uma função do Lambda para usar nesse padrão. Observação: Para obter mais informações sobre como criar uma função do Lambda, consulte	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Conceitos básicos do AWS Lambda no Guia do desenvolvedor do Lambda. 6. (Opcional) Se você escolher a função Create Lambda, deverá configurar o CloudFormation modelo da AWS incluído pelo aplicativo Java antes de implantar essa pilha. O modelo inclui ApplicationName, SpillBucket AthenaCatalogName, e outras configurações do aplicativo. Observação: depois de implantar esse aplicativo baseado em Java, a pilha cria uma função do Lambda que permite que o Athena se comunique com o DynamoDB. Isso torna suas tabelas acessíveis por meio de comandos SQL. 7. Implantação da função do Lambda. 8. Escolha Próximo.	

Tarefa	Descrição	Habilidades necessárias
Verifique se a função do Lambda pode acessar o bucket de vazamento do S3.	1. Abra o console do lambda. 2. No painel de navegação, escolha Funções e, em seguida, escolha a função que você criou anteriormente. 3. Escolha a guia Configuração. 4. No painel esquerdo, escolha Variáveis de ambiente e confirme se o valor da chave é `spill_bucket` . 5. No painel esquerdo, escolha Permissões e, na seção Perfil de execução, escolha o perfil do IAM anexo. Observação: você é direcionado para o perfil do IAM anexo à sua função do Lambda no console do IAM. 6. Confirme se você tem permissão de gravação no bucket `spill_bucket` . Se ocorrerem erros, consulte a seção Informações adicionais neste padrão para obter orientação.	Desenvolvedor

Acessar tabelas do DynamoDB a partir do Athena

Tarefa	Descrição	Habilidades necessárias
Consultar as tabelas do DynamoDB.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Athena. 2. No painel de navegação, escolha Fontes de dados e, em seguida, Criar fonte de dados. 3. No painel de navegação , selecione Editor de consultas. 4. Na guia Editor, na seção Dados, em Fonte de dados, escolha sua fonte de dados em Fonte de dados. 5. Em Banco de dados, escolha seu banco de dados. 6. Para Consulta 1, insira a seguinte consulta: `SELECT * FROM dydbtable1 t1;` 7. Escolha Executar e, em seguida, verifique o resultado na tabela. 8. Para Consulta 2, insira a seguinte consulta: `SELECT * FROM dydbtable2 t2;` 9. Escolha Executar e, em seguida, verifique o resultado na tabela.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Unir duas tabelas do DynamoDB.	O DynamoDB é um armazenamento de dados NoSQL e não fornece suporte à operação de junção de SQL. Consequentemente, você deve realizar uma operação de junção em duas tabelas do DynamoDB: 1. Selecione o ícone de adição para criar uma nova consulta. 2. Para Consulta 3, insira a seguinte consulta: `SELECT pk1, salary, bonus FROM dydbtable1 t1 JOIN dydbtable2 t2 ON t1.pk1 = t2.pk2;`	Desenvolvedor

Recursos relacionados

- Conector do Amazon Athena para o DynamoDB (AWS Labs)
- Consulte qualquer fonte de dados com a nova consulta federada do Amazon Athena (blog do AWS Big Data)
- Referência da versão do mecanismo Athena (Guia do usuário do Athena)
- Simplifique a extração e a análise de dados do Amazon DynamoDB usando o AWS Glue e o Amazon Athena (blog do banco de dados da AWS)

Mais informações

Se você executar uma consulta no Athena com `spill_bucket` no formato `{bucket_name}/folder_name/`, poderá receber a seguinte mensagem de erro:

```
"GENERIC_USER_ERROR: Encountered an exception[java.lang.RuntimeException] from your
 LambdaFunction[arn:aws:lambda:us-east-1:xxxxxx:function:testdynamodb] executed in
 context[retrieving meta-data] with message[You do NOT own the spill bucket with the
 name: s3://amzn-s3-demo-bucket/athena_dynamodb_spill_data/]
This query ran against the "default" database, unless qualified by the query. Please
 post the error message on our forum  or contact customer support with Query Id:
 [query-id]"
```

Para solucionar esse erro, atualize a variável de ambiente da função do Lambda `spill_bucket` para `{bucket_name_only}` e, em seguida, atualize a seguinte política do IAM do Lambda para obter acesso de gravação no bucket:

```
{
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::spill_bucket",
                "arn:aws:s3:::spill_bucket/*"
            ],
            "Effect": "Allow"
        }
```

Como alternativa, você pode remover o conector da fonte de dados do Athena criado anteriormente e recriá-lo usando somente `{bucket_name}` para `spill_bucket`.

Configure um espaço de dados mínimo viável para compartilhar dados entre organizações

Criado por Ramy Hcini (Think-it), Ismail Abdellaoui (Think-it), Malte Gasseling (Think-it), Jorge Hernandez Suarez (AWS) e Michael Miller (AWS)

Resumo

Os espaços de dados são redes federadas para troca de dados com confiança e controle sobre os dados como princípios fundamentais. Eles permitem que as organizações compartilhem, troquem e colaborem em dados em grande escala, oferecendo uma solução econômica e independente de tecnologia.

Os espaços de dados têm o potencial de impulsionar significativamente os esforços para um futuro sustentável usando a solução de problemas baseada em dados com uma end-to-end abordagem que envolve todas as partes interessadas relevantes.

Esse padrão orienta você pelo exemplo de como duas empresas podem usar a tecnologia de espaço de dados na Amazon Web Services (AWS) para impulsionar sua estratégia de redução de emissões de carbono. Nesse cenário, a empresa X fornece dados de emissões de carbono, que a empresa Y consome. Consulte a seção Informações adicionais para obter os seguintes detalhes da especificação do espaço de dados:

- Participantes
- Caso de negócios
- Autoridade de espaço de dados
- Componentes do espaço de dados
- Serviços de espaço de dados
- Dados a serem trocados
- Modelo de dados
- Conector Tractus-X EDC

O padrão inclui etapas para o seguinte:

- Implantação da infraestrutura necessária para um espaço de dados básico com dois participantes em AWS execução.

- Trocando dados de emissões de carbono– intensidade usando os conectores de forma segura.

Esse padrão implanta um cluster Kubernetes que hospedará conectores de espaço de dados e seus serviços por meio do Amazon Elastic Kubernetes Service (Amazon EKS).

O plano de controle e o plano de dados do Eclipse Dataspace Components (EDC) são ambos implantados no Amazon EKS. O gráfico oficial do Tractus-X Helm implanta os serviços PostgreSQL e Vault como dependências. HashiCorp

Além disso, o serviço de identidade é implantado no Amazon Elastic Compute Cloud EC2 (Amazon) para replicar um cenário real de um espaço de dados mínimo viável (MVDS).

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS para implantar a infraestrutura de sua escolha Região da AWS
- Um usuário AWS Identity and Access Management (IAM) com acesso ao Amazon S3 que será usado temporariamente como usuário técnico (o conector EDC atualmente não suporta o uso de funções). Recomendamos que você crie um usuário do IAM especificamente para essa demonstração e que esse usuário tenha permissões limitadas associadas a ela.)
- AWS Command Line Interface (AWS CLI) instalado e configurado em sua escolha Região da AWS
- AWS credenciais de segurança
- eksctl em sua estação de trabalho
- Git na sua estação de trabalho
- kubectl
- Helm
- Carteiro
- Um certificado SSL/TLS AWS Certificate Manager (ACM)
- Um nome DNS que apontará para um Application Load Balancer (o nome DNS deve estar coberto pelo certificado ACM)
- HashiCorp Vault (Para obter informações sobre como usar AWS Secrets Manager para gerenciar segredos, consulte a seção Informações adicionais.)

Versões do produto

- AWS CLI versão 2+
- Coleção Postman v2.1

Limitações

- Seleção de conectores – Essa implantação usa um conector baseado em EDC. No entanto, certifique-se de considerar os pontos fortes e as funcionalidades dos conectores EDC e FIWARE True para tomar uma decisão informada que se alinhe às necessidades específicas da implantação.
- Construção do conector EDC – A solução de implantação escolhida se baseia no gráfico Tractus-X EDC Connector Helm, uma opção de implantação bem estabelecida e amplamente testada. A decisão de usar esse gráfico é motivada por seu uso comum e pela inclusão de extensões essenciais na compilação fornecida. Embora o PostgreSQL HashiCorp e o Vault sejam componentes padrão, você tem a flexibilidade de personalizar sua própria construção de conectores, se necessário.
- Acesso ao cluster privado – O acesso ao cluster EKS implantado é restrito aos canais privados. A interação com o cluster é realizada exclusivamente por meio do uso `kubectl` de um IAM. O acesso público aos recursos do cluster pode ser habilitado usando balanceadores de carga e nomes de domínio, que devem ser implementados seletivamente para expor serviços específicos a uma rede mais ampla. No entanto, não recomendamos fornecer acesso público.
- Foco na segurança – A ênfase é colocada na abstração das configurações de segurança de acordo com as especificações padrão para que você possa se concentrar nas etapas envolvidas na troca de dados do conector EDC. Embora as configurações de segurança padrão sejam mantidas, é fundamental habilitar comunicações seguras antes de expor o cluster à rede pública. Essa precaução garante uma base sólida para o manuseio seguro de dados.
- Custo da infraestrutura – Uma estimativa do custo da infraestrutura pode ser encontrada usando o. AWS Calculadora de Preços Um cálculo simples mostra que os custos podem chegar a 162,92 USD por mês para a infraestrutura implantada.

Arquitetura

A arquitetura MVDS compreende duas nuvens privadas virtuais (VPCs), uma para o serviço de identidade Dynamic Attribute Provisioning System (DAPS) e outra para o Amazon EKS.

Arquitetura DAPS

O diagrama a seguir mostra o DAPS em execução em EC2 instâncias controladas por um grupo de Auto Scaling. Um Application Load Balancer e uma tabela de rotas expõem os servidores DAPS. O Amazon Elastic File System (Amazon EFS) sincroniza os dados entre as instâncias do DAPS.

Arquitetura Amazon EKS

Os espaços de dados são projetados para serem soluções independentes de tecnologia, e existem várias implementações. Esse padrão usa um cluster Amazon EKS para implantar os componentes técnicos do espaço de dados. O diagrama a seguir mostra a implantação do cluster EKS. Os nós de trabalho são instalados em sub-redes privadas. Os pods do Kubernetes acessam a instância Amazon Relational Database Service (Amazon RDS) para PostgreSQL, que também está nas sub-redes privadas. Os pods do Kubernetes armazenam dados compartilhados no Amazon S3.

Ferramentas

AWS serviços

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre EC2 instâncias, contêineres e endereços IP em uma ou mais zonas de disponibilidade.

Outras ferramentas

- O eksctl é utilitário de linha de comando para criar e gerenciar clusters do Kubernetes no Amazon EKS.
- O Git é um sistema de controle de versão distribuído e de código aberto.
- HashiCorp O Vault fornece armazenamento seguro com acesso controlado para credenciais e outras informações confidenciais.
- O Helm é um gerenciador de pacotes de código aberto para Kubernetes que ajuda você a instalar e gerenciar aplicativos em seu cluster Kubernetes.
- kubectl é uma interface de linha de comando que ajuda você na execução de comandos em clusters do Kubernetes.
- O Postman é uma plataforma de API.

Repositório de código

Os arquivos YAML de configuração do Kubernetes e os scripts Python para esse padrão estão disponíveis no repositório. GitHub aws-patterns-edc O padrão também usa o repositório Tractus-X EDC.

Práticas recomendadas

Amazon EKS e isolamento das infraestruturas dos participantes

Os namespaces no Kubernetes separarão a infraestrutura do provedor da empresa X da infraestrutura do consumidor da empresa Y nesse padrão. Para obter mais informações, consulte os guias de melhores práticas do EKS.

Em uma situação mais realista, cada participante teria um cluster Kubernetes separado rodando dentro do seu próprio cluster. Conta da AWS A infraestrutura compartilhada (DAPS nesse padrão) seria acessível pelos participantes do espaço de dados e estaria completamente separada das infraestruturas dos participantes.

Épicos

Configure o ambiente e provisione um cluster e EC2 instâncias do EKS

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositório na sua estação de trabalho, execute o seguinte comando: `git clone https://github.com/Think-iT-Labs/aws-patterns-edc` A estação de trabalho deve ter acesso ao seu Conta da AWS.	DevOps engenheiro
Provisione o cluster Kubernetes e configure namespaces.	Para implantar um cluster EKS padrão simplificado em sua conta, execute o seguinte `eksctl` comando na estação de trabalho em que você clonou o repositório: `eksctl create cluster` O comando cria a VPC e as sub-redes públicas e privadas que abrangem três zonas de disponibilidade diferentes. Depois que a camada de rede é criada, o comando cria duas `m5.large` EC2 instâncias dentro de um grupo de Auto Scaling.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	Para obter mais informaçõ es e exemplos de resultados, consulte o guia eksctl.
	
	Depois de provisionar o cluster privado, adicione o novo cluster EKS à sua configuração local do Kubernetes executando o seguinte comando:
	
	`aws eks update-ku beconfig --name <EKS CLUSTER NAME> --region <AWS REGION>`
	
	Esse padrão usa o `eu-west-1` Região da AWS para executar todos os comandos. No entanto, você pode executar os mesmos comandos de sua preferência Região da AWS.
	
	Para confirmar se seus nós EKS estão em execução e prontos, execute o seguinte comando:
	
	`kubectl get nodes`	

Tarefa	Descrição	Habilidades necessárias

Configure os namespaces.	Para criar namespaces para o provedor e o consumidor, execute os seguintes comandos:
	`kubectl create ns provider`
	`kubectl create ns consumer`
	Nesse padrão, é importante usar `provider` e `consumer` como namespaces para ajustar as configurações nas próximas etapas.
		DevOps engenheiro

Implantar o serviço de identidade

Tarefa	Descrição	Habilidades necessárias
Implante o DAPS usando AWS CloudFormation.	Para facilitar o gerenciamento das operações do DAPS, o servidor DAPS é instalado nas EC2 instâncias. Para instalar o DAPS, use o AWS CloudFormation modelo. Você precisará do certificado do ACM e do nome DNS na seção Pré-requisitos. O modelo implanta e configura o seguinte: • Application Load Balancer	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• Auto Scaling group (Grupo do Auto Scaling) • EC2 instâncias configuradas com dados do usuário para instalar todos os pacotes necessários • Perfis do IAM • TAPINHAS Você pode implantar o AWS CloudFormation modelo fazendo login AWS Management Console e usando o AWS CloudFormation console. Você também pode implantar o modelo usando um AWS CLI comando como o seguinte: `aws cloudformation create-stack --stack-name daps \ --template-body file://aws-patterns-edc/cloudformation.yml --parameters \ ParameterKey=CertificateARN,ParameterValue=<ACM Certificate ARN> \ ParameterKey=DNSName,ParameterValue=<DNS name> \ ParameterKey=InstanceType,ParameterValue=<EC2 instance type> \`	

Tarefa	Descrição	Habilidades necessárias
	`ParameterKey=Environmentname,ParameterValue=<Environment Name> --capabilities CAPABILITY_NAMED_IAM` O nome do ambiente é de sua própria escolha. Recomendamos usar um termo significativo, como `DapsInfrastructure`, porque ele será refletido nas tags AWS de recursos. Para esse padrão, `t3.small` é grande o suficiente para executar o fluxo de trabalho DAPS, que tem três contêineres Docker. O modelo implanta as EC2 instâncias em sub-redes privadas. Isso significa que as instâncias não podem ser acessadas diretamente por meio de SSH (Secure Shell) pela Internet. As instâncias são provisionadas com a função e o AWS Systems Manager agente do IAM necessários para permitir o acesso às instâncias em execução por meio do Gerenciador de sessões, um	

Tarefa	Descrição	Habilidades necessárias

	recurso de. AWS Systems Manager
	
	Recomendamos usar o Gerenciador de Sessões para acesso. Como alternativa, você pode provisionar um bastion host para permitir o acesso SSH da Internet. Ao usar a abordagem bastion host, a EC2 instância pode levar mais alguns minutos para começar a ser executada .
	
	Depois que o AWS CloudFormation modelo for implantado com sucesso, aponte o nome DNS para o nome DNS do Application Load Balancer. Para confirmar, execute o seguinte comando:
	
	`dig <DNS NAME>`
	
	A saída deve ser semelhante ao seguinte:
	
	`; <<>> DiG 9.16.1-Ubuntu <<>> edc-pattern.think-it.io`
	`;; global options: +cmd`
	`;; Got answer:`
	`;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42344`	

Tarefa	Descrição	Habilidades necessárias
	;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ;; QUESTION SECTION: ;edc-pattern.think- it.io. IN A ;; ANSWER SECTION: edc-pattern.think- it.io. 276 IN CNAME daps- alb-iap9zmwy3kn8-13287 73120.eu-west-1.el b.amazonaws.com. daps-alb-iap9zmwy3k n8-1328773120.eu-w est-1.elb.amazonaw s.com. 36 IN A 52.208.240.129 daps-alb-iap9zmwy3kn8 -1328773120.eu-wes t-1.elb.amazonaws. com. 36 IN A 52.210.15 5.124	

Tarefa	Descrição	Habilidades necessárias

Registre os conectores dos participantes no serviço DAPS.	De dentro de qualquer uma das EC2 instâncias provisionadas para o DAPS, registre os participantes:
	1. Execute o script disponível na EC2 instância usando o usuário root:
	`cd /srv/mvds/omejdn-daps`
	2. Registre o provedor:
	`bash scripts/register_connector.sh <provider_name>`
	3. Cadastre o consumidor:
	`bash scripts/register_connector.sh <consumer_name>`
	A escolha dos nomes não afeta as próximas etapas. Recomendamos o uso de `provider companyx` e `consumer` ou `companyy` e.
	Os comandos de registro também configurarão automaticamente o serviço DAPS com as informações necessárias obtidas dos certificados e chaves criados.
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Enquanto estiver conectado a um servidor DAPS, reúna as informações necessárias para as etapas posteriores da instalação: 1. De `omejdn-daps/config/clients.yml` get the `client id` para o fornecedor e o consumidor. Os `client id` valores são cadeias longas de dígitos hexadecimais. 2. No `omejdn-daps/keys` diretório, copie o conteúdo dos `provider.key` arquivos `consumer.cert` `consumer.key` `provider.cert` ,, e. Recomendamos copiar e colar o texto em arquivos com nomes semelhantes prefixados `daps-` em sua estação de trabalho. Você deve ter o cliente IDs para o provedor e o consumidor e deve ter quatro arquivos em seu diretório de trabalho em sua estação de trabalho: • O nome do arquivo de origem `consumer.cert`	

Tarefa	Descrição	Habilidades necessárias
	se torna o nome do arquivo da estação de trabalho. `daps-consumer.cert` • O nome do arquivo de origem `consumer.key` se torna o nome do arquivo da estação de trabalho. `daps-consumer.key` • O nome do arquivo de origem `provider.cert` se torna o nome do arquivo da estação de trabalho. `daps-provider.cert` • O nome do arquivo de origem `provider.key` se torna o nome do arquivo da estação de trabalho. `daps-provider.key`	

Implemente os conectores dos participantes

Tarefa	Descrição	Habilidades necessárias
Clone o repositório Tractus-X EDC e use a versão 0.4.1.	A construção do conector Tractus-X EDC requer que os serviços PostgreSQL (banco de dados de ativos) e HashiCorp Vault (gerenciamento de segredos) sejam implantados e disponibilizados. Há muitas versões diferentes dos gráficos Tractus-X EDC	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	Helm. Esse padrão especific a a versão 0.4.1 porque usa o servidor DAPS.
	
	As versões mais recentes usam o Managed Identity Wallet (MIW) com uma implementação distribuída do serviço de identidade.
	
	Na estação de trabalho em que você criou os dois namespaces do Kubernetes, clone o repositório tractusx-edc e confira a ramificação. `release/0.4.1`
	
	`git clone https://github.com/eclipse-tractusx/tractusx-edc`
	
	`cd tractusx-edc`
	
	`git checkout release/0.4.1`	

Tarefa	Descrição	Habilidades necessárias

Configure a carta Tractus-X EDC Helm.	Modifique a configuração do modelo de gráfico Tractus-X Helm para permitir que os dois conectores interajam juntos.
	
	Para fazer isso, você adicionar ia o namespace ao nome DNS do serviço para que ele pudesse ser resolvido por outros serviços no cluster. Essas modificações devem ser feitas no `charts/tractusx-connector/templates/_helpers.tpl` arquivo. Esse padrão fornece uma versão final modificada desse arquivo para você usar. Copie e coloque na `daps` seção do arquivo`charts/tractusx-connector/templates/_helpers.tpl` .
	
	Certifique-se de comentar todas as dependências do DAPS em: `charts/tractusx-connector/Chart.yaml`
	
	`dependencies:`
	`  # IDS Dynamic Attribute Provisioning Service (IAM)`
	`  #  - name: daps`
	`  # version: 0.0.1`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre> # repository:
	 "file://./subcharts/
	omejdn"
	  # alias: daps
	  # condition:
	 install.daps</pre>	

Tarefa	Descrição	Habilidades necessárias

Configure os conectores para usar o PostgreSQL no Amazon RDS.	(Opcional) A instância do Amazon Relational Database Service (Amazon RDS) não é necessária nesse padrão. No entanto, é altamente recomendável usar o Amazon RDS ou o Amazon Aurora, pois eles oferecem recursos como alta disponibilidade, backup e recuperação.
	
	Para substituir o PostgreSQL no Kubernetes pelo Amazon RDS, faça o seguinte:
	
	1. Provisione a instância do Amazon RDS for PostgreSQL.
	2. Em `Chart.yaml` , comente a `PostgreSQL` seção.
	3. Em `provider_values.yml` `econsumer_values.yml` , configure a `postgresql` seção da seguinte forma:
	
	`postgresql:`
	`  auth:`
	`  database: edc`
	`  password: <RDS PASSWORD>`
	`  username: <RDS Username>`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre> jdbcUrl: jdbc:post
	gresql://<RDS DNS
	 NAME>:5432/edc
	  username: <RDS
	 Username>
	  password: <RDS
	 PASSWORD>
	  primary:
	  persistence:
	  enabled: false
	  readReplicas:
	  persistence:
	  enabled: false</pre>	

Tarefa	Descrição	Habilidades necessárias
Configure e implante o conector do provedor e seus serviços.	Para configurar o conector do provedor e seus serviços, faça o seguinte: 1. Para baixar o `provider_edc.yaml` arquivo do `edc_helm_configs` diretório para a pasta atual do gráfico do Helm, execute o seguinte comando: `wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/provider_edc.yaml> -P charts/tractusx-connector/` 2. Substitua as seguintes variáveis (também marcadas no arquivo) por seus valores: • `CLIENT_ID` – O ID gerado pelo DAPS. Eles `CLIENT_ID` devem estar `/srv/mvds/omejdn-daps/config/clients.yml/config/clients.yml` no servidor DAPS. Deve ser uma sequência de caracteres hexadecimais.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	• `DAPS_URL`– O URL do servidor DAPS. Ele deve `https://{DNS name}` usar o nome DNS que você configuro u ao executar o AWS CloudFormation modelo.
	• `VAULT_TOKEN` – O token a ser usado para autorização do Vault. Escolha qualquer valor.
	• `vault.fullnameOver ride` – `vault-pro vider` .
	• `vault.hashicorp.ur l` – `http://vault- provider:8200/` .
	
	Os valores anteriores pressupõem que o nome da implantação e o nome do namespace sejam provider.
	3. Para executar o gráfico do Helm em sua estação de trabalho, use os seguintes comandos:
	
	`cd charts/tractusx-co nnector`
	
	`helm dependency build`
	
	`helm upgrade -- install provider ./ -f`	

Tarefa	Descrição	Habilidades necessárias
	`provider_edc.yaml -n provider`	

Tarefa	Descrição	Habilidades necessárias

Adicione o certificado e as chaves ao cofre do provedor.	Para evitar confusão, produza os seguintes certificados fora do `tractusx-edc/charts` diretório.
	
	Por exemplo, execute o comando a seguir para mudar para seu diretório inicial:
	
	`cd ~`
	
	Agora você precisa adicionar os segredos necessários ao provedor no cofre.
	
	Os nomes dos segredos dentro do cofre são os valores das chaves na `secretNames:` seção do `provider_edc.yml` arquivo. Por padrão, eles são configurados da seguinte forma:
	
	`secretNames:`
	`transferProxyTokenSignerPrivateKey: transfer-proxy-token-signer-private-key`
	`transferProxyTokenSignerPublicKey: transfer-proxy-token-signer-public-key`
	`transferProxyTokenEncryptionAesKey: transfer-`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`proxy-token-encryption-aes-key dapsPrivateKey: daps-private-key dapsPublicKey: daps-public-key`
	
	Uma chave Advanced Encryption Standard (AES), uma chave privada, uma chave pública e um certificado autoassinado são gerados inicialmente. Posteriormente, eles são adicionados como segredos ao cofre.
	
	Além disso, esse diretório deve conter os `daps-provider.key` arquivos `daps-provider.cert` e que você copiou do servidor DAPS.
	
	1. Execute os seguintes comandos :
	
	`# generate a private key openssl ecparam -name prime256v1 -genkey -noout -out provider-private-key.pem # generate corresponding public key openssl ec -in provider-private-key.pem -pubout -out`	

Tarefa	Descrição	Habilidades necessárias
	provider-public-key.pem # create a self-signed certificate openssl req -new -x509 -key provider-private-key.pem -out provider-cert.pem -days 360 # generate aes key openssl rand -base64 32 > provider-aes.key 2. Antes de adicionar os segredos ao cofre, converta-os de várias linhas em linhas únicas substituindo as quebras de linha por: \n cat provider-private-key.pem | sed 's/$/\\\n/'\|tr -d '\n' > provider-private-key.pem.line cat provider-public-key.pem \| sed 's/$/\\\n/'|tr -d '\n' > provider-public-key.pem.line cat provider-cert.pem | sed 's/$/\\\n/'\|tr -d '\n' > provider-cert.pem.line cat provider-aes.key \| sed 's/$/\\\n/'|tr -d '\n' > provider-aes.key.line	

Tarefa	Descrição	Habilidades necessárias
	``` ## The following block is for daps certifica te and key openssl x509 -in daps-provider.cert - outform PEM | sed 's/ $/\\\\n/'\|tr -d '\\n' > daps-provider.cert .line cat daps-provider.key \| sed 's/$/\\\\n/'| tr -d '\\n' > daps- provider.key.line ``` 3. Para formatar os segredos que serão adicionados ao Vault, execute os seguintes comandos: ``` JSONFORMAT='{"cont ent": "%s"}' #create a single line in JSON format printf "${JSONFO RMAT}\\n" "`cat  provider-private- key.pem.line`" > provider-private-k ey.json printf "${JSONFO RMAT}\\n" "`cat  provider-public- key.pem.line`" > provider-public-ke y.json printf "${JSONFO RMAT}\\n" "`cat  provider-cert.pem. line`" > provider- cert.json ```	

Tarefa	Descrição	Habilidades necessárias

	`printf "${JSONFORMAT}\\n" "`cat provider-aes.key.line`" > provider-aes.json`
	
	`printf "${JSONFORMAT}\\n" "`cat daps-provider.key.line`" > daps-provider.key.json`
	`printf "${JSONFORMAT}\\n" "`cat daps-provider.cert.line`" > daps-provider.cert.json`
	
	Os segredos agora estão no formato JSON e estão prontos para serem adicionados ao cofre.
	4. Para obter o nome do pod para o cofre, execute o seguinte comando:
	`kubectl get pods -n provider|egrep "vault|NAME"`
	
	O nome do pod será semelhante `"vault-provider-0"` a. Esse nome é usado ao criar uma porta de encaminhamento para o cofre. A porta de encaminhamento permite que você acesse	

Tarefa	Descrição	Habilidades necessárias
	o cofre para adicionar o segredo. Você deve executar isso em uma estação de trabalho que tenha as credenciais da AWS configuradas. 5. Para acessar o cofre, use `kubectl` para configura r um encaminhamento de porta: `kubectl port-forward <VAULT_POD_NAME> 8200:8200 -n provider` Agora você deve conseguir acessar o cofre por meio do seu navegador ou da CLI. Navegador 1. Usando o navegador , navegue até http://12 7.0.0.1:8200, que usará a porta de encaminhamento que você configurou. 2. Faça login usando o token que você configurou anteriormente`provider_ edc.yml` . No mecanismo de segredos, crie três segredos. Cada segredo terá um `Path for this secret` valor, que é o nome secreto mostrado	

Tarefa	Descrição	Habilidades necessárias
	na lista a seguir. Dentro da `secret data` seção, o nome da chave será `content` e o valor será a única linha de texto do respectivo arquivo nomeado `.line`. 3. Os nomes secretos são provenientes da `secretNames` seção do `provider_edc.yml` arquivo. 4. Crie os seguintes segredos: • Segredo `transfer-proxy-token-signer-private-key` com nome de arquivo `provider-private-key.pem.line` • Segredo `transfer-proxy-token-signer-public-key` com nome de arquivo `provider-cert.pem.line` • Segredo `transfer-proxy-token-encryption-aes-key` com nome de arquivo `provider-aes.key.line`	

Tarefa	Descrição	Habilidades necessárias
	• Segredo `daps-private-key` com nome de arquivo `daps-provider.key.line` • Segredo `daps-public-key` com nome de arquivo `daps-provider.cert.line` CLI do Vault A CLI também usará a porta de encaminhamento que você configurou. 1. Em sua estação de trabalho, instale a CLI do Vault seguindo as instruções na documentação do Vault. HashiCorp 2. Para fazer login no cofre usando o token que você configurou`provider_edc.yml`, execute o seguinte comando: `vault login -address=http://127.0.0.1:8200` Com o token correto, você deve ver a mensagem `"Success! You are now authenticated."`	

Tarefa	Descrição	Habilidades necessárias

	3. Para criar os segredos usando os arquivos formatados em JSON que você criou anteriormente, execute o seguinte código:
	
	`vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-signer-private-key @provider-private-key.json`
	`vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-signer-public-key @provider-cert.json`
	`vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-encryption-aes-key @provider-aes.json`
	
	`vault kv put -address=http://127.0.0.1:8200 secret/daps-private-key @daps-provider.key.json`
	`vault kv put -address=http://127.0.0.1:8200 secret/daps-public-key @daps-provider.cert.json`	

Tarefa	Descrição	Habilidades necessárias

Configure e implante o conector do consumidor e seus serviços.	As etapas para configurar e implantar o consumidor são semelhantes às que você concluiu para o provedor:
	
	1. Para copiar o `consumer_edc.yaml` do aws-patterns-edcrepositório para a pasta `tractusx-edc/charts/tractusx-connecto` r, execute os seguintes comandos:
	
	`cd tractusx-edc`
	
	`wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/consumer_edc.yaml -P charts/tractusx-connector/`
	
	2. Atualize as seguintes variáveis com seus valores reais:
	
	• `CONSUMER_CLIENT_ID` – O ID gerado pelo DAPS. Eles `CONSUMER_CLIENT_ID` devem estar `config/clients.yml` no servidor DAPS.	

Tarefa	Descrição	Habilidades necessárias

	• `DAPS_URL`– O mesmo URL do DAPS que você usou para o provedor.
	• `VAULT_TOKEN` – O token a ser usado para autorização do Vault. Escolha qualquer valor.
	• `vault.fullnameOverride` – `vault-consumer`
	• `vault.hashicorp.url` – `http://vault-provider:8200/`
	
	Os valores anteriores pressupõem que o nome da implantação e o nome do namespace sejam. `consumer`
	3. Para executar o gráfico do Helm, use os seguintes comandos:
	
	`cd charts/tractusx-connector`
	
	`helm upgrade --install consumer ./ -f consumer_edc.yaml -n consumer`	

Tarefa	Descrição	Habilidades necessárias

Adicione o certificado e as chaves ao cofre do consumidor.	Do ponto de vista da segurança, recomendamos regenerar os certificados e as chaves de cada participante do espaço de dados. Esse padrão regenera certificados e chaves para o consumidor.
	
	As etapas são muito semelhantes às do provedor. Você pode verificar os nomes secretos no `consumer_edc.yml` arquivo.
	
	Os nomes dos segredos dentro do cofre são os valores das chaves na `secretNames:` seção do`consumer_edc.yml file` . Por padrão, eles são configurados da seguinte forma:
	
	`secretNames:`
	`transferProxyTokenSignerPrivateKey: transfer-proxy-token-signer-private-key`
	`transferProxyTokenSignerPublicKey: transfer-proxy-token-signer-public-key`
	`transferProxyTokenEncryptionAesKey: transfer-proxy-token-encryption-aes-key`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre>dapsPrivateKey: daps-private-key
	dapsPublicKey: daps-public-key</pre>
	Os `daps-consumer.key` arquivos `daps-consumer.cert` e que você copiou do servidor DAPS já devem existir nesse diretório.
	1. Execute os seguintes comandos :
	<pre># generate a private key
	openssl ecparam -name prime256v1 -genkey -noout -out consumer-private-key.pem
	# generate corresponding public key
	openssl ec -in consumer-private-key.pem -pubout -out consumer-public-key.pem
	# create a self-signed certificate
	openssl req -new -x509 -key consumer-private-key.pem -out consumer-cert.pem -days 360
	# generate aes key
	openssl rand -base64 32 > consumer-aes.key</pre>	

Tarefa	Descrição	Habilidades necessárias

	2. Edite manualmente os arquivos para substituir quebras \n de linha ou use três comandos semelhantes aos seguintes:
	
	`cat consumer-private-key.pem | sed 's/$/\\\n/'|tr -d '\\n' > consumer-private-key.pem.line`
	`cat consumer-public-key.pem | sed 's/$/\\\n/'|tr -d '\\n' > consumer-public-key.pem.line`
	`cat consumer-cert.pem | sed 's/$/\\\\n/'|tr -d '\\n' > consumer-cert.pem.line`
	`cat consumer-aes.key | sed 's/$/\\\\n/'|tr -d '\\n' > consumer-aes.key.line`
	`cat daps-consumer.cert | sed 's/$/\\\\n/'|tr -d '\\n' > daps-consumer.cert.line`
	`cat daps-consumer.key | sed 's/$/\\\\n/'| tr -d '\\n' > daps-consumer.key.line`
	
	3. Para formatar os segredos que serão adicionados ao Vault, execute os seguintes comandos:	

Tarefa	Descrição	Habilidades necessárias

	`JSONFORMAT='{"content": "%s"}'`
	
	`#create a single line in JSON format`
	
	`printf "${JSONFORMAT}\\n" "`cat consumer-private-key.pem.line`" > consumer-private-key.json`
	`printf "${JSONFORMAT}\\n" "`cat consumer-public-key.pem.line`" > consumer-public-key.json`
	`printf "${JSONFORMAT}\\n" "`cat consumer-cert.pem.line`" > consumer-cert.json`
	`printf "${JSONFORMAT}\\n" "`cat consumer-aes.key.line`" > consumer-aes.json`
	
	`printf "${JSONFORMAT}\\n" "`cat daps-consumer.key.line`" > daps-consumer.key.json`
	`printf "${JSONFORMAT}\\n" "`cat daps-consumer.cert.line`" > daps-consumer.cert.json`	

Tarefa	Descrição	Habilidades necessárias
	Os segredos agora estão no formato JSON e estão prontos para serem adicionados ao cofre. 4. Para obter o nome do pod para o cofre do consumidor, execute o seguinte comando: `kubectl get pods -n consumer | egrep "vault|NAME"` O nome do pod será semelhante `"vault-consumer-0"` a. Esse nome é usado ao criar uma porta de encaminhamento para o cofre. A porta de encaminhamento permite que você acesse o cofre para adicionar o segredo. Você deve executar isso em uma estação de trabalho que tenha AWS credenciais configuradas. 5. Para acessar o cofre, use `kubectl` para configurar um encaminhamento de porta:	

Tarefa	Descrição	Habilidades necessárias
	`kubectl port-forward <VAULT_POD_NAME> 8201:8200 -n consumer` Desta vez, a porta local é 8201, para que você possa ter portas de encaminhamento em vigor tanto para o produtor quanto para o consumidor. Navegador Você pode usar seu navegador para se conectar a http://localhost:8201/ para acessar o cofre do consumidor e criar os segredos com nomes e conteúdo conforme descrito. Os segredos e arquivos que contêm o conteúdo são os seguintes: • Segredo `transfer-proxy-token-signer-private-key` com nome de arquivo `consumer-private-key.pem.line` • Segredo `transfer-proxy-token-signer-public-key` com nome de arquivo	

Tarefa	Descrição	Habilidades necessárias

	`consumer-cert.pem.line`
	• Segredo `transfer-proxy-token-encryption-aes-key` com nome de arquivo `consumer-aes.key.line`
	
	CLI do Vault
	
	Usando a CLI do Vault, você pode executar os seguintes comandos para fazer login no cofre e criar os segredos:
	
	1. Faça login no cofre usando o token que você configurou em `consumer_edc.yml` :
	
	``
	vault login -address=http://127.0.0.1:8201
	``
	
	Com o token correto, você deve ver a mensagem `"Success! You are now authenticated."`
	2. Para criar os segredos usando os arquivos formatados em JSON que você criou anteriormente, execute o código a seguir:	

Tarefa	Descrição	Habilidades necessárias

	`vault kv put -address= http://127.0.0.1:8 201 secret/transfer- proxy-token-signer-p rivate-key @consumer -private-key.json`
	`vault kv put - address=http://12 7.0.0.1:8201 secret/ transfer-proxy-token -signer-public-key @consumer-cert.json`
	`vault kv put -address= http://127.0.0.1:8 201 secret/transfer- proxy-token-encrypti on-aes-key @consumer -aes.json`
	`vault kv put -address= http://127.0.0.1:8 201 secret/daps- private-key @daps-con sumer.key.json`
	`vault kv put - address=http://12 7.0.0.1:8201 secret/ daps-public-key @daps-consumer.cer t.json`	

Configure um cliente HTTP para interagir com a API de gerenciamento dos conectores

Tarefa	Descrição	Habilidades necessárias
Configure o encaminhamento de portas.	1. Para verificar o status dos pods, execute os seguintes comandos:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`kubectl get pods -n provider`
	`kubectl get pods -n consumer`
	
	2. Para garantir que as implantações do Kubernetes tenham sido bem-sucedidas, veja os registros dos pods do Kubernetes do provedor e do consumidor executando os seguintes comandos:
	
	`kubectl logs -n provider <producer control plane pod name>`
	`kubectl logs -n consumer <consumer control plane pod name>`
	
	O cluster é privado e não pode ser acessado publicamente. Para interagir com os conectores, use o recurso de encaminhamento de portas do Kubernetes para encaminhar o tráfego gerado pela sua máquina para o plano de controle do conector.
	
	1. No primeiro terminal, encaminhe as solicitações do consumidor para a API	

Tarefa	Descrição	Habilidades necessárias

	de gerenciamento pela porta 8300:
	
	`kubectl port-forward deployment/consumer-tractusx-connector-controlplane 8300:8081 -n consumer`
	
	2. No segundo terminal, encaminhe as solicitações do provedor para a API de gerenciamento pela porta 8400:
	
	`kubectl port-forward deployment/provider-tractusx-connector-controlplane 8400:8081 -n provider`	

Tarefa	Descrição	Habilidades necessárias
Crie buckets S3 para o provedor e o consumidor.	Atualmente, o conector EDC não usa credenciais temporárias da AWS, como as fornecidas ao assumir uma função. O EDC suporta somente o uso de uma combinação de ID de chave de acesso IAM e chave de acesso secreta. São necessários dois buckets S3 para as etapas posteriores. Um bucket S3 é usado para armazenar dados disponibi lizados pelo provedor. O outro bucket do S3 é para dados recebidos pelo consumidor. O usuário do IAM deve ter permissão para ler e gravar objetos somente nos dois buckets nomeados. Um ID de chave de acesso e um par de chaves de acesso secreto precisam ser criados e mantidos em segurança. Depois que esse MVDS for desativado, o usuário do IAM deverá ser excluído. O código a seguir é um exemplo de política do IAM para o usuário: {	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	"Version": "2012-10-17", "Statement": [{ "Sid": "Stmt1708699805237", "Action": ["s3:GetObject", "s3:GetObjectVersion", "s3:ListAllMyBuckets", "s3:ListBucket", "s3:ListBucketMultipartUploads", "s3:ListBucketVersions", "s3:PutObject"], "Effect": "Allow", "Resource": ["arn:aws:s3:::<S3 Provider Bucket>", "arn:aws:s3:::<S3 Consumer Bucket>", "arn:aws:s3:::<S3 Provider Bucket>/*", "arn:aws:s3:::<S3 Consumer Bucket>/*"] }] }	

Tarefa	Descrição	Habilidades necessárias
Configure o Postman para interagir com o conector.	Agora você pode interagir com os conectores por meio da sua EC2 instância. Use o Postman como um cliente HTTP e forneça Coleções Postman para os conectores do provedor e do consumidor. Importe as coleções do `aws-pattern-edc` repositório para sua instância do Postman. Esse padrão usa variáveis de coleção do Postman para fornecer informações às suas solicitações.	Desenvolvedor de aplicativos, Engenheiro de dados

Forneça dados de pegada de carbono da empresa X por meio do conector

Tarefa	Descrição	Habilidades necessárias
Prepare os dados de intensidade das emissões de carbono a serem compartilhados.	Primeiro, você precisa decidir sobre o ativo de dados a ser compartilhado. Os dados da empresa X representam a pegada de emissões de carbono de sua frota de veículos. O peso é o peso bruto do veículo (GVW) em toneladas e as emissões estão em gramas por tonelada-quilômetro (g CO2 e/t-km) de CO2 acordo	Engenheiro de dados, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	com a medição (WTW): Wheel-to-Well • Tipo de veículo: Van; peso: < 3,5; emissões: 800 • Tipo de veículo: caminhão urbano; peso: 3,5 ± 7,5; emissões: 315 • Tipo de veículo: veículo médio de mercadorias (MGV); peso: 7,5 ± 20; emissões: 195 • Tipo de veículo: veículo pesado de mercadori as (HGV); peso: > 20; emissões: 115 Os dados de exemplo estão no `carbon_emissions_d ata.json` arquivo no `aws-patterns-edc` repositório. A empresa X usa o Amazon S3 para armazenar objetos. Crie o bucket do S3 e armazene o objeto de dados de exemplo nele. Os comandos a seguir criam um bucket do S3 com configura ções de segurança padrão. É altamente recomendável consultar as melhores práticas de segurança para o Amazon S3.	

Tarefa	Descrição	Habilidades necessárias

	`aws s3api create-bucket <BUCKET_NAME> --region <AWS_REGION>`
	`# You need to add '--create-bucket-configuration`
	`# LocationConstraint=<AWS_REGION>' if you want to create # the bucket outside of us-east-1 region`
	
	`aws s3api put-object --bucket <BUCKET_NAME> \`
	`--key <S3 OBJECT NAME> \`
	`--body <PATH OF THE FILE TO UPLOAD>`
	
	O nome do bucket do S3 deve ser globalmente exclusivo. Para obter mais informações sobre regras de nomenclatura, consulte a documentação da AWS.	

Tarefa	Descrição	Habilidades necessárias
Registre o ativo de dados no conector do provedor usando o Postman.	Um ativo de dados do conector EDC contém o nome dos dados e sua localização. Nesse caso, o ativo de dados do conector EDC apontará para o objeto criado no bucket do S3: • Conector: Provedor • Solicitação: Criar ativo • Variáveis da coleção: atualizaçãoASSET_NAME . Escolha um nome significativo que represente o ativo. • Corpo da solicitação: atualize o corpo da solicitação com o bucket do S3 que você criou para o provedor. `"dataAddress": { "edc:type": "AmazonS3", "name": "Vehicle Carbon Footprint", "bucketName": "<REPLACE WITH THE SOURCE BUCKET NAME>", "keyName": "<REPLACE WITH YOUR OBJECT NAME>", "region": "<REPLACE WITH THE BUCKET REGION>", "accessKeyId": "<REPLACE WITH YOUR ACCESS KEY ID>",`	Desenvolvedor de aplicativos, Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias

	<pre>"secretAc
	cessKey": "<REPLACE
	WITH SECRET ACCESS
	KEY>"
	}</pre>
	• Resposta: uma solicitação bem-sucedida retorna a hora de criação e o ID do ativo recém-criado.
	<pre>{
	"@id": "c89aa31c-
	ec4c-44ed-9e8c-16
	47f19d7583"
	}</pre>
	• Variável de coleção ASSET_ID: atualize a variável de coleção Postman `ASSET_ID` com a ID que foi gerada automaticamente pelo conector EDC após a criação.	

Tarefa	Descrição	Habilidades necessárias

Defina a política de uso do ativo.	Um ativo de dados EDC deve estar associado a políticas de uso claras. Primeiro, crie a definição de política no conector do provedor.
	
	A política da empresa X é permitir que os participantes do espaço de dados usem os dados da pegada de carbono.
	
	• Corpo da solicitação:
	  • Conector: Provedor
	  • Solicitação: Criar política
	  • Variáveis de coleção: atualize a `Policy Name` variável com o nome da política.
	• Resposta: Uma solicitação bem-sucedida retorna a hora criada e o ID da política recém-criada. Atualize a variável de coleta `POLICY_ID` com o ID da política gerada pelo conector EDC após a criação.
		Desenvolvedor de aplicativos, Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
Defina uma oferta de contrato EDC para o ativo e sua política de uso.	Para permitir que outros participantes solicitem acesso aos seus dados, ofereça-os em um contrato que especifiq ue as condições e permissões de uso: • Conector: Provedor • Solicitação: Criar definição de contrato • Variáveis de coleta: atualize a `Contract Name` variável com um nome para a oferta ou definição do contrato.	Desenvolvedor de aplicativos, Engenheiro de dados

Descubra os ativos e chegue a um acordo sobre os contratos definidos

Tarefa	Descrição	Habilidades necessárias
Solicite o catálogo de dados compartilhado pela empresa X.	Como consumidora de dados no espaço de dados, a empresa Y precisa primeiro descobrir os dados que estão sendo compartilhados por outros participantes. Nessa configuração básica, você pode fazer isso solicitando que o conector do consumidor solicite o catálogo de ativos disponíve is diretamente do conector do provedor.	Desenvolvedor de aplicativos, Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias

	• Conector: Consumidor
	• Solicitação: Solicitar catálogo
	• Resposta: Todos os ativos de dados disponíveis do provedor, juntamente com suas políticas de uso anexadas. Como consumidor de dados, procure o contrato de seu interesse e atualize as seguintes variáveis de coleta de acordo.
	  • `CONTRACT_OFFER_ID` – O ID da oferta de contrato que o consumidor deseja negociar
	  • `ASSET_ID`– O ID do ativo que o consumidor deseja negociar
	  • `PROVIDER_CLIENT_ID` – O ID do conector do provedor com o qual negociar	

Tarefa	Descrição	Habilidades necessárias
Inicie uma negociação de contrato para os dados de intensidade de emissões de carbono da empresa X.	Agora que você identificou o ativo que deseja consumir, inicie um processo de negociação de contrato entre os conectores do consumidor e do provedor. • Conector: Consumidor • Solicitação: Negociação de contrato • Variáveis de coleção: atualize a `CONSUMER_CLIENT_ID` variável com o ID do conector do consumidor com o qual negociar. O processo pode levar algum tempo até atingir o estado VERIFICADO. Você pode verificar o estado da negociação do contrato e o ID do contrato correspondente usando a `Get Negotiation` solicitação.	Desenvolvedor de aplicativos, Engenheiro de dados

Consuma os dados usando o contrato

Tarefa	Descrição	Habilidades necessárias
Consuma dados de endpoints HTTP.	(Opção 1) Para usar o plano de dados HTTP para consumir dados no espaço de dados,	Desenvolvedor de aplicativos, Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	você pode usar webhook.site para emular um servidor HTTP e iniciar o processo de transferência no conector do consumidor: • Conector: Consumidor • Solicitação: Negociação de contrato • Variáveis de coleta: atualize a `Contract Agreement ID` variável com o ID do contrato gerado pelo conector EDC. • Corpo da solicitação: atualize o corpo da solicitação para especificar HTTP `dataDestination` junto com o URL do webhook: `{ "dataDestination": { "type": "HttpProxy" }, "privateProperties": { "receiverHttpEndpoint": "<WEBHOOK URL>" } }` O conector enviará as informações necessári	

Tarefa	Descrição	Habilidades necessárias
	as para baixar o arquivo diretamente para o URL do webhook. A carga recebida é semelhante à seguinte: `{ "id": "dcc90391-3819-4b54-b401-1a005a029b78", "endpoint": "http://consumer-tractusx-connector-dataplane.consumer:8081/api/public", "authKey": "Authorization", "authCode": "<AUTH CODE YOU RECEIVE IN THE ENDPOINT>", "properties": { "https://w3id.org/edc/v0.0.1/ns/cid": "vehicle-carbon-footprint-contract:4563abf7-5dc7-4c28-bc3d-97f45e32edac:b073669b-db20-4c83-82df-46b583c4c062" } }` Use as credenciais recebidas para obter o ativo do S3 que foi compartilhado pelo provedor.	

Tarefa	Descrição	Habilidades necessárias
	Nesta última etapa, você deve enviar a solicitação para o plano de dados do consumidor (portas de encaminhamento adequadas), conforme indicado na carga útil (`endpoint`).	

Tarefa	Descrição	Habilidades necessárias
Consuma dados diretamente dos buckets do S3.	(Opção 2) Use a integração do Amazon S3 com o conector EDC e aponte diretamente para o bucket do S3 na infraestrutura do consumidor como destino: • Corpo da solicitação: atualize o corpo da solicitação para especificar o bucket do S3 como um DataDestination. Esse deve ser o bucket do S3 que você criou anteriormente para armazenar dados recebidos pelo consumidor. `{ "dataDestination": { "type": "AmazonS3", "bucketName": "{{ REPLACE WITH THE DESTINATION BUCKET NAME }}", "keyName": "{{ REPLACE WITH YOUR OBJECT NAME }}", "region": "{{ REPLACE WITH THE BUCKET REGION }}", "accessKeyId": "{{ REPLACE WITH YOUR ACCESS KEY ID }}", "secretAccessKey": "{{ REPLACE`	Engenheiro de dados, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	<pre>WITH SECRET ACCESS
	KEY }}"
	}
	}
	}</pre>	

Solução de problemas

Problema	Solução
O conector pode levantar um problema sobre o formato PEM do certificado.	Concatene o conteúdo de cada arquivo em uma única linha adicionando. \n

Recursos relacionados

- DSSC
- Criação de espaços de dados para casos de uso de sustentabilidade (estratégia AWS Prescriptive Guidance da Think-it)
- AWS para espaços de dados
- Documentação do Tractus-X
- DAPS
- Habilitando o compartilhamento de dados por meio de espaços de dados e da AWS (postagem no blog)

Mais informações

Especificações do espaço de dados

Participantes

Participante	Descrição da empresa	Foco da empresa

Empresa X	Opera uma frota de veículos na Europa e na América do Sul para transportar várias mercadorias.	Visa tomar decisões baseadas em dados para reduzir a intensidade de sua pegada de carbono.
Empresa Y	Uma autoridade reguladora ambiental	Aplica regulamentações e políticas ambientais projetadas para monitorar e mitigar o impacto ambiental de empresas e indústrias, incluindo a intensidade das emissões de carbono.

Caso de negócios

A empresa X usa tecnologia de espaço de dados para compartilhar dados de pegada de carbono com um auditor de conformidade, a empresa Y, para avaliar e abordar o impacto ambiental das operações logísticas da empresa X.

Autoridade de espaço de dados

A autoridade do espaço de dados é um consórcio de organizações que governam o espaço de dados. Nesse padrão, tanto a empresa X quanto a empresa Y formam o órgão de governança e representam uma autoridade federada de espaço de dados.

Componentes do espaço de dados

Componente	Implementação escolhida	Informações adicionais
Protocolo de troca de conjuntos de dados	Protocolo Dataspace versão 0.8	• JSON-LD • Vocabulário do Catálogo de Dados (DCAT)
Conector de espaço de dados	Conector Tractus-X EDC versão 0.4.1	• Extensões EDC
Políticas de troca de dados	Política de USO padrão	• Linguagem Aberta de Direitos Digitais (ODRL)

Serviços de espaço de dados

Serviço	Implementação	Informações adicionais
Serviço de identidade	Sistema de provisionamento dinâmico de atributos (DAPS)	“Um Sistema Dinâmico de Provisionamento de Atributos (DAPS) tem a intenção de determinar certos atributos para organizações e conectores. Portanto, terceiros não precisam confiar neste último, desde que confiem nas afirmações do DAPS.” — TAPETES Para focar na lógica do conector, o espaço de dados é implantado em uma EC2 máquina Amazon usando o Docker Compose.
Serviço de descoberta	Catálogo federado Gaia-X	“O Catálogo Federado constitui um repositório indexado de autodescrições do Gaia-X para permitir a descoberta e seleção de provedores e suas ofertas de serviços. As autodescrições são as informações fornecidas pelos participantes sobre si mesmos e sobre seus serviços na forma de propriedades e reivindicações.” — Kickstarter do ecossistema Gaia-X

Dados a serem trocados

Ativos de dados	Descrição	Formato
Dados de emissões de carbono	Valores de intensidade para diferentes tipos de veículos na região especificada (Europa e América do Sul) de toda a frota de veículos	Arquivo JSON

Modelo de dados

```
{
  "region": "string",
  "vehicles": [
// Each vehicle type has its Gross Vehicle Weight (GVW) category and its emission
 intensity in grams of CO2 per Tonne-Kilometer (g CO2 e/t-km) according to the "Well-
to-Wheel" (WTW) measurement.
    {
      "type": "string",
      "gross_vehicle_weight": "string",
      "emission_intensity": {
        "CO2": "number",
        "unit": "string"
      }
    }
  ]
}
```

Conector Tractus-X EDC

Para a documentação de cada parâmetro EDC do Tractus-X, consulte o arquivo de valores original.

A tabela a seguir lista todos os serviços, junto com suas portas e endpoints expostos correspondentes para referência.

Nome do serviço	Porta e caminho
Ambiente de gerenciamento	• gerenciamento: – Porta: 8081 Caminho: `/management` • controle – Porta: 8083 Caminho: `/control`

	• Porta do protocolo: Caminho 8084: `/api/v1/dsp` • métricas – Porta: 9090 Caminho: `/metrics` • observabilidade – Porta: 8085 Caminho: `/observability`
Plano de dados	padrão – Porta: 8080 Caminho: `/api` público – Porta: 8081 Caminho: `/api/dataplane/control` proxy – Porta: 8186 Caminho: `/proxy` métricas – Porta: 9090 Caminho: `/metrics` observabilidade – Porta: 8085 Caminho: `/observability`
Cofre	Porta: 8200
PostgreSQL	Porta: 5432

Usando o AWS Secrets Manager Manager

É possível usar o Secrets Manager em vez do HashiCorp Vault como gerenciador de segredos. Para fazer isso, você deve usar ou criar a extensão AWS Secrets Manager EDC.

Você será responsável por criar e manter sua própria imagem, porque o Tractus-X não fornece suporte para o Secrets Manager.

Para fazer isso, você precisa modificar os arquivos Gradle de compilação do plano de controle e do plano de dados do conector introduzindo sua extensão AWS Secrets Manager EDC (veja este artefato maven para ver um exemplo) e, em seguida, criar, manter e referenciar a imagem do Docker.

Para obter mais informações sobre a refatoração da imagem Docker do conector Tractus-X, consulte Refactor Tractus-X EDC Helm charts.

Para simplificar, evitamos reconstruir a imagem do conector nesse padrão e usamos o HashiCorp Vault.

Configure a classificação específica do idioma para os resultados da consulta do Amazon Redshift usando uma UDF escalar do Python

Criado por Ethan Stark (AWS)

Resumo

Esse padrão fornece as etapas e o código de amostra para usar uma UDF escalar do Python (função definida pelo usuário) para configurar a classificação linguística sem distinção entre maiúsculas e minúsculas para os resultados da consulta do Amazon Redshift. É necessário usar uma UDF escalar do Python porque o Amazon Redshift retorna resultados com base na ordenação binária UTF-8 e não é compatível com a classificação específica da linguagem. Uma UDF em Python é um código de processamento não SQL baseado em um programa Python 2.7 e executado em um data warehouse. Você pode executar o código UDF do Python com uma instrução SQL em uma única consulta. Para obter mais informações, consulte a postagem do blog de Big Data da AWS sobre Introdução ao Python UDFs no Amazon Redshift.

Os dados de amostra nesse padrão são baseados no alfabeto turco para fins de demonstração. A UDF escalar do Python nesse padrão foi criada para fazer com que os resultados da consulta padrão do Amazon Redshift estejam em conformidade com a ordem linguística dos caracteres no idioma turco. Para obter mais informações, consulte o Exemplo do idioma turco na seção Informações adicionais desse padrão. Você pode modificar a UDF escalar do Python nesse padrão para outras linguagens.

Pré-requisitos e limitações

Pré-requisitos

- Cluster do Amazon Redshift com um banco de dados, esquema e tabelas
- Usuário do Amazon Redshift com permissões CREATE TABLE e CREATE FUNCTION
- Python 2.7 ou superior

Limitações

A classificação linguística usada pelas consultas nesse padrão não diferencia maiúsculas de minúsculas.

Arquitetura

Pilha de tecnologia

- Amazon Redshift
- UDFs do Python

Ferramentas

Serviços da AWS

- O Amazon Redshift é um serviço de data warehouse em escala de petabytes gerenciado na Nuvem AWS. O Amazon Redshift é integrado ao seu data lake, o que permite que você use seus dados para adquirir novos insights para seus negócios e clientes.

Outras ferramentas

- As funções definidas pelo usuário Python (UDFs) são funções que você pode escrever em Python e depois chamar em instruções SQL.

Épicos

Desenvolva código para classificar os resultados da consulta em ordem linguística

Tarefa	Descrição	Habilidades necessárias

Crie uma tabela para seus dados de amostra.	Para criar uma tabela no Amazon Redshift e inserir seus dados de amostra na tabela, use as seguintes instruções SQL:
	`CREATE TABLE my_table (first_name varchar(30));`
	`INSERT INTO my_table (first_name)`
		Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias

	``
	VALUES
	    ('ali'),
	    ('Ali'),
	    ('ırmak'),
	    ('IRMAK'),
	    ('irem'),
	    ('İREM'),
	    ('oğuz'),
	    ('OĞUZ'),
	    ('ömer'),
	    ('ÖMER'),
	    ('sedat'),
	    ('SEDAT'),
	    ('şule'),
	``	

	Note Os primeiros nomes nos dados da amostra incluem caracteres especiais do alfabeto turco. Para obter mais informações sobre as considera ções sobre o idioma turco neste exemplo, consulte Exemplo do idioma turco na seção Informações adicionai s desse padrão.	

Tarefa	Descrição	Habilidades necessárias

Verifique a classificação padrão dos dados da amostra.	Para ver a classificação padrão dos seus dados de amostra no Amazon Redshift, execute a seguinte consulta:
	`SELECT first_name FROM my_table ORDER BY first_name;`
	A consulta retorna a lista de nomes próprios da tabela que você criou anteriormente:
	`first_name`
	`---------------`
	`Ali`
	`IRMAK`
	`OĞUZ`
	`SEDAT`
	`ali`
	`irem`
	`oğuz`
	`sedat`
	`ÖMER`
	`ömer`
	`İREM`
	`ırmak`
	`ŞULE`
	`şule`
	Os resultados da consulta não estão na ordem correta porque a ordem padrão do binário UTF-8 não acomoda a ordem linguística dos caracteres especiais turcos.
		Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
Crie uma UDF escalar em Python	Para criar uma UDF escalar em Python, use o seguinte código SQL: `CREATE OR REPLACE FUNCTION collate_sort (value varchar) RETURNS varchar IMMUTABLE AS $$ def sort_str(val): import string dictionary = { 'I': 'ı', 'ı': 'h~', 'İ': 'i', 'Ş': 's~', 'ş': 's~', 'Ğ': 'g~', 'ğ': 'g~', 'Ü': 'u~', 'ü': 'u~', 'Ö': 'o~', 'ö': 'o~', 'Ç': 'c~', 'ç': 'c~' } for key, value in dictionary.items(): val = val.replace(key, value) return val.lower()`	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias

	`    return sort_str( value)`
	
	`$$ LANGUAGE plpythonu;`	

Consulte os dados de amostra.	Para consultar os dados de amostra usando as UDFs do Python, execute esta consulta SQL:
	
	`SELECT first_name FROM my_table ORDER BY collate_order(firs t_name);`
	
	A consulta agora retorna os dados de amostra em ordem linguística turca:
	
	`first_name`
	`---------------`
	`ali`
	`Ali`
	`ırmak`
	`IRMAK`
	`irem`
	`İREM`
	`oğuz`
	`OĞUZ`
	`ömer`
	`Ömer`
	`sedat`
	`SEDAT`
	`şule`
	`ŞULE`
		Engenheiro de dados

Recursos relacionados

- Cláusula ORDER BY (documentação do Amazon Redshift)
- Criar uma UDF escalar em Python (documentação do Amazon Redshift)

Mais informações

Exemplo de idioma turco

O Amazon Redshift retorna os resultados da consulta com base na ordem de classificação binária UTF-8, não na ordem de classificação específica do idioma. Isso significa que se você consultar uma tabela do Amazon Redshift contendo caracteres turcos, os resultados da consulta não serão classificados de acordo com a ordem linguística do idioma turco. O idioma turco contém seis caracteres especiais (ç, ı, ğ, ö, ş e ü) que não existem no alfabeto latino. Esses caracteres especiais são colocados no final de um conjunto de resultados ordenado com base na ordem binária UTF-8, conforme mostra a tabela a seguir.

Ordenação binária UTF-8	Ordenação linguística turca
a	a
b	b
c	c
d	ç (*)
p	d
f	p
g	f
h	g
i	ğ (*)
j	h
k	i (*)

l	i
m	j
n	k
o	l
p	m
r	n
s	o
t	ö (*)
u	p
v	r
y	s
z	ş (*)
ç (*)	t
ğ (*)	u
i (*)	ü (*)
ö (*)	v
ş (*)	y
ü (*)	z

> **Note**
>
> O asterisco (*) indica um caractere especial no idioma turco.

Como ilustra a tabela acima, o caractere especial ç está entre c e d na ordenação linguística turca, mas aparece depois de z na ordem binária UTF-8. A UDF escalar no Python nesse padrão usa o seguinte dicionário de substituição de caracteres para substituir os caracteres especiais turcos pelos caracteres correspondentes equivalentes ao latim.

Caractere especial turco	Caractere equivalente em latim
ç	c~
ı	h~
ğ	g~
ö	o~
ş	s~
ü	u~

> **Note**
>
> Um caractere tilde (~) é anexado ao final dos caracteres latinos que substituem os caracteres especiais turcos correspondentes.

Modifique uma função UDF escalar do Python

Para modificar a função UDF escalar do Python a partir desse padrão para que a função aceite um parâmetro localizar e ofereça suporte a um dicionário de várias transações, use o seguinte código SQL:

```
CREATE OR REPLACE FUNCTION collate_sort (value varchar, locale varchar)
RETURNS varchar
IMMUTABLE
AS
$$
    def sort_str(val):
       import string
       # Turkish Dictionary
       if locale == 'tr-TR':
```

```
            dictionary = {
               'I': 'ı',
               'ı': 'h~',
               'İ': 'i',
               'Ş': 's~',
               'ş': 's~',
               'Ğ': 'g~',
               'ğ': 'g~',
               'Ü': 'u~',
               'ü': 'u~',
               'Ö': 'o~',
               'ö': 'o~',
               'Ç': 'c~',
               'ç': 'c~'
        }
        # German Dictionary
        if locale == 'de-DE':
            dictionary = {
               ....
               ....
        }

        for key, value in dictionary.items():
            val = val.replace(key, value)

        return val.lower()

    return sort_str(value)

$$ LANGUAGE plpythonu;
```

O código de exemplo a seguir mostra como consultar a UDFs do Python modificada:

```
SELECT first_name FROM my_table ORDER BY collate_order(first_name, 'tr-TR');
```

Assine uma função do Lambda para notificações de eventos de buckets do S3 em diferentes regiões da AWS

Criado por Suresh Konathala, Andrew Preston e Arindom Sarkar

Resumo

As notificações de eventos do Amazon Simple Storage Service (Amazon S3) publicam notificações para determinados eventos em seu bucket do S3 (por exemplo, eventos criados por objetos, eventos de remoção de objetos ou eventos de restauração de objetos). Você pode usar uma função do AWS Lambda para processar essas notificações de acordo com os requisitos do seu aplicativo. No entanto, a função do Lambda não pode assinar diretamente notificações de buckets do S3 hospedados em diferentes regiões da AWS.

A abordagem desse padrão implanta um cenário de fanout para processar notificações do Amazon S3 de buckets do S3 entre regiões usando um tópico do Amazon Simple Notification Service (Amazon SNS) para cada região. Esses tópicos do SNS regional enviam notificações de eventos do Amazon S3 para uma fila do Amazon Simple Queue Service (Amazon SQS) em uma região central que também contém sua função do Lambda. A função do Lambda se inscreve nessa fila do SQS e processa as notificações de eventos de acordo com os requisitos da sua organização.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Buckets S3 existentes em várias regiões, incluindo uma região central para hospedar a fila do Amazon SQS e a função do Lambda.
- AWS Command Line Interface (AWS CLI), instalada e configurada. Para obter mais informações, consulte Instalação, atualização e desinstalação da AWS CLI na documentação da AWS CLI.
- Familiaridade com o cenário de fanout no Amazon SNS. Para obter mais informações, consulte Cenários comuns do Amazon SNS na documentação do Amazon SNS.

Arquitetura

O diagrama a seguir mostra a arquitetura da abordagem desse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. O Amazon S3 envia notificações de eventos sobre buckets do S3 (por exemplo, objeto criado, objeto removido ou objeto restaurado) para um tópico do SNS na mesma região.
2. O tópico do SNS publica o evento em uma fila do SQS na região central.
3. A fila do SQS é configurada como a fonte de eventos para sua função do Lambda e armazena em buffer as mensagens de eventos para a função do Lambda.
4. A função do Lambda pesquisa mensagens na fila do SQS e processa as notificações de eventos do Amazon S3 de acordo com os requisitos do seu aplicativo.

Pilha de tecnologia

- Lambda
- Amazon SNS
- Amazon SQS
- Amazon S3

Ferramentas

- AWS CLI: o AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto para interagir com serviços da AWS por meio de comandos em seu shell de linha de comando. Com configuração mínima, você pode executar comandos da AWS CLI que implementam funcionalidade equivalente àquela fornecida pelo Console de Gerenciamento da AWS baseado em navegador a partir de um prompt de comando.
- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em várias contas e regiões da AWS.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.

- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.
- Amazon SQS : o Amazon Simple Queue Service (Amazon SQS) oferece uma fila hospedada segura, durável e disponível que permite integrar e desacoplar sistemas e componentes de software distribuídos. O Amazon SQS oferece suporte a filas padrão e FIFO.

Épicos

Crie a fila do SQS e a função do Lambda em sua região central

Tarefa	Descrição	Habilidades necessárias
Crie uma fila do SQS com um gatilho do Lambda.	Faça login no Console de Gerenciamento da AWS e use as instruções do tutorial Usando o Lambda com o Amazon SQS na documentação do AWS Lambda para criar os seguintes recursos em sua região central: • Uma função de execução do Lambda • Uma função do Lambda para processar os eventos do Amazon S3 • Uma fila do SQS **Note** Certifique-se de configurar a fila SQS como a fonte	AWS DevOps, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	do evento para sua função Lambda.	

Crie um tópico do SNS e configure notificações de eventos para os buckets do S3 em cada região necessária

Tarefa	Descrição	Habilidades necessárias
Crie um tópico do SNS para receber notificações de eventos do Amazon S3.	Crie um tópico do SNS em uma região da qual você deseja receber notificações de eventos do Amazon S3. Para obter mais informações, consulte Criação de um tópico SNS na documentação do Amazon SNS. **Important** Certifique-se de registrar o Amazon Resource Name (ARN) do seu tópico do SNS.	AWS DevOps, arquiteto de nuvem
Assinar o tópico SNS na fila central do SQS.	Assine seu tópico do SNS na fila do SQS hospedada pela sua região central. Para obter mais informações sobre isso, consulte Assinar um tópico do SNS na documentação do Amazon SNS.	AWS DevOps, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Atualize a política de acesso do tópico do SNS.	1. Abra o console do Amazon SNS, selecione Tópicos e, em seguida, selecione o tópico SNS que você criou anteriormente. 2. Selecione Editar e, em seguida, expanda a seção Política de acesso - opcional. 3. Anexe a seguinte política de acesso ao seu tópico do SNS para permitir a permissão `sns:publish` para o Amazon S3 e, em seguida, selecione Salvar: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "0", "Effect": "Allow", "Principal": { "Service": "s3.amazonaws.com" }, "Action": "sns:Publish", "Resource": "arn:aws:sns:us-west-2::s3Events-SNSTopic-us-west-2" } ] }`	AWS DevOps, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure notificações para cada bucket do S3 na região.	Configure notificações de eventos para cada bucket do S3 na região. Para obter mais informações, consulte Habilitação e configuração de notificações de eventos usando o console do Amazon S3 na documentação do Amazon S3. **Note** Na seção Destino, escolha o tópico SNS e especifique o ARN do tópico SNS que você criou anteriorm ente.	AWS DevOps, arquiteto de nuvem
Repita esse épico para todas as regiões necessárias.	**Important** Repita as tarefas neste épico para cada região da qual você deseja receber notificações de eventos do Amazon S3, incluindo sua região central.	AWS DevOps, arquiteto de nuvem

Recursos relacionados

- Como configurar uma política de acesso (documentação do Amazon SQS)

- Como configurar uma fila do SQS como uma origem de eventos (documentação do AWS Lambda)
- Como configurar uma fila do SQS para iniciar uma função do Lambda (documentação do Amazon SQS)
- AWS::Lambda::Function recurso (CloudFormation documentação da AWS)

Três tipos de trabalho de ETL do AWS Glue para converter dados em Apache Parquet

Criado por Adnan Alvee (AWS), Karthikeyan Ramachandran (AWS) e Nith Govindasivan (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), o AWS Glue é um serviço para extração, transformação e carregamento (ETL) totalmente gerenciado. O AWS Glue torna econômico categorizar os dados, limpá-los, aprimorá-los e movê-los de modo confiável entre vários armazenamentos e fluxos de dados.

Esse padrão fornece diferentes tipos de trabalho no AWS Glue e usa três scripts diferentes para demonstrar a criação de trabalhos de ETL.

Você pode usar o AWS Glue para escrever trabalhos de ETL em um ambiente de shell Python. Você também pode criar trabalhos ETL em lote e de streaming usando Python PySpark () ou Scala em um ambiente gerenciado do Apache Spark. Para começar a criar trabalhos de ETL, esse padrão se concentra em trabalhos ETL em lote usando Python, shell e Scala. PySpark Os trabalhos de shell do Python são destinados a workloads que exigem menor poder computacional. O ambiente gerenciado do Apache Spark é destinado a workloads que exigem alto poder computacional.

O Apache Parquet foi desenvolvido para dar suporte a esquemas eficientes de compressão e codificação. Ele pode acelerar suas workloads de análise porque armazena dados de forma colunar. A conversão de dados em Parquet pode economizar espaço de armazenamento, custo e tempo no longo prazo. Para saber mais sobre o Parquet, consulte a postagem do blog Apache Parquet: Como ser um herói com o formato de dados colunares de código aberto.

Pré-requisitos e limitações

Pré-requisitos

- Função do AWS Identity and Access Management (IAM) (se você não tiver uma função, consulte a seção Informações adicionais.)

Arquitetura

Pilha de tecnologias de destino

- AWS Glue
- Amazon Simple Storage Service (Amazon S3)
- Apache Parquet

Automação e escala

- Os fluxos de trabalho do AWS Glue oferecem suporte à automação total de um pipeline de ETL.
- Você pode alterar o número de unidades de processamento de dados (DPUs) ou tipos de trabalhadores para escalar horizontal e verticalmente.

Ferramentas

Serviços da AWS

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Glue é um serviço de ETL totalmente gerenciado para categorizar, limpar, enriquecer e mover dados entre armazenamentos de dados e fluxos de dados.

Outras ferramentas

- O Apache Parquet é um formato de arquivos de dados orientados por colunas de código aberto projetado para armazenamento e recuperação.

Configuração

Use os dados a seguir para configurar a potência computacional do AWS Glue ETL. Para reduzir custos, use as configurações mínimas ao executar a workload fornecida nesse padrão.

- Python shell: você pode usar 1 DPU para utilizar 16 GB de memória ou 0,0625 DPU para utilizar 1 GB de memória. Esse padrão usa 0,0625 DPU, que é o padrão no console do AWS Glue.
- Python ou Scala para Spark: se você escolher os tipos de trabalho relacionados ao Spark no console, o AWS Glue, por padrão, usa 10 operadores e o tipo de operador G.1X. Esse padrão usa dois operadores, que é o número mínimo permitido, com o tipo de operador padrão, que é suficiente e econômico.

A tabela a seguir mostra os diferentes tipos de operadores do AWS Glue para o ambiente Apache Spark. Como um trabalho de Python shell não usa o ambiente Apache Spark para executar o Python, ele não está incluído na tabela.

	Padrão	G.1X	G.2X
vCPU	4	4	8
Memória	16 GB	16 GB	32 GB
Espaço em disco	50 GB	64 GB	128 GB
Executor por operador	2	1	1

Código

Para ver o código usado nesse padrão, incluindo o perfil do IAM e a configuração de parâmetros, consulte a seção Informações adicionais.

Épicos

Carregar os dados

Tarefa	Descrição	Habilidades necessárias
Carregar dados para um bucket do S3 novo ou existente.	Crie ou use um bucket do S3 existente na sua conta. Faça upload do arquivo sample_data.csv na seção Anexos e anote a localização do bucket e do prefixo do S3.	AWS geral

Criar e executar o trabalho do AWS Glue

Tarefa	Descrição	Habilidades necessárias
Criar o trabalho do AWS Glue.	Na seção ETL do console do AWS Glue, adicione	Desenvolvedor, nuvem ou dados

Tarefa	Descrição	Habilidades necessárias
	uma tarefa do AWS Glue. Selecione o tipo de trabalho apropriado, a versão do AWS Glue e o tipo de DPU/ operador correspondente e o número de operadores. Consulte a seção Configura ção para obter detalhes.	
Alterar os locais de entrada e saída.	Copie o código correspon dente ao seu trabalho do AWS Glue e altere o local de entrada e saída que você anotou no épico Upload dos dados.	Desenvolvedor, nuvem ou dados

Tarefa	Descrição	Habilidades necessárias
Configurar os parâmetros.	Você pode usar os trechos fornecidos na seção Informações adicionais para definir parâmetros para seu trabalho de ETL. O AWS Glue usa quatro nomes de argumentos internamente: • `--conf` • `--debug` • `--mode` • `--JOB_NAME` O parâmetro `--JOB_NAME` deve ser inserido explicitamente no console do AWS Glue. Escolha Trabalhos, Editar trabalho, Configuração de segurança, bibliotecas de scripts e parâmetros do trabalho (opcional). Insira `--JOB_NAME` como chave e forneça um valor. Você também pode usar a AWS Command Line Interface (AWS CLI) da AWS ou a API do AWS Glue para definir esse parâmetro. O parâmetro `--JOB_NAME` é usado pelo Spark e não é necessário em um trabalho do ambiente shell do Python.	Desenvolvedor, nuvem ou dados

Tarefa	Descrição	Habilidades necessárias
	Você deve adicionar `--` antes de cada nome de parâmetro ; caso contrário, o código não funcionará. Por exemplo, para os trechos de código, os parâmetros de localização devem ser invocados por `--input_loc` e `--output_loc` .	
Executar o trabalho de ETL.	Execute seu trabalho e verifique a saída. Observe quanto espaço foi reduzido em relação ao arquivo original.	Desenvolvedor, nuvem ou dados

Recursos relacionados

Referências

- Apache Spark
- AWS Glue: como funciona
- Preços do AWS Glue

Tutoriais e vídeos

- O que é o AWS Glue?

Mais informações

Perfil do IAM

Ao criar os trabalhos do AWS Glue, você pode usar um perfil existente do IAM que tenha as permissões mostradas no seguinte trecho de código ou uma nova função.

Use o seguinte código YAML para criar um novo perfil.

```
# (c) 2022 Amazon Web Services, Inc. or its affiliates. All Rights Reserved. This AWS
 Content is provided subject to the terms of the AWS Customer
# Agreement available at https://aws.amazon.com/agreement/ or other written agreement
 between Customer and Amazon Web Services, Inc.

AWSTemplateFormatVersion: "2010-09-09"

Description: This template will setup IAM role for AWS Glue service.

Resources:
  rGlueRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "glue.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole
      Policies:
        - PolicyName: !Sub "${AWS::StackName}-s3-limited-read-write-inline-policy"
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - "s3:PutObject"
                  - "s3:GetObject"
                Resource: "arn:aws:s3:::*/*"
      Tags:
        - Key  : "Name"
          Value : !Sub "${AWS::StackName}"

Outputs:
  oGlueRoleName:
    Description: AWS Glue IAM role
    Value:
      Ref: rGlueRole
```

```
    Export:
      Name: !Join [ ":", [ !Ref "AWS::StackName", rGlueRole ] ]
```

Phyton shell do AWS Glue

O código Python usa os Pandas e as PyArrow bibliotecas para converter dados em Parquet. A biblioteca Pandas já está disponível. A PyArrow biblioteca é baixada quando você executa o padrão, porque é uma execução única. Você pode usar arquivos de roda PyArrow para converter em uma biblioteca e fornecer o arquivo como um pacote de biblioteca. Para obter mais informações sobre empacotamento de arquivos wheel, consulte Fornecer sua própria biblioteca Python.

Parâmetros do Python shell do AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["input_loc", "output_loc"])
```

Código do Phyton shell do AWS Glue

```
from io import BytesIO
import pandas as pd
import boto3
import os
import io
import site
from importlib import reload
from setuptools.command import easy_install
install_path = os.environ['GLUE_INSTALLATION']
easy_install.main( ["--install-dir", install_path, "pyarrow"] )
reload(site)
import pyarrow


input_loc = "s3://bucket-name/prefix/sample_data.csv"
output_loc = "s3://bucket-name/prefix/"


input_bucket = input_loc.split('/', 1)[0]
object_key = input_loc.split('/', 1)[1]


output_loc_bucket = output_loc.split('/', 1)[0]
```

```
output_loc_prefix = output_loc.split('/', 1)[1]


s3 = boto3.client('s3')
obj = s3.get_object(Bucket=input_bucket, Key=object_key)
df = pd.read_csv(io.BytesIO(obj['Body'].read()))


parquet_buffer = BytesIO()
s3_resource = boto3.resource('s3')
df.to_parquet(parquet_buffer, index=False)
s3_resource.Object(output_loc_bucket, output_loc_prefix +  'data' +
 '.parquet').put(Body=parquet_buffer.getvalue())
```

Trabalho do AWS Glue Spark com Python

Para usar um tipo de trabalho do AWS Glue Spark com Python, escolha Spark como tipo de trabalho. Escolha o Spark 3.1, Python 3 com melhor tempo de startup do trabalho (Glue versão 3.0) como a versão do AWS Glue.

Parâmetros do Python do AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["JOB_NAME", "input_loc", "output_loc"])
```

Trabalho do AWS Glue Spark com código Python

```
import sys
from pyspark.context import SparkContext
from awsglue.context import GlueContext
from awsglue.transforms import *
from awsglue.dynamicframe import DynamicFrame
from awsglue.utils import getResolvedOptions
from awsglue.job import Job


sc = SparkContext()
glueContext = GlueContext(sc)
spark = glueContext.spark_session
job = Job(glueContext)
```

```
input_loc = "s3://bucket-name/prefix/sample_data.csv"
output_loc = "s3://bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(\
    connection_type = "s3", \
    connection_options = {
        "paths": [input_loc]}, \
    format = "csv",
    format_options={
        "withHeader": True,
        "separator": ","
    })


outputDF = glueContext.write_dynamic_frame.from_options(\
    frame = inputDyf, \
    connection_type = "s3", \
    connection_options = {"path": output_loc \
        }, format = "parquet")
```

Para um grande número de arquivos grandes compactados (por exemplo, 1.000 arquivos com cerca de 3 MB cada), use o parâmetro `compressionType` com o parâmetro `recurse` para ler todos os arquivos que estão disponíveis dentro do prefixo, conforme mostrado no código a seguir.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Para um grande número de arquivos pequenos compactados (por exemplo, 1.000 arquivos cada um com cerca de 133 KB), use o parâmetro `groupFiles` junto com os parâmetros `compressionType` e os parâmetros `recurse`. O parâmetro `groupFiles` agrupa arquivos pequenos em vários arquivos grandes e o parâmetro `groupSize` controla o agrupamento no tamanho especificado em bytes (por exemplo, 1 MB). O trecho de código a seguir fornece um exemplo do uso desses parâmetros no código.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                           "groupFiles" :"inPartition",
 "groupSize" :"1048576",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Sem nenhuma alteração nos nós de processamento, essas configurações permitem que o trabalho do AWS Glue leia vários arquivos (grandes ou pequenos, com ou sem compactação) e os grave no destino no formato Parquet.

Trabalho do AWS Glue Spark com Scala

Para usar um tipo de trabalho do AWS Glue Spark com Scala, escolha Spark como tipo de trabalho e Linguagem como Scala. Escolha o Spark 3.1, Scala 2 com melhor tempo de startup do trabalho (Glue versão 3.0) como a versão do AWS Glue. Para economizar espaço de armazenamento, o seguinte exemplo do AWS Glue com Scala também usa o atributo `applyMapping` para converter tipos de dados.

Parâmetros do AWS Glue Scala

```
import com.amazonaws.services.glue.util.GlueArgParser val args =
 GlueArgParser.getResolvedOptions(sysArgs, Seq("JOB_NAME", "inputLoc",
 "outputLoc").toArray)
```

Trabalho do AWS Glue Spark com código Scala

```
import com.amazonaws.services.glue.GlueContext
import com.amazonaws.services.glue.MappingSpec
import com.amazonaws.services.glue.DynamicFrame
import com.amazonaws.services.glue.errors.CallSite
import com.amazonaws.services.glue.util.GlueArgParser
import com.amazonaws.services.glue.util.Job
import com.amazonaws.services.glue.util.JsonOptions
```

```
import org.apache.spark.SparkContext
import scala.collection.JavaConverters._


object GlueScalaApp {
  def main(sysArgs: Array[String]) {

    @transient val spark: SparkContext = SparkContext.getOrCreate()
    val glueContext: GlueContext = new GlueContext(spark)

    val inputLoc = "s3://bucket-name/prefix/sample_data.csv"
    val outputLoc = "s3://bucket-name/prefix/"

    val readCSV = glueContext.getSource("csv", JsonOptions(Map("paths" ->
 Set(inputLoc)))).getDynamicFrame()

    val applyMapping = readCSV.applyMapping(mappings = Seq(("_c0", "string", "date",
 "string"), ("_c1", "string", "sales", "long"),
    ("_c2", "string", "profit", "double")), caseSensitive = false)

    val formatPartition = applyMapping.toDF().coalesce(1)

    val dynamicFrame = DynamicFrame(formatPartition, glueContext)

    val dataSink = glueContext.getSinkWithFormat(
        connectionType = "s3",
        options = JsonOptions(Map("path" -> outputLoc )),
        transformationContext = "dataSink", format =
 "parquet").writeDynamicFrame(dynamicFrame)
  }
}
```

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Visualize os logs de auditoria do Amazon Redshift usando o Amazon Athena e o Amazon QuickSight

Criado por Sanket Sirsikar (AWS) e Gopal Krishna Bhatia (AWS)

Resumo

A segurança é parte integrante das operações de banco de dados na Amazon Web Services (AWS) Cloud. Sua organização deve garantir o monitoramento das atividades e conexões dos usuários do banco de dados para detectar possíveis incidentes e riscos de segurança. Esse padrão ajuda a monitorar os seus bancos de dados para fins de segurança e solução de problemas, que é um processo conhecido como auditoria de banco de dados.

Esse padrão fornece um script SQL que automatiza a criação de uma tabela e visualizações do Amazon Athena para um painel de relatórios na Amazon que ajuda você a auditar os logs do QuickSight Amazon Redshift. Isso garante que os usuários responsáveis pelo monitoramento das atividades do banco de dados tenham acesso conveniente aos recursos de segurança de dados.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um cluster existente do Amazon Redshift. Para obter mais informações , consulte Criar um cluster do Amazon Redshift na documentação do Amazon Redshift.
- Acesso a um grupo de trabalho existente do Athena. Para obter mais informações, consulte Como os grupos de trabalho funcionam na documentação do Amazon Athena.
- Um bucket de origem do Amazon Simple Storage Service (Amazon S3) existente com as permissões necessárias do AWS Identity and Access Management (IAM) necessárias. Para obter mais informações, consulte Permissões de bucket para o registro em log do Amazon Redshift do Registro em log do banco de dados e auditoria na documentação do Amazon Redshift.

Arquitetura

Pilha de tecnologia

- Athena
- Amazon Redshift
- Amazon S3
- QuickSight

Ferramentas

- O Amazon Athena: o Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão.
- Amazon QuickSight — QuickSight é um serviço de inteligência de negócios (BI) escalável, sem servidor, incorporável e baseado em aprendizado de máquina.
- Amazon Redshift: o Amazon Redshift é um serviço de data warehousing em escala de petabytes e em nível empresarial totalmente gerenciado.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet.

Épicos

Configurar o cluster do Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Habilitar o registro em log de auditoria para o cluster do Amazon Redshift.	1. Faça login no Console de Gerenciamento da AWS, abra o console do Amazon Redshift, escolha CLUSTERS e, em seguida, escolha o cluster para o qual você deseja habilitar o registro em log. 2. Escolha a guia Proprieda des e habilite auditoria seguindo as instruções em Configuração da auditoria usando o console na	DBA, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	documentação do Amazon Redshift.	

Tarefa	Descrição	Habilidades necessárias
Ative o registro em log no grupo de parâmetros de cluster do Amazon Redshift.	Você pode habilitar a auditoria de logs de conexão, logs de usuário e logs de atividade de usuário ao mesmo tempo usando o Console de Gerenciamento da AWS, a referência de API do Amazon Redshift ou a AWS Command Line Interface (AWS CLI). Para auditorar os logs de atividade do usuário, você também deve habilitar o parâmetro `enable_user_activity_logging` do banco de dados. Se você habilitar somente o atributo de registro em log da auditoria, mas não o parâmetro associado, os logs de auditoria do banco de dados registram em log as informações de conexão e de usuários, mas não os logs de atividades do usuário. O parâmetro `enable_user_activity_logging` não está ativado por padrão, mas você pode ativá-lo alterando-o de `false` para `true`.	DBA, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	Important Você precisa criar um novo grupo de parâmetros de cluster com o `user_activity_logging` parâmetro ativado e anexá-lo ao seu cluster do Amazon Redshift. Para obter mais informações , consulte Modificar um cluster na documentação do Amazon Redshift. Para obter mais informações sobre essa tarefa, consulte Grupos de parâmetros do Amazon Redshift e Configuração da auditoria usando o console na documentação do Amazon Redshift.	

Tarefa	Descrição	Habilidades necessárias
Configure permissões de bucket do S3 para registro em log de cluster do Amazon Redshift.	Quando você ativa o registro em log, o Amazon Redshift coleta informações de registro em log e as carrega para os arquivos de log armazenados no bucket do S3. Você pode criar um bucket do S3 novo ou usar um existente. **Important** Certifique-se de que o Amazon Redshift tenha as permissões do IAM necessárias para acessar o bucket do S3. Para obter mais informações, consulte Permissões de bucket para o registro em log de auditoria do Amazon Redshift do Registro em log de auditoria do banco de dados na documentação do Amazon Redshift.	DBA, engenheiro de dados

Criar a tabela e as visualizações do Athena

Tarefa	Descrição	Habilidades necessárias
Criar a tabela e as visualizações do Athena para consultar	Abra o console do Amazon Athena e use a consulta da	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
os dados do log de auditoria do Amazon Redshift no bucket do S3.	linguagem de definição de dados (DDL) do script SQL `AuditLogging.sql` (em anexo) para criar a tabela e as visualizações dos registros de atividades do usuário, logs do usuário e logs de conexão. Para obter mais informações e instruções, consulte o tutorial Criar tabelas e executar consultas do Amazon Athena Workshop.	

Configure o monitoramento de registros no QuickSight painel

Tarefa	Descrição	Habilidades necessárias
Crie um QuickSight painel usando o Athena como fonte de dados.	Abra o QuickSight console da Amazon e crie um QuickSight painel seguindo as instruções no tutorial Visualize QuickSight usando o Athena do Amazon Athena Workshop.	DBA, engenheiro de dados

Recursos relacionados

- Criar tabelas e executar consultas no Athena.
- Visualize QuickSight usando o Athena

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Visualize relatórios de credenciais do IAM para todas as contas da AWS usando a Amazon QuickSight

Criado por Parag Nagwekar (AWS) e Arun Chandapillai (AWS)

Resumo

> **Warning**
>
> Os usuários do IAM têm credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

É possível usar os relatórios de credenciais do AWS Identity and Access Management (IAM) para ajudar você a atender aos requisitos de segurança, auditoria e conformidade da organização. Os relatórios de credenciais fornecem uma lista de todos os usuários em suas contas da AWS e mostram o status de suas credenciais, como senhas, chaves de acesso e dispositivos com autenticação multifator (MFA). Você pode usar relatórios de credenciais para várias contas da AWS gerenciadas pelo AWS Organizations.

Esse padrão inclui etapas e códigos para ajudar você a criar e compartilhar relatórios de credenciais do IAM para todas as contas da AWS em sua organização usando QuickSight painéis da Amazon. Você pode compartilhar os painéis com as partes interessadas em sua organização. Os relatórios podem ajudar sua organização a alcançar os seguintes resultados comerciais específicos:

- Identificar incidentes de segurança relacionados aos usuários do IAM
- Acompanhar a migração em tempo real de usuários do IAM para autenticação única (SSO)
- Rastrear regiões da AWS acessadas por usuários do IAM
- Manter-se em conformidade
- Compartilhar informações com outras partes interessadas

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- As contas de membros da organização.
- Um perfil do IAM com permissões para acessar contas em Organizations
- AWS Command Line Interface (AWS CLI) versão 2, instalada e configurada
- Uma assinatura da edição Amazon QuickSight Enterprise

Arquitetura

Pilha de tecnologia

- Amazon Athena
- Amazon EventBridge
- Amazon QuickSight
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS Organizations

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para configurar um fluxo de trabalho que captura dados de relatórios de credenciais do IAM de várias contas da AWS.

1. EventBridge invoca uma função Lambda diariamente.
2. A função do Lambda assume um perfil do IAM em todas as contas da AWS em toda a organização. Em seguida, a função cria o relatório de credenciais do IAM e armazena os dados do relatório em um bucket do S3 centralizado. É necessário habilitar a criptografia e desabilitar o acesso público no bucket do S3.

3. Um crawler do AWS Glue rastreia o bucket do S3 diariamente e atualiza a tabela do Athena adequadamente.
4. QuickSight importa e analisa os dados do relatório de credenciais e cria um painel que pode ser visualizado e compartilhado com as partes interessadas.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, funções do Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras contas da AWS.
- QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Código

O código desse padrão está disponível no GitHub getiamcredsreport-allaccounts-orgrepositório. Você pode usar o código desse repositório para criar relatórios de credenciais do IAM em todas as contas da AWS em Organizations e armazená-los em um local central.

Épicos

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Configure a edição Amazon QuickSight Enterprise.	1. Ative a edição Amazon QuickSight Enterprise em sua conta da AWS. Para obter mais informações, consulte Gerenciando o acesso do usuário dentro da Amazon QuickSight na QuickSight documentação. 2. Para conceder permissões de painel, obtenha o Amazon Resource Name (ARN) dos QuickSight usuários.	Administrador da AWS, AWS DevOps, administrador de nuvem, arquiteto de nuvem
Integre a Amazon QuickSight com o Amazon S3 e o Athena.	Você deve QuickSight autorizar o uso do Amazon S3 e do Athena antes de implantar a pilha da AWS. CloudFormation	Administrador da AWS, AWS DevOps, administrador de nuvem, arquiteto de nuvem

Implante a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	1. Clone o GitHub getiamcredsreport-allaccounts-orgrepositório em sua máquina local executando o seguinte comando: `git clone https://g`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`ithub.com/aws-samples/getiamcredsreport-allaccounts-org`	

Tarefa	Descrição	Habilidades necessárias
Implantar a infraestrutura.	1. Faça login no Console de Gerenciamento da AWS e abra o console do CloudFormation . 2. No painel de navegação , escolha Criar pilha e, em seguida, escolha Com novos recursos (padrão). 3. Na página Identificar recursos, escolha Próximo. 4. Na página Especificar modelo, em Origem do modelo, selecione Carregar um arquivo de modelo. 5. Escolha Escolher arquivo, selecione o **`Cloudformation-createcredrepo.yaml`** arquivo do seu GitHub repositório clonado e escolha Avançar. 6. Em Parâmetros, atualize `IAMRoleName` com seu perfil do IAM. Esse deve ser o perfil do IAM que você deseja que o Lambda assuma em todas as contas da organização. Essa função cria o relatório de credenciais. Observação: a função não precisa estar presente em todas as contas nesta etapa da criação da pilha.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	7. Em Parâmetros, atualize `S3BucketName` com o nome do bucket do S3 em que o Lambda pode armazenar as credenciais de todas as contas. 8. Em Nome da pilha, insira o nome da pilha. 9. Selecione Enviar. 10. Observe o nome da função do Lambda.	
Criar uma política de permissão do IAM.	Crie uma política do IAM para cada conta da AWS em sua organização com as seguintes permissões: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:GenerateCredentialReport", "iam:GetCredentialReport" ], "Resource": "*" } ] }`	AWS DevOps, administrador de nuvem, arquiteto de nuvem, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias

Crie um perfil do IAM com uma política de confiança.	1. Crie um perfil do IAM para as contas da AWS e anexe a política de permissão que você criou na etapa anterior.
	2. Anexe ao perfil do IAM a política de confiança a seguir:
	
	`{ "Version":"2012-10-17", "Statement":[ { "Effect": "Allow", "Principal":{ "AWS":[ "arn:aws:iam::<MasterAccountID>:role/<LambdaRole>" ] }, "Action": "sts:AssumeRole" } ] }`
	
	Important
	`arn:aws:iam::<MasterAccountID>:role/<LambdaRo`
		Administrador de nuvem, arquiteto de nuvem, Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`le>` Substitua pelo ARN da função do Lambda que você anotou anteriormente. **Note** As organizações normalmente usam a automação para criar funções do IAM para suas contas da AWS. Recomendamos o uso dessa automação, se disponível. Como alternativa, você pode usar o script `CreateRoleforOrg.py` do repositório de código. O script exige uma função administrativa existente ou qualquer outro perfil do IAM que tenha permissão para criar uma política e um perfil do IAM em cada conta da AWS.	

Tarefa	Descrição	Habilidades necessárias
Configure QuickSight a Amazon para visualizar os dados.	1. Faça login QuickSight com suas credenciais. 2. Crie um conjunto de dados usando o Athena (usando o banco de dados `iamcredreportdb` e a tabela `“cfn_iamcredreport”`) e, em seguida, automaticamente atualize o conjunto de dados . 3. Crie uma análise em QuickSight. 4. Crie um QuickSight painel.	AWS DevOps, administrador de nuvem, arquiteto de nuvem, engenheiro de dados

Mais informações

Considerações adicionais

Considere o seguinte:

- Depois de CloudFormation implantar a infraestrutura, você pode esperar para que os relatórios sejam criados no Amazon S3 e analisados pelo Athena até que o Lambda e o AWS Glue sejam executados de acordo com seus cronogramas. Como alternativa, você pode executar o Lambda manualmente para obter os relatórios no Amazon S3 e, em seguida, executar o crawler AWS Glue para obter a tabela do Athena criada a partir dos dados.
- QuickSight é uma ferramenta poderosa para analisar e visualizar dados com base nos requisitos da sua empresa. Você pode usar parâmetros QuickSight para controlar os dados do widget com base nos campos de dados que você escolher. Além disso, você pode usar uma QuickSight análise para criar parâmetros (por exemplo, campos Conta, Data e Usuário`partition_0`, como, `epartition_1`, `user` respectivamente) do seu conjunto de dados para adicionar controles aos parâmetros de Conta, Data e Usuário.
- Para criar seus próprios QuickSight painéis, consulte QuickSight Workshops no site do AWS Workshop Studio.

- Para ver exemplos de QuickSight painéis, consulte o repositório GitHub getiamcredsreport-allaccounts-orgde códigos.

Resultados de negócios desejados

Você pode usar este padrão para alcançar os resultados comerciais desejados a seguir:

- Identificar incidentes de segurança relacionados aos usuários do IAM: investigue cada usuário em todas as contas da AWS em sua organização usando um único painel de controle. Você pode acompanhar a tendência das regiões individuais da AWS acessadas mais recentemente por um usuário do IAM e dos serviços que eles usaram.
- Acompanhar a migração em tempo real dos usuários do IAM para a autenticação de SSO : ao usar o SSO, os usuários podem fazer login uma vez com uma única credencial e acessar várias contas e aplicativos da AWS. Se você planeja migrar seus usuários do IAM para o SSO, este padrão pode ajudá-lo a fazer a transição para o SSO e monitorar todo o uso de credenciais de usuário do IAM (como acesso ao Console de Gerenciamento da AWS ou uso de chaves de acesso) em todas as contas da AWS.
- Rastrear as regiões da AWS acessadas pelos usuários do IAM: você pode controlar o acesso de usuário do IAM às regiões para vários fins, como soberania de dados e controle de custos. Você também pode monitorar o uso de regiões por qualquer usuário do IAM.
- Manter-se em conformidade: ao seguir o princípio do privilégio mínimo, você pode conceder somente as permissões específicas do IAM necessárias para realizar uma tarefa específica. Além disso, você pode monitorar o acesso aos serviços da AWS, ao Console de Gerenciamento da AWS e o uso de credenciais de longo prazo.
- Compartilhar informações com outras partes interessadas: você pode compartilhar painéis selecionados com outras partes interessadas, sem conceder a elas acesso a relatórios de credenciais do IAM ou contas da AWS.

Mais padrões

- Autentique os usuários existentes do aplicativo React usando o Amazon Cognito e a interface do usuário do AWS Amplify
- Extraia automaticamente conteúdo de arquivos PDF usando o Amazon Textract
- Crie um modelo de previsão de inicialização a frio usando o DeepAR para séries temporais no SageMaker Amazon AI Studio Lab
- Crie relatórios detalhados de custo e uso para clusters do Amazon EMR usando o Explorador de Custos da AWS
- Crie relatórios detalhados de custos e uso para o Amazon RDS e o Amazon Aurora
- Crie relatórios detalhados de custo e uso para trabalhos do AWS Glue usando o Explorador de Custos da AWS
- Implante um trabalho do AWS Glue com um pipeline de CodePipeline CI/CD da AWS
- Incorpore um QuickSight painel da Amazon em um aplicativo Angular local
- Garanta que um cluster do Amazon Redshift seja criptografado na criação
- Garanta que a criptografia para dados em repouso do Amazon EMR esteja habilitada no lançamento
- Estime os custos de armazenamento de uma tabela do Amazon DynamoDB
- Execute consultas SQL do Amazon Redshift usando o Terraform
- Extraia e consulte atributos de AWS IoT SiteWise metadados em um data lake
- Gere insights de dados usando o AWS Mainframe Modernization e o Amazon Q em QuickSight
- Gere insights de dados do Db2 z/OS usando o AWS Mainframe Modernization Amazon Q em QuickSight
- Conceda às instâncias do SageMaker notebook acesso temporário a um CodeCommit repositório em outra conta da AWS
- Identifique e alerte quando os recursos do Amazon Data Firehose não estiverem criptografados com uma chave AWS KMS
- Importe a biblioteca psycopg2 para interagir com seu banco AWS Lambda de dados PostgreSQL
- Ingira e analise os registros de segurança da AWS no Microsoft Sentinel
- Migre o Amazon RDS para Oracle para o Amazon RDS para PostgreSQL no modo SSL usando o AWS DMS

- Migre um banco de dados Oracle para o Amazon RDS for Oracle usando adaptadores de arquivo simples GoldenGate Oracle
- Migre um banco de dados Oracle para o Amazon Redshift usando o AWS DMS e o AWS SCT
- Migre dados de um ambiente Hadoop local para o Amazon S3 usando com a AWS para o Amazon S3 DistCp PrivateLink
- Migre do Couchbase Server para o Couchbase Capella na AWS
- Migre workloads on-premises da Cloudera para a Cloudera Data Platform na AWS
- Monitorar clusters do Amazon EMR para criptografia em trânsito na execução
- Gerencie o failover Multi-AZ para clusters do EMR usando o Application Recovery Controller
- Automatize implantações azul/verdes dos bancos de dados globais Amazon Aurora usando princípios de IaC
- Provisione AWS Service Catalog produtos com base em AWS CloudFormation modelos usando GitHub Ações
- Execute testes de unidade para trabalhos de ETL do Python AWS Glue usando a estrutura pytest
- Configure um painel de monitoramento da Grafana para a AWS ParallelCluster
- Descarregue dados de um cluster do Amazon Redshift entre contas para o Amazon S3
- Verificar se os novos clusters do Amazon Redshift têm os endpoints SSL necessários
- Verificar se os novos clusters do Amazon Redshift são executados em uma VPC
- Visualize os resultados do modelo de IA/ML usando o Flask e o AWS Elastic Beanstalk

Computação

Tópicos

- Contêineres e microsserviços
- Sem servidor
- Redes
- Entrega de conteúdo

Contêineres e microsserviços

Tópicos

- Acesse um banco de dados Amazon Neptune a partir de um contêiner Amazon EKS
- Acesse aplicativos de contêineres de forma privada no Amazon ECS usando a AWS PrivateLink e um Network Load Balancer
- Acesse aplicativos de contêineres de forma privada no Amazon ECS usando o AWS Fargate, a PrivateLink AWS e um Network Load Balancer
- Acesse aplicativos de contêineres de forma privada no Amazon EKS usando a AWS PrivateLink e um Network Load Balancer
- Ativar mTLS no AWS App Mesh usando a AWS Private CA no Amazon EKS
- Automatize backups para instâncias de banco de dados do Amazon RDS para PostgreSQL usando o AWS Batch
- Automatize a implantação do Manipulador do término do nó no Amazon EKS usando um pipeline de CI/CD
- Compilar e implantar automaticamente uma aplicação em Java no Amazon EKS usando um pipeline de CI/CD
- Crie uma definição de tarefa do Amazon ECS e monte um sistema de arquivos em EC2 instâncias usando o Amazon EFS
- Implantar funções do Lambda com imagens de contêiner
- Implante microsserviços Java no Amazon ECS usando o AWS Fargate
- Implante recursos e pacotes do Kubernetes usando o Amazon EKS e um repositório de charts do Helm no Amazon S3
- Implante um exemplo de microsserviço Java no Amazon EKS e exponha o microsserviço usando um Application Load Balancer
- Implante um aplicativo em cluster no Amazon ECS usando o AWS Copilot
- Implemente um aplicativo baseado em gRPC em um cluster Amazon EKS e acesse-o com um Application Load Balancer
- Implantar e depure clusters do Amazon EKS
- Implantar contêineres usando o Elastic Beanstalk
- Gere um endereço IP de saída estático usando uma função do Lambda, Amazon VPC e uma arquitetura de tecnologia sem servidor

- Identifique automaticamente imagens de contêineres duplicadas ao migrar para um repositório Amazon ECR
- Instale o agente SSM nos nós de trabalho do Amazon EKS usando o Kubernetes DaemonSet
- Instale o agente SSM e o CloudWatch agente nos nós de trabalho do Amazon EKS usando preBootstrapCommands
- Migre os controladores de entrada NGINX ao ativar o modo automático do Amazon EKS
- Migre suas cargas de trabalho de contêiner do Azure Red Hat OpenShift (ARO) para Serviço Red Hat OpenShift na AWS (ROSA)
- Otimizar imagens do Docker geradas pelo AWS App2Container
- Coloque pods do Kubernetes no Amazon EKS usando afinidade de nó, taints e tolerâncias
- Replique imagens filtradas de contêineres do Amazon ECR entre contas ou regiões
- Alternar as credenciais do banco de dados sem reiniciar os contêineres
- Execute tarefas do Amazon ECS na Amazon WorkSpaces com o Amazon ECS Anywhere
- Execute um contêiner Docker da API web ASP.NET Core em uma instância Amazon Linux EC2
- Executar workloads orientadas por mensagens em grande escala usando o AWS Fargate
- Executar workloads monitoradas com armazenamento de dados persistente usando o Amazon EFS no Amazon EKS com o AWS Fargate
- Configure o escalonamento automático orientado por eventos no Amazon EKS usando o Amazon EKS Pod Identity e o KEDA
- Simplifique as implantações do PostgreSQL no Amazon EKS usando o PGO
- Simplifique a autenticação de aplicativos com TLS mútuo no Amazon ECS usando o Application Load Balancer
- Mais padrões

Acesse um banco de dados Amazon Neptune a partir de um contêiner Amazon EKS

Criado por Ramakrishnan Palaninathan (AWS)

Resumo

Esse padrão estabelece uma conexão entre o Amazon Neptune, que é um banco de dados gráfico totalmente gerenciado, e o Amazon Elastic Kubernetes Service (Amazon EKS), um serviço de orquestração de contêineres, para acessar um banco de dados Neptune. Os clusters de banco de dados Neptune estão confinados em uma nuvem privada virtual (VPC) ativada. AWS Por esse motivo, acessar o Neptune exige uma configuração cuidadosa da VPC para permitir a conectividade.

Ao contrário do Amazon Relational Database Service (Amazon RDS) para PostgreSQL, o Neptune não depende de credenciais típicas de acesso ao banco de dados. Em vez disso, ele usa funções AWS Identity and Access Management (IAM) para autenticação. Portanto, conectar-se ao Neptune a partir do Amazon EKS envolve a configuração de uma função do IAM com as permissões necessárias para acessar o Neptune.

Além disso, os endpoints do Neptune são acessíveis somente na VPC em que o cluster reside. Isso significa que você precisa definir as configurações de rede para facilitar a comunicação entre o Amazon EKS e o Neptune. Dependendo de seus requisitos específicos e preferências de rede, existem várias abordagens para configurar a VPC para permitir uma conectividade perfeita entre o Neptune e o Amazon EKS. Cada método oferece vantagens e considerações distintas, que fornecem flexibilidade na criação da arquitetura do banco de dados para atender às necessidades do seu aplicativo.

Pré-requisitos e limitações

Pré-requisitos

- Instale a versão mais recente do kubectl (veja as instruções). Para verificar sua versão, execute:

```
kubectl version --short
```

- Instale a versão mais recente do eksctl (veja as instruções). Para verificar sua versão, execute:

```
eksctl info
```

- Instale a versão mais recente da AWS Command Line Interface (AWS CLI) versão 2 (consulte as instruções). Para verificar sua versão, execute:

```
aws --version
```

- Crie um cluster de banco de dados Neptune (consulte as instruções). Certifique-se de estabelecer comunicações entre a VPC do cluster e o Amazon EKS por meio de emparelhamento de VPC ou outro método. AWS Transit Gateway Verifique também se o status do cluster está “disponível” e se ele tem uma regra de entrada na porta 8182 para o grupo de segurança.
- Configure um provedor IAM OpenID Connect (OIDC) em um cluster Amazon EKS existente (consulte as instruções).

Versões do produto

- Amazon EKS 1.27
- Motor Amazon Neptune versão 1.3.0.0 (2023-11-15)

Arquitetura

O diagrama a seguir mostra a conexão entre os pods do Kubernetes em um cluster do Amazon EKS e o Neptune para fornecer acesso a um banco de dados do Neptune.

Automação e escala

Você pode usar o Amazon EKS Horizontal Pod Autoscaler para escalar essa solução.

Ferramentas

Serviços

- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon Neptune é um serviço de banco de dados gráfico que ajuda você a criar e executar aplicativos que funcionam com conjuntos de dados altamente conectados.

Práticas recomendadas

Para obter as melhores práticas, consulte Identity and Access Management nos guias de melhores práticas do Amazon EKS.

Épicos

Definição de variáveis de ambiente

Tarefa	Descrição	Habilidades necessárias
Verifique o contexto do cluster.	Antes de interagir com seu cluster Amazon EKS usando o Helm ou outras ferramentas de linha de comando, você deve definir variáveis de ambiente que encapsulem os detalhes do seu cluster. Essas variáveis são usadas em comandos subsequentes para garantir que elas tenham como alvo o cluster e os recursos corretos. Primeiro, confirme se você está operando no contexto correto do cluster. Isso garante que todos os comandos subsequentes sejam enviados para o cluster Kubernetes pretendido. Para verificar o contexto atual, execute o comando a seguir. `kubectl config current-context`	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Defina a `CLUSTER_NAME` variável.	Defina a variável de `CLUSTER_NAME` ambiente para seu cluster Amazon EKS. No comando a seguir, substitua o valor `us-west-2` da amostra pelo correto Região da AWS para seu cluster. Substitua o valor `eks-workshop` da amostra pelo nome do cluster existente. `export CLUSTER_NAME=$(aws eks describe-cluster --region us-west-2 --name eks-workshop --query "cluster.name" --output text)`	Administrador da AWS, administrador de nuvem
Valide a saída.	Para validar se as variáveis foram definidas corretamente, execute o comando a seguir. `echo $CLUSTER_NAME` Verifique se a saída desse comando corresponde à entrada especificada na etapa anterior.	Administrador da AWS, administrador de nuvem

Crie uma função do IAM e associe-a ao Kubernetes

Tarefa	Descrição	Habilidades necessárias
Criar uma conta de serviço do .	Você usa funções do IAM para contas de serviço para	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	mapear suas contas de serviço do Kubernetes para funções do IAM, a fim de permitir o gerenciamento refinado de permissões para seus aplicativos que são executados no Amazon EKS. Você pode usar eksctl para criar e associar uma função do IAM a uma conta de serviço específica do Kubernete s dentro do seu cluster Amazon EKS. A política AWS gerenciada `NeptuneFu llAccess` permite acesso de gravação e leitura ao cluster Neptune especificado. **Important** Você deve ter um endpoint OIDC associado ao seu cluster antes de executar esses comandos.	
	Crie uma conta de serviço que você deseja associar a uma política AWS gerenciad a chamada`NeptuneFu llAccess` .	

Tarefa	Descrição	Habilidades necessárias

	`eksctl create iamserviceaccount --name eks-neptune-sa --namespace default --cluster $CLUSTER_NAME --attach-policy-arn arn:aws:iam::aws:policy/NeptuneFullAccess --approve --override-existing-serviceaccounts`
	
	onde `eks-neptune-sa` está o nome da conta de serviço que você deseja criar.
	
	Após a conclusão, esse comando exibe a seguinte resposta:
	
	`2024-02-07 01:12:39 [#] created serviceaccount "default/eks-neptune-sa"`	

Tarefa	Descrição	Habilidades necessárias

Verifique se a conta está configurada corretamente.	Certifique-se de que a conta `eks-neptune-sa` de serviço esteja configurada corretamente no namespace padrão do seu cluster.
	`kubectl get sa eks-neptune-sa -o yaml`
	O resultado deve ser semelhante ao seguinte:
	`apiVersion: v1`
	`kind: ServiceAccount`
	`metadata:`
	`  annotations:`
	`  eks.amazonaws.com/role-arn: arn:aws:iam::123456789123:role/eksctl-eks-workshop-addon-iamserviceaccount-d-Role1-Q35yKgdQOlmM`
	`  creationTimestamp: "2024-02-07T01:12:39Z"`
	`  labels:`
	`  app.kubernetes.io/managed-by: eksctl`
	`  name: eks-neptune-sa`
	`  namespace: default`
	`  resourceVersion: "5174750"`
	`  uid: cd6ba2f7-a0f5-40e1-a6f4-4081e0042316`
		Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

Verifique a conectividade.	Implante um pod de amostra chamado `pod-util` e verifique a conectividade com o Neptune.
	
	`apiVersion: v1`
	`kind: Pod`
	`metadata:`
	`  name: pod-util`
	`  namespace: default`
	`spec:`
	`  serviceAccountName:`
	` eks-neptune-sa`
	`  containers:`
	`  - name: pod-util`
	`  image: public.ec`
	`r.aws/patrickc/tro`
	`ubleshoot-util`
	`  command:`
	`  - sleep`
	`  - "3600"`
	`  imagePullPolicy:`
	` IfNotPresent`
	
	`kubectl apply -f pod-`
	`util.yaml`
	
	`kubectl exec --stdin --`
	`tty pod-util -- /bin/`
	`bash`
	`bash-5.1# curl -X POST`
	` -d '{"gremlin":"g.V()`
	`.limit(1)"}' https://`
	`db-neptune-1.cluste`
	`r-xxxxxxxxxxx.us-`
	`west-2.neptune.ama`
	`zonaws.com:8182/gr`
	`emlin`
		Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	`{"requestId":"a4964f2d-12b1-4ed3-8a14-eff511431a0e","status":{"message":"","code":200,"attributes":{"@type":"g:Map","@value":[]},"result":{"data":{"@type":"g:List","@value":[]},"meta":{"@type":"g:Map","@value":[]}}}`
	`bash-5.1# exit`
	`exit`	

Validar a atividade de conexão

Tarefa	Descrição	Habilidades necessárias
Ative a autenticação do banco de dados do IAM.	Por padrão, a autenticação de banco de dados do IAM está desabilitada quando você cria um cluster de banco de dados do Neptune. Você pode ativar ou desativar a autenticação do banco de dados do IAM usando AWS Management Console o. Siga as etapas na AWS documentação para habilitar a autenticação do banco de dados do IAM no Neptune.	Administrador da AWS, administrador de nuvem
Verifique as conexões.	Nesta etapa, você interage com o `pod-util` contêiner, que já está em execução, para	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	instalar o awscurl e verificar a conexão.
	
	1. Execute o comando a seguir para encontrar o pod.
	
	`kubectl get pods`
	
	O resultado deve ser semelhante ao seguinte:
	
	`NAME READY STATUS RESTARTS AGE pod-util 1/1 Running 0 50m`
	
	2. Execute o comando a seguir para instalar o awscurl.
	
	`kubectl exec --stdin --tty pod-util -- /bin/bash bash-5.1# pip3 install awscurl Installing collected packages: idna, configparser, configargparse, charset-normalizer, certifi, requests, awscurl Successfully installed awscurl-0.32 certifi-2024.2.2 charset-normalizer-3.3.2 configargparse-1.7 configparser-6.0.0 idna-3.6 requests-2.31.0`	

Tarefa	Descrição	Habilidades necessárias
	bash-5.1# awscurl https://db-neptune-1.cluster-xxxxxxxxxxxx.us-west-2.neptune.amazonaws.com:8182/status --region us-west-2 --service neptune-db {"status":"healthy","startTime":"Thu Feb 08 01:22:14 UTC 2024","dbEngineVersion":"1.3.0.0.R1","role":"writer","dfeQueryEngine":"viaQueryHint","gremlin":{"version":"tinkerpop-3.6.4"},"sparql":{"version":"sparql-1.1"},"opencypher":{"version":"Neptune-9.0.20190305-1.0"},"labMode":{"ObjectIndex":"disabled","ReadWriteConflictDetection":"enabled"},"features":{"SlowQueryLogs":"disabled","ResultCache":{"status":"disabled"},"IAMAuthentication":"enabled","Streams":"disabled","AuditLog":"disabled"},"settings":{"clusterQueryTimeoutInMs":"120000","SlowQueryLogsThreshold":"5000"}}	

Solução de problemas

Problema	Solução
Não consigo acessar o banco de dados Neptune.	Revise a política do IAM que está anexada à conta de serviço. Certifique-se de que ele permita as ações necessárias (por exemplo,`neptune:Connec,neptune:DescribeDBInstances`) para as operações que você deseja executar.

Recursos relacionados

- Conceda às cargas de trabalho do Kubernetes acesso ao AWS uso de contas de serviço do Kubernetes (documentação do Amazon EKS)
- Funções do IAM para contas de serviço (documentação do Amazon EKS)
- Criação de um novo cluster de banco de dados Neptune (documentação do Amazon Neptune)

Acesse aplicativos de contêineres de forma privada no Amazon ECS usando a AWS PrivateLink e um Network Load Balancer

Criado por Kirankumar Chandrashekar (AWS)

Resumo

Esse padrão descreve como hospedar de forma privada um aplicativo de contêiner Docker no Amazon Elastic Container Service (Amazon ECS) por trás de um Network Load Balancer e acessar o aplicativo usando a AWS. PrivateLink Você pode usar uma rede privada para acessar, de forma segura, serviços na Nuvem do Amazon Web Services (AWS). O Amazon Relational Database Service (Amazon RDS) hospeda os banco de dados relacional para o aplicativo em execução no Amazon ECS com alta disponibilidade (HA). O Amazon Elastic File System (Amazon EFS) é usado se o aplicativo exigir armazenamento persistente.

O serviço Amazon ECS que executa os aplicativos Docker, com um Network Load Balancer no front-end, pode ser associado a um endpoint de nuvem privada virtual (VPC) para acesso por meio da AWS. PrivateLink Esse serviço de VPC endpoint pode então ser compartilhado com outros VPCs usando seus VPC endpoints.

Você também pode usar o AWS Fargate em vez de um grupo do Amazon Auto EC2 Scaling. Para obter mais informações, consulte Acesse aplicativos de contêineres de forma privada no Amazon ECS usando o AWS Fargate, a PrivateLink AWS e um Network Load Balancer.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) versão 2, instalado e configurado no Linux, macOS ou Windows
- Docker, instalado e configurado no Linux, macOS ou Windows
- Um aplicativo em execução no Docker

Arquitetura

Pilha de tecnologia

- Amazon CloudWatch
- Nuvem de computação elástica da Amazon (Amazon EC2)
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS PrivateLink
- AWS Secrets Manager
- Application Load Balancer
- Network Load Balancer
- VPC

Automação e escala

- Você pode usar CloudFormation a AWS para criar esse padrão usando a infraestrutura como código.

Ferramentas

- Amazon EC2 — A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS.
- Amazon EC2 Auto Scaling — O Amazon EC2 Auto Scaling ajuda você a garantir que você tenha o número correto de instâncias da EC2 Amazon disponíveis para lidar com a carga do seu aplicativo.
- Amazon ECS: o Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um serviço de registro de imagem de contêiner, seguro, escalável e confiável.
- Amazon EFS: o Amazon Elastic File System (Amazon EFS) fornece um sistema de arquivos NFS elástico simples, escalável, totalmente gerenciável e pronto para uso com serviços de Nuvem AWS e atributos on-premises.

- AWS Lambda: o AWS Lambda é um serviço de computação com tecnologia para executar código sem provisionamento ou gerenciamento de servidores.
- Amazon RDS: o Amazon Relational Database Service (Amazon RDS) é um serviço Web que facilita a configuração, a operação e escalabilidade de um banco de dados relacional na Nuvem AWS.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet. Ele foi projetado para facilitar a computação de escala na web para os desenvolvedores.
- AWS Secrets Manager: o Secrets Manager permite a substituição de credenciais codificadas no seu código, incluindo senhas, e oferece uma chamada de API para o Secrets Manager para recuperar o segredo de forma programática.
- Amazon VPC: o Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você.
- Elastic Load Balancing — O Elastic Load Balancing distribui o tráfego de entrada de aplicativos ou de rede em vários destinos, como instâncias, contêineres e endereços IP EC2 da Amazon, em várias zonas de disponibilidade.
- Docker: o Docker ajuda os desenvolvedores a empacotar, enviar e executar qualquer aplicativo como um contêiner leve, portátil e autossuficiente.

Épicos

Criar componentes de rede

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. Escolha Criar VPC e escolha VPC e muito mais. 2. Insira um nome para sua VPC e escolha um intervalo de blocos CIDR apropriado. 3. Especifique duas zonas de disponibilidade, duas	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	sub-redes públicas e quatro sub-redes privadas. Duas sub-redes privadas são para tarefas do Amazon ECS e duas sub-redes privadas são para bancos de dados do Amazon RDS. 4. Especifique um gateway NAT para cada zona de disponibilidade. 5. Escolha Criar VPC.	

Criar os balanceadores de carga

Tarefa	Descrição	Habilidades necessárias
Criar um Network Load Balancer.	1. Abra o EC2 console da Amazon e escolha a região da AWS que contém sua VPC. 2. Em Balanceamento de carga, escolha Balancead ores de carga e escolha Criar balanceador de carga. 3. Escolha Network Load Balancer e, em seguida, Criar. 4. Na página Configurar balanceador de carga, configure seu Network Load Balancer e seu receptor. Importante: certifique-se	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	de escolher o esquema do seu Network Load Balancer como Interno. 5. Escolha as configurações de segurança aplicáveis, configure um grupo de segurança e um grupo-alvo. Escolha Instância ou IP como o Tipo de destino na seção Configurar roteamento. Certifique-se de não registrar um alvo. 6. Depois de definir todas as configurações, escolha Avançar: Revisão e, em seguida, escolha Criar.	

Tarefa	Descrição	Habilidades necessárias
Criar um Application Load Balancer.	1. No EC2 console da Amazon, escolha a mesma região que contém sua VPC. 2. Em Balanceamento de carga, escolha Balancead ores de carga e escolha Criar balanceador de carga. 3. Selecione Application Load Balancer e clique em Criar. 4. **Important** Configure seu Application Load Balancer e seu receptor. Certifiqu e-se de escolher o esquema do Application Load Balancer como Interno. 5. Escolha as configurações de segurança aplicávei s, configure um grupo de segurança e um grupo-alv o. Escolha Instância ou IP como o Tipo de destino na seção Configurar roteament o. Certifique-se de não registrar um alvo. 6. Depois de definir todas as configurações, escolha	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Avançar: Revisão e, em seguida, escolha Criar.	

Criar um sistema de arquivos do Amazon EFS

Tarefa	Descrição	Habilidades necessárias
Criar um sistema de arquivos do Amazon EFS.	1. Abra o console do Amazon EFS e escolha Criar sistema de arquivos. 2. Na caixa de diálogo Criar sistema de arquivos, insira um nome para seu sistema de arquivos e escolha sua VPC. 3. Escolha Criar para criar o sistema de arquivos. 4. Instalar e configurar seu sistema de arquivos do Amazon EFS.	Administrador de nuvem
Monte destinos para as sub-redes.	1. Volte ao console do Amazon EFS e escolha Sistemas de arquivos. A página Sistemas de arquivos mostra os sistemas de arquivos do Amazon EFS em sua conta. 2. Escolha o sistema de arquivos que você criou e escolha Gerenciar para exibir as Zonas de Disponibilidade. Para	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	adicionar um destino de montagem, escolha Adicionar destino de montagem e adicione as quatro sub-redes privadas que você criou.	
Verifique se as sub-redes estão montadas como destinos.	1. No console do Amazon EFS, escolha Sistemas de arquivos. 2. Escolha Rede para exibir a lista de destinos de montagem existentes. Certifique-se de que elas incluam as quatro sub-redes que você criou.	Administrador de nuvem

Criar um bucket do S3.

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Abra o console do Amazon S3 e crie um bucket do S3 para armazenar os ativos estáticos do seu aplicativo, se necessário.	Administrador de nuvem

Crie um segredo do Secrets Manager

Tarefa	Descrição	Habilidades necessárias
Crie uma chave do AWS KMS para criptografar o segredo do Secrets Manager.	Abra o console do AWS Key Management Service (AWS	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	KMS) e crie uma chave do KMS.	
Crie um segredo do Secrets Manager para armazenar a senha do Amazon RDS.	1. Abra o console do AWS Secrets Manager e crie um novo segredo escolhend o escolha Armazenar um novo segredo. 2. Escolha a chave do KMS que você criou e armazene seu novo segredo.	Administrador de nuvem

Criar uma instância de do Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de sub-redes de banco de dados.	1. Crie o console do Amazon RDS e escolha Grupos de sub-rede. 2. Escolha Criar grupo de sub-redes de banco de dados e insira um nome e uma descrição para seu grupo de sub-redes de banco de dados. 3. Escolha a VPC que você criou anteriormente e escolha as zonas de disponibilidade e sub-redes . Escolha Criar.	Administrador de nuvem
Crie uma instância de do Amazon RDS.	Crie e configure uma instância do Amazon RDS nas sub-redes privadas. Certifique-	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	se de que o Multi-AZ esteja ativado para HA.	
Carregue dados na instância do Amazon RDS.	Carregue os dados relaciona is exigidos pelo seu aplicativ o na sua instância do Amazon RDS. Esse processo irá variar dependendo das necessida des do seu aplicativo, bem como de como o esquema do banco de dados é definido e projetado.	Administrador de nuvem, DBA

Criar os componentes do Amazon ECS

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do ECS.	1. Abra o Console do Amazon ECS e selecione Clusters. 2. Escolha Criar clusters e configure um cluster ECS de acordo com as especific ações necessárias.	Administrador de nuvem
Criar as imagens do Docker.	Crie as imagens do Docker seguindo as instruções na seção Recursos relacionados.	Administrador de nuvem
Crie repositórios do Amazon ECR.	1. No console do Amazon ECR, escolha Repositórios. 2. Escolha Criar repositório e insira um nome exclusivo para o seu repositório. 3. Configure o repositório de acordo com suas especific	Administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ações, incluindo criptografia do AWS KMS, se necessário.	
Autentique seu cliente do Docker no repositório do Amazon ECR.	Para autenticar seu cliente Docker para o repositório Amazon ECR, execute o comando “`aws ecr get-login-password` na CLI da AWS.	Administrador de nuvem
Envie imagens do Docker ao repositório do Amazon ECR.	1. Identifique a imagem do Docker que você deseja enviar e execute o comando `docker images` na CLI da AWS. 2. Marque a sua imagem com o registro do Amazon ECR, o repositório e a combinação opcional de nomes de etiquetas da imagem. 3. Envie a imagem do Docker executando o comando`docker push`. 4. Repita essas etapas para todas as imagens necessárias.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar uma definição de tarefa do Amazon ECS.	É necessária uma definição de tarefa para executar contêineres do Docker no Amazon ECS. 1. Retorne ao console do Amazon ECS, escolha Definições de tarefas e, em seguida, escolha Criar nova definição de tarefa. 2. Na página Select compatibilities, selecione o tipo de inicialização que sua tarefa deve usar e escolha Next step. **Important** Para obter ajuda na configuração da definição de tarefa, consulte “Criar uma definição de tarefa” na seção Recursos relacionados. Certifique-se de fornecer as imagens do Docker que você enviou para o Amazon ECR.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um serviço do Amazon ECS.	Crie um serviço do Amazon ECS usando o cluster ECS que você criou anteriormente. Certifique-se de escolher Amazon EC2 como o tipo de lançamento e escolher a definição de tarefa criada na etapa anterior, bem como o grupo-alvo do Application Load Balancer.	Administrador de nuvem

Crie um grupo Amazon EC2 Auto Scaling

Tarefa	Descrição	Habilidades necessárias
Crie uma configuração de ativação.	Abra o EC2 console da Amazon e crie uma configuração de lançamento. Certifique-se de que os dados do usuário tenham o código para permitir que as EC2 instâncias se juntem ao cluster ECS desejado. Para ver um exemplo do código necessário, consulte a seção Recursos relacionados.	Administrador de nuvem
Crie um grupo Amazon EC2 Auto Scaling.	Volte para o EC2 console da Amazon e, em Auto Scaling, escolha grupos de Auto Scaling. Configure um grupo do Amazon EC2 Auto Scaling. Certifique-se de escolher as sub-redes privadas e a	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	configuração de inicialização que você criou anteriormente.	

Configurar a AWS PrivateLink

Tarefa	Descrição	Habilidades necessárias
Configure o PrivateLink endpoint da AWS.	1. No console da Amazon VPC, crie um endpoint da AWS PrivateLink . 2. Associe esse endpoint ao Network Load Balancer, que disponibiliza o aplicativo hospedado no Amazon ECS de forma privada aos clientes. Para obter mais informações, consulte a seção Recursos relacionados.	Administrador de nuvem

Criar um VPC endpoint

Tarefa	Descrição	Habilidades necessárias
Crie um VPC endpoint	Crie um VPC endpoint para o endpoint da AWS que PrivateLink você criou anteriormente. O nome de domínio totalmente qualificado (FQDN) do VPC endpoint apontará para o FQDN do endpoint da AWS. PrivateLi	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	nk Isso cria uma interface de rede elástica para o serviço de endpoint da VPC que os endpoints de DNS podem acessar.	

Criar a função do Lambda

Tarefa	Descrição	Habilidades necessárias
Criar a função do Lambda.	No console do AWS Lambda, crie uma função do Lambda para atualizar os endereços IP do Application Load Balancer como destinos para o Network Load Balancer. Para obter mais informações sobre isso, consulte a postagem do blog Como usar o AWS Lambda para habilitar endereços IP estáticos para Application Load Balancers.	Desenvolvedor de aplicativos

Recursos relacionados

Criar os balanceadores de carga:

- Use um Network Load Balancer para o Amazon ECS
- Criar um Network Load Balancer
- Use um Application Load Balancer para o Amazon ECS
- Criar um Application Load Balancer

Criar um sistema de arquivos do Amazon EFS

- Criar um sistema de arquivos do Amazon EFS
- Crie destinos de montagem no Amazon EFS

Criar um bucket do S3

- Criar um bucket do S3

Criar um segredo do Secrets Manager:

- Crie chaves no AWS KMS
- Criar um segredo no AWS Secrets Manager

Criar uma instância de do Amazon RDS:

- Criar uma instância de banco de dados do Amazon RDS

Criar os componentes do Amazon ECS:

- Criar um cluster do Amazon ECS
- Criar uma imagem do Docker
- Criar um repositório do Amazon ECR
- Autentique o Docker com o repositório do Amazon ECR
- Enviar uma imagem para um repositório do Amazon ECR
- Criar uma definição de tarefa do Amazon ECS
- Criar um serviço do Amazon ECS

Crie um grupo do Amazon EC2 Auto Scaling:

- Criar uma configuração de execução
- Criar um grupo do Auto Scaling usando uma configuração de execução
- Instâncias de contêiner bootstrap com dados de EC2 usuários da Amazon

Configure a AWS PrivateLink:

- Serviços de endpoint de VPC (AWS) PrivateLink

Criar um endpoint da VPC:

- Interface de endpoints VPC (AWS) PrivateLink

Criar a função do Lambda:

- Criar uma função do Lambda

Outros recursos:

- Usando endereços IP estáticos para Application Load Balancers
- Acessando serviços com segurança pela AWS PrivateLink

Acesse aplicativos de contêineres de forma privada no Amazon ECS usando o AWS Fargate, a PrivateLink AWS e um Network Load Balancer

Criado por Kirankumar Chandrashekar (AWS)

Resumo

Esse padrão descreve como hospedar de forma privada um aplicativo de contêiner Docker na nuvem da Amazon Web Services (AWS) usando o Amazon Elastic Container Service (Amazon ECS) com um tipo de lançamento do AWS Fargate, atrás de um Network Load Balancer, e acessar o aplicativo usando a AWS. PrivateLink O Amazon Relational Database Service (Amazon RDS) hospeda os banco de dados relacional para o aplicativo em execução no Amazon ECS com alta disponibilidade (HA). Você pode usar o Amazon Elastic File System (Amazon EFS) se o aplicativo exigir armazenamento persistente.

Esse padrão usa um tipo de lançamento Fargate para o serviço do Amazon ECS executando os aplicativos Docker, com um Network Load Balancer no frontend. Em seguida, ele pode ser associado a um endpoint de nuvem privada virtual (VPC) para acesso por meio da AWS. PrivateLink Esse serviço de VPC endpoint pode então ser compartilhado com outras pessoas VPCs usando seus VPC endpoints.

Você pode usar o Fargate com o Amazon ECS para executar contêineres sem precisar gerenciar servidores ou clusters de instâncias do Amazon Elastic Compute Cloud (Amazon). EC2 Você também pode usar um grupo do Amazon EC2 Auto Scaling em vez do Fargate. Para obter mais informações, consulte Acesse aplicativos de contêineres de forma privada no Amazon ECS usando a AWS PrivateLink e um Network Load Balancer.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) versão 2, instalado e configurado no Linux, macOS ou Windows
- Docker, instalado e configurado no Linux, macOS ou Windows
- Um aplicativo em execução no Docker

Arquitetura

Pilha de tecnologia

- Amazon CloudWatch
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon EFS
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- AWS Fargate
- AWS PrivateLink
- AWS Secrets Manager
- Application Load Balancer
- Network Load Balancer
- VPC

Automação e escala

- Você pode usar CloudFormation a AWS para criar esse padrão usando a infraestrutura como código.

Ferramentas

Serviços da AWS

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres da AWS que é seguro, escalável e confiável.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido que facilita a execução, a parada e o gerenciamento de contêineres em um cluster.
- O Amazon Elastic File System (Amazon EFS) fornece um sistema de arquivos NFS elástico simples, escalável e totalmente gerenciado para uso com serviços de nuvem e recursos locais da AWS.

- AWS Fargateé uma tecnologia que você pode usar com o Amazon ECS para executar contêineres sem precisar gerenciar servidores ou clusters de EC2 instâncias da Amazon.
- O Amazon Relational Database Service (Amazon RDS) é um serviço web que facilita a configuração, a operação e a escalabilidade de um banco de dados relacional no. Nuvem AWS
- O Amazon Simple Storage Service (Amazon S3) é um armazenamento para a Internet. Ele foi projetado para facilitar a computação de escala na web para os desenvolvedores.
- O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar recursos da AWS em uma rede virtual que você definiu.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos, como EC2 instâncias, contêineres e endereços IP, em várias zonas de disponibilidade.

Outras ferramentas

- O Docker ajuda os desenvolvedores a empacotar, enviar e executar facilmente qualquer aplicativo como um contêiner leve, portátil e autossuficiente.

Épicos

Criar componentes de rede

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. Escolha Criar VPC e escolha VPC e muito mais. 2. Insira um nome para sua VPC e escolha um intervalo de blocos CIDR apropriado. 3. Especifique duas zonas de disponibilidade, duas sub-redes públicas e quatro	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	sub-redes privadas. Duas sub-redes privadas são para tarefas do Amazon ECS e duas sub-redes privadas são para bancos de dados do Amazon RDS. 4. Especifique um gateway NAT para cada zona de disponibilidade. 5. Escolha Criar VPC.	

Criar os balanceadores de carga

Tarefa	Descrição	Habilidades necessárias
Criar um Network Load Balancer.	1. Abra o EC2 console da Amazon e escolha a região da AWS que contém sua VPC. 2. Em Balanceamento de carga, escolha Balancead ores de carga e escolha Criar balanceador de carga. 3. Escolha Network Load Balancer e, em seguida, Criar. 4. Na página Configurar balanceador de carga, configure seu Network Load Balancer e seu receptor. Importante: certifique-se de escolher o esquema do	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	seu Network Load Balancer como Interno. 5. Escolha as configurações de segurança aplicáveis, configure um grupo de segurança e um grupo-alvo. Escolha IP como o Tipo de destino na seção Configurar roteamento. Certifique-se de não registrar um alvo. 6. Depois de definir todas as configurações, escolha Avançar: Revisão e, em seguida, escolha Criar. Para obter ajuda com esse e outros artigos, consulte a seção Recursos relacionados.	

Tarefa	Descrição	Habilidades necessárias
Criar um Application Load Balancer.	1. No EC2 console da Amazon, escolha a mesma região que contém sua VPC. 2. Em Balanceamento de carga, escolha Balanceadores de carga e escolha Criar balanceador de carga. 3. Selecione Application Load Balancer e clique em Criar. 4. **Important** Configure seu Application Load Balancer e seu receptor. Certifique-se de escolher o esquema do Application Load Balancer como Interno. 5. Escolha as configurações de segurança aplicáveis, configure um grupo de segurança e um grupo-alvo. Escolha IP como o Tipo de destino na seção Configurar roteamento. Certifique-se de não registrar um alvo. 6. Depois de definir todas as configurações, escolha	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Avançar: Revisão e, em seguida, escolha Criar.	

Criar um sistema de arquivos do Amazon EFS

Tarefa	Descrição	Habilidades necessárias
Criar um sistema de arquivos do Amazon EFS.	1. Abra o console do Amazon EFS e escolha Criar sistema de arquivos. 2. Na caixa de diálogo Criar sistema de arquivos, insira um nome para seu sistema de arquivos e escolha sua VPC. 3. Escolha Criar para criar o sistema de arquivos. 4. Instalar e configurar seu sistema de arquivos do Amazon EFS.	Administrador de nuvem
Monte destinos para as sub-redes.	1. Volte ao console do Amazon EFS e escolha Sistemas de arquivos. A página Sistemas de arquivos mostra os sistemas de arquivos do Amazon EFS em sua conta. 2. Escolha o sistema de arquivos que você criou e escolha Gerenciar para exibir a Zona de Disponibilidade.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	3. Para adicionar um destino de montagem, escolha Adicionar destino de montagem e adicione as quatro sub-redes privadas que você criou.	
Verifique se as sub-redes estão montadas como destinos.	1. No console do Amazon EFS, escolha Sistemas de arquivos. 2. Escolha Rede para exibir a lista de destinos de montagem existentes. Certifique-se de que elas incluam as quatro sub-redes que você criou.	Administrador de nuvem

Criar um bucket do S3.

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Abra o console do Amazon S3 e crie um bucket do S3 para armazenar os ativos estáticos do seu aplicativo, se necessário.	Administrador de nuvem

Crie um segredo do Secrets Manager

Tarefa	Descrição	Habilidades necessárias
Crie uma chave do AWS KMS para criptografar o segredo do Secrets Manager.	Abra o console do AWS Key Management Service (AWS	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	KMS) e crie uma chave do KMS.	
Crie um segredo do Secrets Manager para armazenar a senha do Amazon RDS.	1. Abra o console do AWS Secrets Manager e crie um novo segredo escolhend o escolha Armazenar um novo segredo. 2. Escolha a chave do KMS que você criou e armazene seu novo segredo.	Administrador de nuvem

Criar uma instância de do Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de sub-redes de banco de dados.	1. Abra o console do Amazon RDS e escolha Grupos de sub-rede. 2. Escolha Criar grupo de sub-redes de banco de dados e insira um nome e uma descrição para seu grupo de sub-redes de banco de dados. 3. Escolha a VPC que você criou anteriormente e escolha as zonas de disponibilidade e sub-redes . Escolha Criar.	Administrador de nuvem
Crie uma instância de do Amazon RDS.	Crie e configure uma instância do Amazon RDS nas sub-redes privadas. Certifique-	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	se de que o Multi-AZ esteja ativado para alta disponibi lidade (HA).	
Carregue dados na instância do Amazon RDS.	Carregue os dados relaciona is exigidos pelo seu aplicativ o na sua instância do Amazon RDS. Esse processo irá variar dependendo das necessida des do seu aplicativo, bem como de como o esquema do banco de dados é definido e projetado.	DBA

Criar os componentes do Amazon ECS

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do ECS.	1. Abra o Console do Amazon ECS e selecione Clusters. 2. Escolha Criar clusters e configure um cluster ECS de acordo com as especific ações necessárias.	Administrador de nuvem
Criar as imagens do Docker.	Crie as imagens do Docker seguindo as instruções na AWS documentação.	Administrador de nuvem
Crie um repositório do Amazon ECR.	1. Abra o console do Amazon EC2 e escolha Repositór ios. 2. Escolha Criar repositório e insira um nome exclusivo para o seu repositório.	Administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	3. Configure o repositório de acordo com suas especific ações, incluindo criptografia do AWS KMS, se necessári o.	
Envie imagens do Docker ao repositório do Amazon ECR.	1. Identifique a imagem do Docker que você deseja enviar e execute o comando `docker images` na AWS CLI. 2. Marque a sua imagem com o registro do Amazon ECR, o repositório e a combinaçã o opcional de nomes de etiquetas da imagem. 3. Envie a imagem do Docker executando o comando`docker push`. 4. Repita essas etapas para todas as imagens necessári as.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar uma definição de tarefa do Amazon ECS.	É necessária uma definição de tarefa para executar contêineres do Docker no Amazon ECS. 1. Retorne ao console do Amazon ECS, escolha Definições de tarefas e, em seguida, escolha Criar nova definição de tarefa. 2. Na página Select compatibilities, selecione o tipo de inicialização que sua tarefa deve usar e escolha Next step. **Important** Para obter ajuda na configuração da definição de tarefa, consulte “Criar uma definição de tarefa” na seção Recursos relacionados. Certifique-se de fornecer as imagens do Docker que você enviou para o Amazon ECR.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um serviço do ECS e escolha Fargate como o tipo de lançamento.	1. Crie um serviço Amazon ECS usando o cluster ECS que você criou anteriorm ente. Certifique-se de escolher Fargate como o tipo de lançamento. 2. Escolha a definição de tarefa criada na etapa anterior e escolha o grupo de destino do Application Load Balancer.	Administrador de nuvem

Configurar a AWS PrivateLink

Tarefa	Descrição	Habilidades necessárias
Configure o PrivateLink endpoint da AWS.	1. Abra o console da Amazon VPC e crie um AWS PrivateLink endpoint. 2. Associe esse endpoint ao Network Load Balancer, que disponibiliza o aplicativ o hospedado no Amazon ECS de forma privada aos clientes.	Administrador de nuvem

Criar um VPC endpoint

Tarefa	Descrição	Habilidades necessárias
Crie um VPC endpoint	Crie um VPC endpoint para o endpoint da AWS que PrivateLink você criou	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	anteriormente. O nome de domínio totalmente qualifica do (FQDN) do VPC endpoint apontará para o FQDN do endpoint da AWS. PrivateLi nk Isso cria uma interface de rede elástica para o serviço de endpoint da VPC que os endpoints do Domain Name Service podem acessar.	

Defina o alvo

Tarefa	Descrição	Habilidades necessárias
Adicione o Application Load Balancer como destino.	Para adicionar o Applicati on Load Balancer como destino para o Network Load Balancer, siga as instruções na documentação.AWS	Desenvolvedor de aplicativos

Recursos relacionados

Criar os balanceadores de carga:

- Use um Network Load Balancer para o Amazon ECS
- Criar um Network Load Balancer
- Use um Application Load Balancer para o Amazon ECS
- Criar um Application Load Balancer

Criar um sistema de arquivos do Amazon EFS

- Criar um sistema de arquivos do Amazon EFS

- Crie destinos de montagem no Amazon EFS

Criar um segredo do Secrets Manager:

- Crie chaves no AWS KMS
- Criar um segredo no AWS Secrets Manager

Criar uma instância de do Amazon RDS:

- Criar uma instância de banco de dados do Amazon RDS

Criar os componentes do Amazon ECS

- Criar um repositório do Amazon ECR
- Autentique o Docker com o repositório do Amazon ECR
- Enviar uma imagem para um repositório do Amazon ECR
- Criar uma definição de tarefa do Amazon ECS
- Criar um serviço do Amazon ECS

Outros recursos:

- Acessando serviços com segurança pela AWS PrivateLink

Acesse aplicativos de contêineres de forma privada no Amazon EKS usando a AWS PrivateLink e um Network Load Balancer

Criado por Kirankumar Chandrashekar (AWS)

Resumo

Esse padrão descreve como hospedar de forma privada um aplicativo de contêiner Docker no Amazon Elastic Kubernetes Service (Amazon EKS) por trás de um Network Load Balancer e acessar o aplicativo usando a AWS. PrivateLink Você pode usar uma rede privada para acessar, de forma segura, serviços na Nuvem do Amazon Web Services (AWS).

O cluster Amazon EKS que executa os aplicativos Docker, com um Network Load Balancer no front-end, pode ser associado a um endpoint de nuvem privada virtual (VPC) para acesso por meio da AWS. PrivateLink Esse serviço de VPC endpoint pode então ser compartilhado com outras pessoas VPCs usando seus VPC endpoints.

A configuração descrita por esse padrão é uma forma segura de compartilhar o acesso ao aplicativo VPCs entre contas da AWS. Não requer configurações especiais de conectividade ou roteamento, porque a conexão entre as contas do consumidor e do provedor faz parte da espinha dorsal global da AWS e não atravessa a Internet pública.

Pré-requisitos e limitações

Pré-requisitos

- Docker, instalado e configurado em macOS, Linux ou Windows.
- Um aplicativo em execução no Docker.
- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) versão 2, instalado e configurado no Linux, macOS ou Windows.
- Um cluster Amazon EKS existente com sub-redes privadas marcadas e configurado para hospedar aplicativos. Para obter mais informações, consulte Marcação de sub-rede na documentação do Amazon EKS.
- Kubectl, instalado e configurado para acessar recursos em seu cluster Amazon EKS. Para obter mais informações, consulte Instalação do kubectl na documentação do Amazon EKS.

Arquitetura

Pilha de tecnologia

- Amazon EKS
- AWS PrivateLink
- Network Load Balancer

Automação e escala

- Os manifestos do Kubernetes podem ser rastreados e gerenciados em um repositório baseado em Git e implantados usando integração contínua e entrega contínua (CI/CD) na AWS. CodePipeline
- Você pode usar CloudFormation a AWS para criar esse padrão usando infraestrutura como código (IaC).

Ferramentas

- AWS CLI: o AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- Elastic Load Balancing — O Elastic Load Balancing distribui o tráfego de entrada de aplicativos ou de rede em vários destinos, como instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (EC2Amazon), em uma ou mais zonas de disponibilidade.

- Amazon EKS: o Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço gerenciado que você pode usar para executar o Kubernetes na AWS, eliminando a necessidade de instalar, operar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- Amazon VPC: o Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você.
- Kubectl: o Kubectl é um utilitário de linha de comando para executar comandos em clusters Kubernetes.

Épicos

Implante os arquivos de manifesto de implantação e serviço do Kubernetes

Tarefa	Descrição	Habilidades necessárias

Crie o arquivo de manifesto de implantação do Kubernetes.	Crie um arquivo de manifesto de implantação modificando o arquivo de exemplo a seguir de acordo com seus requisitos.
	
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: sample-app`
	`spec:`
	`  replicas: 3`
	`  selector:`
	`  matchLabels:`
	`  app: nginx`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: nginx`
	`  spec:`
	`  containers:`
	`  - name: nginx`
	`  image:`
	` public.ecr.aws/z9d2n7e1/nginx:1.19.5`
	`  ports:`
	`  - name: http`
	`  containerPort: 80`
	
	Note
	Esse é um exemplo de arquivo de configuração do NGINX que é
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	implantado usando a imagem do Docker do NGINX. Para obter mais informações, consulte Como usar a imagem oficial do Docker do NGINX na documentação do Docker.	
Implante o arquivo de manifesto de implantação do Kubernetes.	Execute o seguinte comando para aplicar o arquivo do manifesto de implantação ao cluster do Amazon EKS: `kubectl apply -f <your_deployment_file_name>`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Crie o arquivo do manifesto do serviço do Kubernetes.	Crie um serviço de manifesto de serviço modificando o arquivo de exemplo a seguir de acordo com seus requisitos.
	
	`apiVersion: v1`
	`kind: Service`
	`metadata:`
	`  name: sample-service`
	`  annotations:`
	`  service.beta.kubernetes.io/aws-load-balancer-type: nlb`
	`  service.beta.kubernetes.io/aws-load-balancer-internal: "true"`
	`spec:`
	`  ports:`
	`  - port: 80`
	`  targetPort: 80`
	`  protocol: TCP`
	`  type: LoadBalancer`
	`  selector:`
	`  app: nginx`
	
	Important
	Certifique-se de incluir o seguinte `annotations` para definir um Network Load Balancer interno:
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`service.beta.kubernetes.io/aws-load-balancer-type: nlb` `service.beta.kubernetes.io/aws-load-balancer-internal: "true"`	
Implante o arquivo de manifesto do serviço Kubernetes.	Execute o seguinte comando para aplicar o arquivo de manifesto do serviço ao cluster do Amazon EKS: `kubectl apply -f <your_service_file_name>`	DevOps engenheiro

Criar os endpoints

Tarefa	Descrição	Habilidades necessárias
Registre o nome do Network Load Balancer.	Execute o comando a seguir para recuperar o nome do Network Load Balancer: `kubectl get svc sample-service -o wide` Registre o nome do Network Load Balancer, que é necessário para criar um PrivateLink endpoint da AWS.	DevOps engenheiro
Crie um PrivateLink endpoint da AWS.	Faça login no AWS Management Console, abra	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	o console da Amazon VPC e crie um endpoint da AWS PrivateLink . Associe esse endpoint ao Network Load Balancer, isso torna o aplicativo disponível de forma privada para os clientes. Para obter mais informações, consulte VPC endpoint services (AWS PrivateLink) na documentação da Amazon VPC. **Important** Se a conta do consumidor exigir acesso ao aplicativo, o ID da conta da AWS da conta do consumidor deverá ser adicionado à lista de diretores permitidos para a configuração do PrivateLink endpoint da AWS. Para obter mais informações, consulte Adicionar e remover permissões para o serviço de endpoint na documentação da Amazon VPC.	

Tarefa	Descrição	Habilidades necessárias
Crie um VPC endpoint	No console da Amazon VPC, escolha Serviços de endpoint e escolha Criar o serviço de endpoint. Crie um endpoint VPC para o endpoint da AWS. PrivateLink O nome de domínio totalment e qualificado (FQDN) do VPC endpoint aponta para o FQDN do endpoint da AWS. PrivateLi nk Isso cria uma interface de rede elástica para o serviço de endpoint da VPC que os endpoints de DNS podem acessar.	Administrador de nuvem

Recursos relacionados

- Usar a imagem do Docker oficial NGINX
- Network Load Balancer no Amazon EKS
- Criação de serviços de endpoint VPC (AWS) PrivateLink
- Adicionar e remover permissões para o serviço de endpoint

Ativar mTLS no AWS App Mesh usando a AWS Private CA no Amazon EKS

Criado por Omar Kahil (AWS), Emmanuel Saliu (AWS), Muhammad Shahzad (AWS) e Andy Wong (AWS)

Resumo

Este padrão mostra como implementar o Mutual Transport Layer Security (mTLS) no Amazon Web Services (AWS) usando certificados da AWS Private Certificate Authority (AWS Private CA) no AWS App Mesh. Ele usa a API do serviço de descoberta secreta (SDS) Envoy por meio do Secure Production Identity Framework for Everyone (SPIFFE). O SPIFFE é um projeto de código aberto da Cloud Native Computing Foundation (CNCF) com amplo suporte da comunidade que fornece gerenciamento de identidade de workload refinado e dinâmico. Para implementar os padrões do SPIFFE, use o ambiente de runtime SPIRE SPIFFE.

O uso do mTLS no App Mesh oferece autenticação bidirecional de pares, pois adiciona uma camada de segurança sobre o TLS e permite que os serviços na malha verifiquem o cliente que está fazendo a conexão. O cliente na relação cliente-servidor também fornece um certificado X.509 durante o processo de negociação da sessão. O servidor usa esse certificado para identificar e autenticar o cliente. Isso ajuda a verificar se o certificado foi emitido por uma autoridade de certificação (CA) confiável e se o certificado é válido.

Pré-requisitos e limitações

Pré-requisitos

- Um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) com grupos de nós autogerenciados ou gerenciados
- App Mesh Controller implantado no cluster com o SDS ativado
- Um certificado privado do AWS Certificate Manager (ACM) que é emitido pela AWS Private CA

Limitações

- O SPIRE não pode ser instalado no AWS Fargate porque o agente SPIRE deve ser executado como um Kubernetes. DaemonSet

Versões do produto

- AWS App Mesh Controller chart 1.3.0 ou superior

Arquitetura

O diagrama a seguir mostra o cluster EKS com App Mesh na VPC. O servidor SPIRE em um nó de processamento se comunica com os SPIRE Agents em outros nós de processamento e com a AWS Private CA. O Envoy é usado para comunicação mTLS entre os nós de processamento do SPIRE Agent.

O diagrama ilustra as seguintes etapas:

1. O certificado é emitido.
2. Solicite o certificado e sua assinatura autenticada.

Ferramentas

Serviços da AWS

- CA privada da AWS — A Autoridade de Certificação Privada da AWS (CA privada da AWS) permite a criação de hierarquias de autoridade de certificação (CA) privada, incluindo raiz e subordinada CAs, sem os custos de investimento e manutenção da operação de uma CA local.
- AWS App Mesh: a AWS App Mesh é uma malha de serviço que facilita o monitoramento e o controle de serviços. O App Mesh padroniza como seus serviços se comunicam, dando visibilidade consistente e controle de tráfego de rede para cada serviço em uma aplicação.
- Amazon EKS: o Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço gerenciado que você pode usar para executar o Kubernetes na AWS, eliminando a necessidade de instalar, operar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.

Outras ferramentas

- Helm: o Helm é um gerenciador de pacotes para o Kubernetes que ajuda a instalar e gerenciar aplicações em seu cluster do Kubernetes. Esse padrão usa o Helm para implantar o controlador do AWS App Mesh.
- Chart do AWS App Mesh Controller: o chart do controlador do AWS App Mesh é usado por esse padrão para habilitar o AWS App Mesh no Amazon EKS.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Configure o App Mesh com o Amazon EKS.	Siga as etapas básicas de implantação fornecidas no repositório.	DevOps engenheiro
Instale o SPIRE.	Instale o SPIRE no cluster EKS usando spire_setup.yaml.	DevOps engenheiro
Instale o certificado da AWS Private CA.	Crie e instale um certifica do para sua CA raiz privada seguindo as instruções na documentação da AWS.	DevOps engenheiro
Conceda permissões para a função de instância do nó do cluster.	Para anexar políticas à função de instância do nó do cluster, use o código que está na seção Informações adicionais.	DevOps engenheiro
Adicione o plug-in SPIRE para a AWS Private CA.	Para adicionar o plug-in à configuração do servidor SPIRE, use o código que está na seção Informações adicionais. Substitua o nome do recurso da Amazon (ARN) `certificate_authority_arn` pelo seu ARN da CA privada. O algoritmo de assinatura usado deve ser o mesmo da CA privada. Substitua `your_region` pela sua região da AWS.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações sobre o plug-in, consulte Plug-in do servidor: UpstreamAuthority “aws_pca”.	
Atualize bundle.cert.	Depois de criar o SPIRE Server, um arquivo `spire-bundle.yaml` será criado. Altere o valor `bundle.crt` no arquivo `spire-bundle.yaml` da CA privada para o certificado público.	DevOps engenheiro

Implementar e registrar as workloads

Tarefa	Descrição	Habilidades necessárias
Registre entradas de nós e workload com o SPIRE.	Para registrar o nó e a workload (serviços) no servidor SPIRE, use o código no repositório.	DevOps engenheiro
Crie uma malha no App Mesh com o mTLS ativado.	Crie uma nova malha no App Mesh com todos os componentes do seu aplicativo de microsserviços (por exemplo, serviço virtual, roteador virtual e nós virtuais).	DevOps engenheiro
Inspecione as entradas registradas.	Você pode inspecionar as entradas registradas para seus nós e workloads executando o comando a seguir.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`kubectl exec -n spire spire-server-0 -- /opt/spire/bin/spire-server entry show` Isso mostrará as entradas dos SPIRE Agents.	

Verificar o tráfego do mTLS

Tarefa	Descrição	Habilidades necessárias
Verifique o tráfego do mTLS.	1. Do serviço de frontend, envie um cabeçalho HTTP para o serviço de backend e verifique uma resposta bem-sucedida com os serviços registrados no SPIRE. 2. Para autenticação TLS mútua, você pode inspecionar a estatística `ssl.handshake` executando o comando a seguir. `kubectl exec -it $POD -n $NAMESPACE -c envoy -- curl http://localhost:9901/stats | grep ssl.handshake` Depois de executar o comando anterior, você deverá ver a contagem `ssl.handshake` de	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	receptores, que será semelhante ao seguinte exemplo: `listener.0.0.0.0_15000.ssl.handshake: 2`	
Verifique se os certificados estão sendo emitidos pela AWS Private CA.	Você pode verificar se os plug-ins foram configurados corretamente e se os certificados estão sendo emitidos pela sua CA privada upstream visualizando os registros em seu SPIRE Server. Execute o seguinte comando: `kubectl logs spire-server-0 -n spire` Em seguida, visualize os logs que são gerados. Esse código pressupõe que seu servidor se chame `spire-server-0` e esteja hospedado em seu namespace spire. Você deve ver o carregamento bem-sucedido dos plug-ins e uma conexão sendo estabelecida com sua CA privada upstream.	DevOps engenheiro

Recursos relacionados

- Uso do mTLS com SPIFFE/SPIRE no AWS App Mesh no Amazon EKS

- Habilitação do mTLS no AWS App Mesh usando SPIFFE/SPIRE em um ambiente Amazon EKS com várias contas
- Passo a passo usado nesse padrão
- Plugin de servidor: UpstreamAuthority “aws_pca”
- Guia de início rápido para Kubernetes

Mais informações

Conceda permissões para a função de instância do nó do cluster

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ACMPCASigning",
            "Effect": "Allow",
            "Action": [
                "acm-pca:DescribeCertificateAuthority",
                "acm-pca:IssueCertificate",
                "acm-pca:GetCertificate",
                "acm:ExportCertificate"
            ],
            "Resource": "*"
        }
    ]
}
AWS Managed Policy: "AWSAppMeshEnvoyAccess"
```

Adicione o plug-in SPIRE para ACM

```
Add the SPIRE plugin for ACM
Change certificate_authority_arn to your PCA ARN. The signing algorithm used must be
 the same as the signing algorithm on the PCA. Change your_region to the appropriate
 AWS Region.
UpstreamAuthority "aws_pca" {
    plugin_data {
        region = "your_region"
        certificate_authority_arn = "arn:aws:acm-pca:...."
        signing_algorithm = "your_signing_algorithm"
    }
}
```

Automatize backups para instâncias de banco de dados do Amazon RDS para PostgreSQL usando o AWS Batch

Criado por Kirankumar Chandrashekar (AWS)

Resumo

Fazer backup de seus bancos de dados PostgreSQL é uma tarefa importante e normalmente pode ser concluído com o utilitário pg_dump, que usa o comando COPIAR por padrão para criar um esquema e uma despejo de dados de um banco de dados PostgreSQL. No entanto, esse processo pode se tornar repetitivo se você precisar de backups regulares para vários bancos de dados PostgreSQL. Se seus bancos de dados PostgreSQL estiverem hospedados na nuvem, você também poderá aproveitar o atributo de backup automatizado fornecido pelo Amazon Relational Database Service (Amazon RDS) para PostgreSQL. Esse padrão descreve como automatizar backups regulares para instâncias de banco de dados Amazon RDS para PostgreSQL usando o utilitário pg_dump.

Observação: as instruções pressupõem que você esteja usando o Amazon RDS. No entanto, você também pode usar essa abordagem para bancos de dados PostgreSQL hospedados fora do Amazon RDS. Para fazer backups, a função do AWS Lambda deve conseguir acessar seus bancos de dados.

Um evento Amazon CloudWatch Events baseado em tempo inicia uma função Lambda que pesquisa tags de backup específicas aplicadas aos metadados das instâncias de banco de dados PostgreSQL no Amazon RDS. Se as instâncias de banco de dados PostgreSQL tiverem a tag DBDump BKP:automated = Active e outras tags de backup necessárias, a função Lambda enviará trabalhos individuais para cada backup de banco de dados para o AWS Batch.

O AWS Batch processa essas tarefas e carrega os dados de backup em um bucket do Amazon Simple Storage Service (Amazon S3). Esse padrão usa um Dockerfile e um arquivo entrypoint.sh para criar uma imagem de contêiner do Docker que é usada para fazer backups no trabalho do AWS Batch. Após a conclusão do processo de backup, o AWS Batch registra os detalhes do backup em uma tabela de inventário no Amazon DynamoDB. Como proteção adicional, um evento CloudWatch Events inicia uma notificação do Amazon Simple Notification Service (Amazon SNS) se um trabalho falhar no AWS Batch.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um ambiente computacional gerenciado ou não gerenciado existente. Para obter mais informações, consulte Ambientes de computação gerenciados e não gerenciados na documentação do AWS Batch.
- Interface de linha de comandos (CLI) versão 2 imagem do Docker, instalada e configurada.
- Instâncias de banco de dados do Amazon RDS para PostgreSQL existentes
- Um bucket do S3 existente
- jDocker, instalado e configurado em macOS, Linux ou Windows
- Familiaridade com a codificação em Lambda.

Arquitetura

Pilha de tecnologia

- CloudWatch Eventos da Amazon
- Amazon DynamoDB
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon RDS
- Amazon SNS
- Amazon S3
- AWS Batch
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- Docker

Ferramentas

- Amazon CloudWatch Events — CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- Amazon DynamoDB: o DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade integrada.

- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um serviço de registro de imagem de contêiner, seguro, escalável e confiável.
- Amazon RDS: o Amazon Relational Database Service (Amazon RDS) é um serviço Web que facilita a configuração, a operação e escalabilidade de um banco de dados relacional na Nuvem AWS.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens de editores para assinantes.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet.
- AWS Batch: o AWS Batch ajuda você a executar workloads de computação em lotes na Nuvem AWS.
- AWS KMS: o AWS Key Management Service (AWS KMS) é um serviço gerenciado que facilita a criação e o controle de chaves do AWS KMS, que criptografam seus dados.
- AWS Lambda: o AWS Lambda é um serviço de computação com tecnologia que ajuda a executar código sem provisionamento ou gerenciamento de servidores.
- AWS Secrets Manager: o Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente.
- Docker: o Docker ajuda os desenvolvedores a empacotar, enviar e executar facilmente qualquer aplicativo como um contêiner leve, portátil e autossuficiente.

Suas instâncias de banco de dados PostgreSQL no Amazon RDS devem ter tags aplicadas aos seus metadados. A função do Lambda pesquisa tags para identificar instâncias de banco de dados que devem ser copiadas, e as tags a seguir são normalmente usadas.

Tag	Descrição
BKP: Automatizado = Ativo DBDump	Identifica uma instância de banco de dados Amazon RDS como candidata para backups.
bpm: = AutomatedBackupSecret <secret_name>	Identifica o segredo do Secrets Manager que contém as credenciais de login do Amazon RDS.

BKP: S3 Bucket automatizado = DBDump <s3_bucket_name>	Identifica o bucket do S3 para enviar backups.
BKP: Frequência automatizada DBDump BKP: Tempo automatizado DBDump	Identifique a frequência e os horários em que o backup dos bancos de dados deve ser feito.
bkp:pgdumpcommand = <pgdump_command>	Identifica os bancos de dados para os quais os backups precisam ser feitos.

Épicos

Crie uma tabela de inventário no DynamoDB

Tarefa	Descrição	Habilidades necessárias
Crie uma tabela no DynamoDB.	Faça login no Console de Gerenciamento da AWS e abra o console do Amazon DynamoDB, e crie uma tabela. Para obter ajuda com esse e outros artigos, consulte a seção Recursos relacionados.	Administrador de nuvem, administrador de banco de dados
Confirme se a tabela foi criada.	Execute o comando `aws dynamodb describe-table --table-name <table-name> | grep TableStatus` . Se a tabela existir, o comando retornará o resultado `"TableStatus": "ACTIVE",` .	Administrador de nuvem, administrador de banco de dados

Crie um tópico do SNS para eventos de trabalho com falha no AWS Batch

Tarefa	Descrição	Habilidades necessárias
Criar um tópico do SNS.	Abra o console do Amazon SNS, escolha Tópicos e crie um tópico do SNS com o nome `JobFailedAlert` . Inscreva um endereço de e-mail ativo no tópico e verifique sua caixa de entrada de e-mail para confirmar o e-mail de assinatura do SNS a partir do AWS Notifications.	Administrador de nuvem
Crie uma regra de evento de trabalho com falha para o AWS Batch.	Abra o CloudWatch console da Amazon, escolha Eventos e, em seguida, escolha Criar regra. Escolha Mostrar opções avançadas, e escolha editar. Em Criar um padrão que selecione eventos para processamento pelos seus destinos, substitua o texto existente pelo código “Evento de trabalho com falha” na seção Informações adicionais. Esse código define uma regra de CloudWatch eventos que começa quando o AWS Batch tem um `Failed` evento.	Administrador de nuvem
Adicione o destino da regra do evento.	Em Destinos, selecione Adicionar destino e, em seguida, selecione o Tópico do SNS `JobFailedAlert` . Configurar os detalhes	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	restantes e criar a regra do CloudWatch Events.	

Desenvolva uma imagem do Docker e enviá-la a um repositório do Amazon ECR

Tarefa	Descrição	Habilidades necessárias
Crie um repositório do Amazon ECR.	Abra o console do Amazon ECR e escolha a região da AWS na qual você deseja criar seu repositór io. Escolha Repositórios e depois Adicionar repositór io. Configure o repositório de acordo com seus requisitos.	Administrador de nuvem
Escreva um Dockerfile.	Faça login no Docker e use o “Dockerfile de amostra” e o “Exemplo de arquivo entrypoin t.sh” da seção Informaçõ es adicionais para criar um Dockerfile.	DevOps engenheiro
Criar uma imagem do Docker e enviá-la ao repositório do Amazon ECR.	Crie o Dockerfile em uma imagem do Docker e envie-a para o repositório do Amazon ECR. Para obter ajuda com esta etapa, consulte a seção Recursos relacionados.	DevOps engenheiro

Crie os componentes do AWS Batch

Tarefa	Descrição	Habilidades necessárias
Criar uma definição de trabalho do AWS Batch.	Abra o console do AWS Batch e crie uma definição de trabalho que inclua o Uniform Resource Identifier (URI) do repositório Amazon ECR como propriedade `Image`.	Administrador de nuvem
Configure a fila de trabalhos do AWS Batch.	No console do AWS Batch, escolha Filas de trabalhos e, em seguida, escolha Criar fila. Crie uma fila de trabalhos que armazenará trabalhos até que o AWS Batch os execute nos recursos do seu ambiente computacional. Importante: certifique-se de escrever uma lógica para que o AWS Batch registre os detalhes do backup na tabela de inventário do DynamoDB.	Administrador de nuvem

Crie e publique uma função do Lambda

Tarefa	Descrição	Habilidades necessárias
Crie uma função do Lambda para pesquisar tags.	Crie uma função do Lambda que pesquise tags em suas instâncias de banco de dados PostgreSQL e identifique candidatos a backup. Certifique-se de que sua função do Lambda possa identificar a tag	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`bkp:AutomatedDBDump = Active` e todas as outras tags necessárias. Importante: a função do Lambda também deve conseguir adicionar trabalhos à fila de trabalhos do AWS Batch.	
Crie um evento de CloudWatch eventos com base no tempo.	Abra o CloudWatch console da Amazon e crie um evento CloudWatch Events que usa uma expressão cron para executar sua função Lambda em uma programação regular. Importante: Todos os eventos programados usam o fuso horário UTC.	Administrador de nuvem

Teste a automação de backup

Tarefa	Descrição	Habilidades necessárias
Criar uma chave do Amazon KMS.	Abra o console do Amazon KMS e crie uma chave KMS que possa ser usada para criptografar as credenciais do Amazon RDS armazenadas no AWS Secrets Manager.	Administrador de nuvem
Criar um segredo do AWS Secrets Manager.	Abra o console do AWS Secrets Manager e armazene suas credenciais do banco de dados do Amazon RDS	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	para PostgreSQL como um segredo.	
Adicione as tags necessárias às instâncias de banco de dados PostgreSQL.	**⚠ Important** Abra o console do Amazon RDS e adicione tags às instâncias de banco de dados PostgreSQL das quais você deseja fazer backup automático. Você pode usar as tags da tabela na seção Ferramentas. Se você precisar de backups de vários bancos de dados PostgreSQL na mesma instância do Amazon RDS, `-d test:-d test1` use como valor para a tag. `bkp:pgdumpcommand teste test1` são nomes de bancos de dados. Certifique-se de que não há espaço após os dois pontos (:).	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Verifique a automação do backup.	Para verificar a automação do backup, você pode invocar a função do Lambda ou aguardar o início da programação de backup. Depois que o processo de backup estiver concluído , verifique se a tabela de inventário do DynamoDB tem uma entrada de backup válida para suas instâncias de banco de dados PostgreSQL. Se corresponderem, o processo de automação de backup será bem-sucedido.	Administrador de nuvem

Recursos relacionados

Crie uma tabela de inventário no DynamoDB

- Crie uma tabela do Amazon DynamoDB

Crie um tópico do SNS para eventos de trabalho com falha no AWS Batch

- Crie um tópico do Amazon SNS
- Envie alertas do SNS sobre eventos de trabalho com falha no AWS Batch

Desenvolva uma imagem do Docker e enviá-la a um repositório do Amazon ECR

- Crie um repositório do Amazon ECR
- Escreva um Dockerfile, crie uma imagem do Docker e envie-a para o Amazon ECR

Crie os componentes do AWS Batch

- Crie uma definição de trabalho do AWS Batch
- Configure seu ambiente computacional e a fila de trabalhos do AWS Batch
- Crie uma fila de trabalhos no AWS Batch

Criar uma função do Lambda

- Crie uma função do Lambda e escreva código
- Use o Lambda com o DynamoDB

Crie um evento de CloudWatch eventos

- Crie um evento de CloudWatch eventos baseado em tempo
- Use expressões cron em eventos do Cloudwatch

Teste a automação de backup

- Crie uma chave do Amazon KMS
- Crie um segredo do Secrets Manager
- Adicione tags a uma instância do Amazon RDS

Mais informações

Evento de trabalho falhado:

```
{
  "detail-type": [
    "Batch Job State Change"
  ],
```

```
  "source": [
    "aws.batch"
  ],
  "detail": {
    "status": [
      "FAILED"
    ]
  }
}
```

Exemplo de Dockerfile:

```
FROM alpine:latest
RUN apk --update add py-pip postgresql-client jq bash && \
pip install awscli && \
rm -rf /var/cache/apk/*
ADD entrypoint.sh /usr/bin/
RUN chmod +x /usr/bin/entrypoint.sh
ENTRYPOINT ["entrypoint.sh"]
```

Exemplo de arquivo entrypoint.sh:

```
 #!/bin/bash
set -e
DATETIME=`date +"%Y-%m-%d_%H_%M"`
FILENAME=RDS_PostGres_dump_${RDS_INSTANCE_NAME}
FILE=${FILENAME}_${DATETIME}

aws configure --profile new-profile set role_arn arn:aws:iam::${TargetAccountId}:role/
${TargetAccountRoleName}
aws configure --profile new-profile set credential_source EcsContainer

echo "Central Account access provider IAM role is: "
aws sts get-caller-identity

echo "Target Customer Account access provider IAM role is: "
aws sts get-caller-identity --profile new-profile

securestring=$(aws secretsmanager get-secret-value --secret-id $SECRETID --output json
 --query 'SecretString' --region=$REGION --profile new-profile)

if [[ ${securestring} ]]; then
    echo "successfully accessed secrets manager and got the credentials"
```

```
    export PGPASSWORD=$(echo $securestring | jq --raw-output | jq -r '.DB_PASSWORD')
    PGSQL_USER=$(echo $securestring | jq --raw-output | jq -r '.DB_USERNAME')
    echo "Executing pg_dump for the PostGres endpoint ${PGSQL_HOST}"
    # pg_dump -h $PGSQL_HOST -U $PGSQL_USER -n dms_sample | gzip -9 -c  | aws s3 cp -
 --region=$REGION  --profile new-profile s3://$BUCKET/$FILE
    # in="-n public:-n private"
    IFS=':' list=($EXECUTE_COMMAND);
    for command in "${list[@]}";
      do
        echo $command;
        pg_dump -h $PGSQL_HOST -U $PGSQL_USER ${command} | gzip -9 -c  | aws s3 cp - --
region=$REGION --profile new-profile s3://${BUCKET}/${FILE}-${command}".sql.gz"
        echo $?;
        if  [[ $? -ne 0 ]]; then
            echo "Error occurred in database backup process. Exiting now....."
            exit 1
        else
            echo "Postgresql dump was successfully taken for the RDS endpoint
 ${PGSQL_HOST} and is uploaded to the following S3 location s3://${BUCKET}/${FILE}-
${command}.sql.gz"
            #write the details into the inventory table in central account
            echo "Writing to DynamoDB inventory table"
            aws dynamodb put-item --table-name ${RDS_POSTGRES_DUMP_INVENTORY_TABLE} --
region=$REGION --item '{ "accountId": { "S": "'"${TargetAccountId}"'" }, "dumpFileUrl":
 {"S": "'"s3://${BUCKET}/${FILE}-${command}.sql.gz"'" }, "DumpAvailableTime": {"S":
 "'"`date +"%Y-%m-%d::%H::%M::%S"` UTC"'"}}'
            echo $?
            if  [[ $? -ne 0 ]]; then
                echo "Error occurred while putting item to DynamoDb Inventory Table.
 Exiting now....."
                exit 1
            else
                echo "Successfully written to DynamoDb Inventory Table
 ${RDS_POSTGRES_DUMP_INVENTORY_TABLE}"
            fi
        fi
      done;
else
    echo "Something went wrong {$?}"
    exit 1
fi

exec "$@"
```

Automatize a implantação do Manipulador do término do nó no Amazon EKS usando um pipeline de CI/CD

Criado por Sandip Gangapadhyay (AWS), John Vargas (AWS), Pragtideep Singh (AWS), Sandeep Gawande (AWS) e Viyoma Sachdeva (AWS)

Resumo

Aviso: CodeCommit A AWS não está mais disponível para novos clientes. Os clientes atuais da AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Na nuvem da Amazon Web Services (AWS), você pode usar o AWS Node Termination Handler, um projeto de código aberto, para lidar com o desligamento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no Kubernetes sem problemas. O AWS Node Termination Handler ajuda a garantir que o plano de controle do Kubernetes responda adequadamente aos eventos que podem fazer com que sua instância fique indisponível. EC2 Esses eventos incluem o seguinte:

- EC2 manutenção programada por instância
- Interrupções da Amazon EC2 Spot Instance
- Escala de grupos do Auto Scaling
- Rebalanceamento de grupos do Auto Scaling em todas as zonas de disponibilidade
- EC2 encerramento da instância por meio da API ou do AWS Management Console

Se um evento não for tratado, o código do aplicativo pode não parar normalmente. Também pode levar mais tempo para recuperar a disponibilidade total ou programar acidentalmente o trabalho nos nós que estão sendo desativados. O `aws-node-termination-handler` (NTH) pode operar em dois modos diferentes: serviço de metadados de instância (IMDS) ou Processador de filas. Para obter mais informações sobre os dois modos, consulte o arquivo Readme.

Esse padrão usa AWS CodeCommit e automatiza a implantação do NTH usando o Processador de Filas por meio de um pipeline de integração contínua e entrega contínua (CI/CD).

> **Note**
>
> Se você estiver usando grupos de nós gerenciados pelo EKS, não precisará do`aws-node-termination-handler`.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um navegador da web compatível com o Console de Gerenciamento da AWS. Consulte a lista de navegadores compatíveis.
- AWS Cloud Development Kit (AWS CDK), instalado.
- `kubectl`, a ferramenta de linha de comando do Kubernetes, instalada.
- `eksctl`, a AWS Command Line Interface (AWS CLI) para o Amazon Elastic Kubernetes Service (Amazon EKS), instalado.
- Um cluster EKS em execução com a versão 1.20 ou superior.
- Um grupo de nós autogerenciados conectado ao cluster do EKS. Para criar um cluster do Amazon EKS com um grupo de nós autogerenciado, execute o comando a seguir.

```
eksctl create cluster --managed=false --region <region> --name <cluster_name>
```

  Para obter mais informações sobre `eksctl`, consulte a documentação do eksctl.
- AWS Identity and Access Management (IAM) provedor OpenID Connect (OIDC) para o seu cluster. Para obter mais informações, consulte Criar um provedor IAM OIDC para o cluster.

Limitações

- Você deve usar uma região da AWS que ofereça suporte ao serviço Amazon EKS.

Versões do produto

- Kubernetes versão 1.20 ou superior
- `eksctl` versão 0.107.0 ou superior
- AWS CDK versão 2.27.0 ou superior

Arquitetura

Pilha de tecnologias de destino

- Uma nuvem privada virtual (VPC)

- Um cluster do EKS
- Amazon Simple Queue Service (Amazon SQS)
- IAM
- Kubernetes

Arquitetura de destino

O diagrama a seguir mostra a visão de alto nível das end-to-end etapas em que a terminação do nó é iniciada.

O fluxo de trabalho mostrado no diagrama consiste nas seguintes etapas de alto nível:

1. O evento de encerramento automático da EC2 instância de escalabilidade é enviado para a fila do SQS.
2. O NTH Pod monitora novas mensagens na fila SQS.
3. O NTH Pod recebe a nova mensagem e faz o seguinte:
   - Protege o nó para que o novo pod não seja executado no nó.
   - Drena o nó, para que o pod existente seja evacuado
   - Envia um sinal de gancho do ciclo de vida para o grupo do Auto Scaling para que o nó possa ser encerrado.

Automação e escala

- O código é gerenciado e implantado pelo AWS CDK, apoiado por pilhas CloudFormation aninhadas da AWS.
- O ambiente de gerenciamento do Amazon EKS é executado em várias zonas de disponibilidade para assegurar alta disponibilidade.
- Para escalabilidade automática, o Amazon EKS oferece suporte ao Kubernetes Cluster Autoscaler e ao Karpenter.

Ferramentas

Serviços da AWS

- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- O Amazon EC2 Auto Scaling ajuda você a manter a disponibilidade do aplicativo e permite que você adicione ou remova automaticamente EC2 instâncias da Amazon de acordo com as condições definidas por você.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.

Outras ferramentas

- Kubectl é uma ferramenta de linha de comando para executar comandos em clusters do Kubernetes. Você pode usar o kubectl para implantar aplicativos, inspecionar e gerenciar recursos de cluster e visualizar registros.

Código

O código desse padrão está disponível no deploy-nth-to-eksrepositório em GitHub .com. O repositório do código contém os seguintes arquivos e pastas.

- `nth folder`— O gráfico do Helm, os arquivos de valores e os scripts para escanear e implantar o CloudFormation modelo da AWS para o Node Termination Handler.
- `config/config.json`: o arquivo de parâmetros de configuração do aplicativo. Esse arquivo contém todos os parâmetros necessários para a implantação do CDK.
- `cdk`: o código-fonte do AWS CDK.

- `setup.sh`: o script usado para implantar o aplicativo AWS CDK para criar o pipeline de CI/CD necessário e outros recursos necessários.
- `uninstall.sh`: o script usado para limpar os recursos.

Para usar o código de exemplo, siga as instruções na seção Épicos.

Práticas recomendadas

Para obter as melhores práticas ao automatizar o Manipulador do término do nó da AWS, consulte o seguinte:

- Guias de melhores práticas do EKS
- Manipulador do término do nó - Configuração

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias

Clone o repositório.	Para clonar o repositório usando SSH (Secure Shell), execute o comando a seguir.
	`git clone git@github.com:aws-samples/deploy-nth-to-eks.git`
	Para clonar o repositório usando HTTPS, execute o comando a seguir.
	`git clone https://github.com/aws-samples/deploy-nth-to-eks.git`
		Desenvolvedor de aplicativos, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	A clonagem do repositório cria uma pasta chamada `deploy-nth-to-eks` . Mude para esse diretório. `cd deploy-nth-to-eks`	
Defina o arquivo kubeconfig.	Defina as suas credenciais da AWS em seu terminal e confirme se você tem direitos para assumir a função de cluster. Você pode usar o seguinte exemplo de código. `aws eks update-kubeconfig --name <Cluster_Name> --region <region>--role-arn <Role_ARN>`	AWS DevOps, DevOps engenheiro, desenvolvedor de aplicativos

Implante o pipeline de CI/CD

Tarefa	Descrição	Habilidades necessárias
Configure os parâmetros.	No arquivo `config/config.json` , configure os seguintes parâmetros necessários. • `pipelineName` : o nome do pipeline de CI/CD a ser criado pelo AWS CDK (por exemplo, `deploy-nth-to-eks-pipeline`). A	Desenvolvedor de aplicativos, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	AWS CodePipeline criará um pipeline com esse nome. • `repositoryName` : O CodeCommit repositório da AWS a ser criado (por exemplo,`deploy-nth-to-eks-repo`). O AWS CDK criará esse repositório e o definirá como origem para o pipeline de CI/CD. **Note** Essa solução criará esse CodeCommit repositório e a ramificação (fornecida no parâmetro de ramificação a seguir). • `branch`: o nome da ramificação no repositório (por exemplo, `main`). Uma confirmação com essa ramificação iniciará o pipeline de CI/CD. • `cfn_scan_script` : o caminho do script que será usado para escanear o CloudFormation modelo da AWS para NTH (`scan.sh`). Esse script existe na `nth`	

Tarefa	Descrição	Habilidades necessárias
	pasta que fará parte do CodeCommit repositório da AWS. • `cfn_deploy_scrip t`: O caminho do script que será usado para implantar o CloudFormation modelo da AWS para NTH (`installApp.sh `). • `stackName` : o nome da CloudFormation pilha a ser implantada. • `eksClusterName` : o nome do cluster existente do EKS. • `eksClusterRole` : o perfil do IAM que será usado para acessar o cluster EKS para todas as chamadas da API Kubernetes (por exemplo, `clusterad min`). Normalmente, essa função é adicionada em `aws-auth ConfigMap` . • `create_cluster_rol e` : para criar o `eksCluste rRole` perfil do IAM, digite sim. Se você quiser fornecer uma função de cluster existente no parâmetro `eksClusterRole` , digite não.	

Tarefa	Descrição	Habilidades necessárias
	• `create_iam_oidc_provider` : para criar um provedor de identidade OIDC do IAM para o cluster, insira sim. Se um provedor IAM OIDC já existir, digite não. Para obter mais informações, consulte Criar um provedor IAM OIDC para o cluster. • `AsgGroupName` : uma lista separada por vírgulas dos nomes de grupos do Auto Scaling que fazem parte do cluster EKS (por exemplo,) `ASG_Group_1,ASG_Group_2` . • `region`: o nome da região da AWS onde o cluster está localizado (por exemplo, `us-east-2`). • `install_cdk` : Se o AWS CDK não estiver instalado atualmente na máquina, digite sim. Execute o comando `cdk --version` para verificar se a versão instalada do AWS CDK é 2.27.0 ou superior. Nesse caso, digite não. Se você digitar sim, o script setup.sh executará o comando `sudo npm`	

Tarefa	Descrição	Habilidades necessárias
	`install -g cdk@2.27.0` para instalar o AWS CDK na máquina. O script requer permissões sudo, portanto, forneça a senha da conta quando solicitado.	
Crie o pipeline de CI/CD para implantar o NTH.	Execute o script setup.sh. `./setup.sh` O script implantará o aplicativo AWS CDK que criará o CodeCommit repositório com o código de exemplo, o pipeline e os CodeBuild projetos com base nos parâmetros de entrada do usuário no `config/config.json` arquivo. Esse script solicitará a senha ao instalar pacotes npm com o comando sudo.	Desenvolvedor de aplicativos, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Analise o pipeline de CI/CD.	Abra o Console de Gerenciamento da AWS e analise os seguintes recursos criados na pilha. • CodeCommit repositório com o conteúdo da pasta `nth` • CodeBuild Projeto da AWS`cfn-scan`, que examinará o CloudFormation modelo em busca de vulnerabilidades. • CodeBuild projeto`Nth-Deploy` , que implantará o CloudFormation modelo da AWS e os gráficos NTH Helm correspondentes por meio do pipeline da AWS CodePipeline . • Um CodePipeline pipeline para implantar o NTH. Depois que o pipeline é executado com sucesso, a versão `aws-node-termination-handler` do Helm é instalada no cluster EKS. Além disso, um pod chamado `aws-node-termination-handler` está sendo executado no	Desenvolvedor de aplicativos, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	namespace `kube-system` do cluster.	

Teste a implantação do NTH

Tarefa	Descrição	Habilidades necessárias
Simule um evento de escalonamento de grupo do Auto Scaling.	Para simular um evento de escalonamento automático, faça o seguinte: 1. No console da AWS, abra o EC2 console e escolha Auto Scaling Groups. 2. Selecione o grupo do Auto Scaling que tem o mesmo nome do fornecido em `config/config.json` e escolha Editar. 3. Diminua a capacidade desejada e mínima em 1. 4. Selecione Atualizar.	
Revise os registros.	Durante o evento de expansão, o NTH Pod isolará e drenará o nó de trabalho correspondente (a EC2 instância que será encerrada como parte do evento de expansão). Para verificar os registros, use o código na seção Informações adicionais.	Desenvolvedor de aplicativos, AWS DevOps, DevOps engenheiro

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpe todos os recursos da AWS.	Para limpar os recursos criados por esse padrão, execute o comando a seguir. `./uninstall.sh` Isso limpará todos os recursos criados nesse padrão excluindo a CloudFormation pilha.	DevOps engenheiro

Solução de problemas

Problema	Solução
O registro npm não está configurado corretamente.	Durante a instalação dessa solução, o script instala o npm install para baixar todos os pacotes necessários. Se, durante a instalação, você se deparar com uma mensagem que diz “Não é possível encontrar o módulo”, o registro npm pode não estar configurado corretamente. Para ver a configuração de registro atual, use o comando a seguir. `npm config get registry` Para definir o registro com `https://registry.npmjs.org/` , execute o seguinte comando.

Problema	Solução
	`npm config set registry https://registry.npmjs.org`
Atrasar a entrega de mensagens do SQS.	Como parte da solução de problemas, se quiser atrasar a entrega da mensagem SQS para o NTH Pod, você pode ajustar o parâmetro de atraso na entrega do SQS. Para obter mais informações, consulte Filas de atraso do Amazon SQS.

Recursos relacionados

- Código-fonte do Manipulador do término do nó da AWS
- EC2 oficina
- AWS CodePipeline
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Kit de desenvolvimento da Nuvem AWS
- AWS CloudFormation

Mais informações

1. Encontre o nome do NTH Pod.

```
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
```

2. Verificar os logs. Um log de exemplo se parece com o seguinte. Isso mostra que o nó foi isolado e drenado antes de enviar o sinal de conclusão do gancho do ciclo de vida do grupo do Auto Scaling.

```
kubectl -n kube-system logs aws-node-termination-handler-65445555-kbqc7
022/07/17 20:20:43 INF Adding new event to the event store
 event={"AutoScalingGroupName":"eksctl-my-cluster-target-nodegroup-
```

```
ng-10d99c89-NodeGroup-ZME36IGAP7O1","Description":"ASG Lifecycle Termination
 event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n","EndTime":"0001-01-01T00:00:00Z","EventID":"asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564","InProgress":fal
east-2.compute.internal","NodeProcessed":false,"Pods":null,"ProviderID":"aws:///us-
east-2c/i-0409f2a9d3085b80e","StartTime":"2022-07-17T20:20:42.702Z","State":""}
2022/07/17 20:20:44 INF Requesting instance drain event-id=asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564
 instance-id=i-0409f2a9d3085b80e kind=SQS_TERMINATE node-name=ip-192-168-75-60.us-
east-2.compute.internal provider-id=aws:///us-east-2c/i-0409f2a9d3085b80e
2022/07/17 20:20:44 INF Pods on node node_name=ip-192-168-75-60.us-
east-2.compute.internal pod_names=["aws-node-qchsw","aws-node-termination-
handler-65445555-kbqc7","kube-proxy-mz5x5"]
2022/07/17 20:20:44 INF Draining the node
2022/07/17 20:20:44 ??? WARNING: ignoring DaemonSet-managed Pods: kube-system/aws-node-
qchsw, kube-system/kube-proxy-mz5x5
2022/07/17 20:20:44 INF Node successfully cordoned and drained
 node_name=ip-192-168-75-60.us-east-2.compute.internal reason="ASG Lifecycle
 Termination event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n"
2022/07/17 20:20:44 INF Completed ASG Lifecycle Hook (NTH-K8S-TERM-HOOK) for instance
 i-0409f2a9d3085b80e
```

Compilar e implantar automaticamente uma aplicação em Java no Amazon EKS usando um pipeline de CI/CD

Criado por MAHESH RAGHUNANDANAN (AWS), James Radtke (AWS) e Jomcy Pappachen (AWS)

Resumo

Esse padrão descreve como criar um pipeline de integração contínua e entrega contínua (CI/CD) que cria e implanta automaticamente um aplicativo Java com as DevSecOps práticas recomendadas em um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) no. Nuvem AWS Esse padrão usa um aplicativo de saudação desenvolvido com uma estrutura Java Spring Boot e que usa o Apache Maven.

Você pode usar a abordagem deste padrão para compilar o código para um aplicativo Java, empacotar os artefatos do aplicativo como uma imagem do Docker, verificar a segurança da imagem e fazer o upload da imagem como um contêiner de workload no Amazon EKS. A abordagem deste padrão é útil se você quiser migrar de uma arquitetura monolítica fortemente acoplada para uma arquitetura de microsserviços. A abordagem também ajuda você a monitorar e gerenciar todo o ciclo de vida de um aplicativo Java, o que garante um nível mais alto de automação e ajuda a evitar erros ou bugs.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Command Line Interface (AWS CLI) versão 2, instalada e configurada. Para obter mais informações sobre isso, consulte Instalação ou atualização para a versão mais recente do AWS CLI na AWS CLI documentação.

  AWS CLI a versão 2 deve ser configurada com a mesma função AWS Identity and Access Management (IAM) que cria o cluster Amazon EKS, porque somente essa função está autorizada a adicionar outras funções do IAM ao `aws-authConfigMap`. Para obter informações e etapas de configuração AWS CLI, consulte Definindo configurações na AWS CLI documentação.
- Funções e permissões do IAM com acesso total AWS CloudFormation a. Para obter mais informações sobre isso, consulte Como controlar o acesso com o IAM na AWS CloudFormation documentação.

- Um cluster Amazon EKS existente, com detalhes do nome da função do IAM e do Amazon Resource Name (ARN) da função do IAM para nós de trabalho no cluster EKS.
- Kubernetes Cluster Autoscaler, instalado e configurado em seu cluster Amazon EKS. Para obter mais informações, consulte Dimensionar a computação de cluster com Karpenter e Cluster Autoscaler na documentação do Amazon EKS.
- Acesso ao código no GitHub repositório.

> **Important**
>
> AWS Security Hub é habilitado como parte dos AWS CloudFormation modelos incluídos no código desse padrão. Por padrão, depois que o Security Hub é ativado, ele vem com um teste gratuito de 30 dias. Após o teste, há um custo associado a isso AWS service (Serviço da AWS). Para obter mais informações sobre preços, consulte Preços do AWS Security Hub.

Versões do produto

- Helm versão 3.4.2 ou superior
- Apache Maven versão 3.6.3 ou mais recente
- BridgeCrew Checkov versão 2.2 ou posterior
- Aqua Security Trivy versão 0.37 ou mais recente

Arquitetura

Pilha de tecnologia

- AWS CodeBuild
- AWS CodeCommit

  Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais. No entanto, essa solução funcionará com qualquer provedor Git de sistema de controle de versão (VCS), GitHub como GitLab ou com alterações mínimas.
- Amazon CodeGuru
- AWS CodePipeline

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon EKS
- Amazon EventBridge
- AWS Security Hub
- Amazon Simple Notification Service (Amazon SNS)

Arquitetura de destino

O diagrama mostra o seguinte fluxo de trabalho:

1. O desenvolvedor atualiza o código do aplicativo Java na ramificação base do CodeCommit repositório, o que cria uma pull request (PR).
2. Assim que o PR é enviado, o Amazon CodeGuru Reviewer revisa automaticamente o código, o analisa com base nas melhores práticas de Java e fornece recomendações ao desenvolvedor.
3. Depois que o PR é mesclado com a filial base, um EventBridge evento da Amazon é criado.
4. O EventBridge evento inicia o CodePipeline pipeline, que começa.
5. CodePipeline executa o estágio de CodeSecurity digitalização (segurança contínua).
6. AWS CodeBuild inicia o processo de verificação de segurança no qual os arquivos Helm de implantação do Dockerfile e do Kubernetes são verificados usando o Checkov, e o código-fonte do aplicativo é escaneado com base em alterações incrementais no código. A verificação do código-fonte do aplicativo é realizada pelo wrapper da interface de linha de comando (CLI) do CodeGuru Reviewer.
7. Se o estágio de verificação de segurança for bem-sucedido, o estágio de compilação (integração contínua) será inicializado.
8. No estágio CodeBuild Build, cria o artefato, empacota o artefato em uma imagem do Docker, escaneia a imagem em busca de vulnerabilidades de segurança usando o Aqua Security Trivy e armazena a imagem no Amazon ECR.
9. As vulnerabilidades detectadas na etapa 8 são enviadas para o Security Hub para análise posterior por desenvolvedores ou engenheiros. O Security Hub fornece uma visão geral e recomendações para corrigir as vulnerabilidades.
10. As notificações por e-mail das fases sequenciais dentro do CodePipeline pipeline são enviadas pelo Amazon SNS.

11. Depois que as fases de integração contínua forem concluídas, CodePipeline entra no estágio de implantação (entrega contínua).
12. A imagem do Docker é implantada no Amazon EKS como uma workload de contêiner (pod) usando charts do Helm.
13. O pod do aplicativo é configurado com o agente Amazon CodeGuru Profiler, que envia os dados de perfil do aplicativo (CPU, uso do heap e latência) para o CodeGuru Profiler, o que ajuda os desenvolvedores a entender o comportamento do aplicativo.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeCommité um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.

  Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais
- O Amazon CodeGuru Profiler coleta dados de desempenho de tempo de execução de seus aplicativos ativos e fornece recomendações que podem ajudá-lo a ajustar o desempenho do seu aplicativo.
- O Amazon CodeGuru Reviewer usa análise de programas e aprendizado de máquina para detectar possíveis defeitos difíceis de serem encontrados pelos desenvolvedores e oferece sugestões para melhorar seu código Java e Python.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar as alterações de software continuamente.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.

- EventBridgeA Amazon é um serviço de barramento de eventos sem servidor que ajuda você a conectar seus aplicativos a dados em tempo real de várias fontes, incluindo AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras. Contas da AWS
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS. Também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outros serviços

- O Helm é um gerenciador de pacotes de código aberto para o Kubernetes.
- O Apache Maven é uma ferramenta de gerenciamento e compreensão de projetos de software.
- BridgeCrew O Checkov é uma ferramenta estática de análise de código para escanear a infraestrutura como arquivos de código (IaC) em busca de configurações incorretas que possam levar a problemas de segurança ou conformidade.
- O Aqua Security Trivy é um scanner abrangente para vulnerabilidades em imagens de contêineres, sistemas de arquivos e repositórios Git, além de problemas de configuração.

Código

O código desse padrão está disponível no GitHub aws-codepipeline-devsecops-amazoneksrepositório.

Práticas recomendadas

- Esse padrão segue as melhores práticas de segurança do IAM para aplicar o princípio de privilégio mínimo para entidades do IAM em todas as fases da solução. Se você quiser estender a solução com ferramentas adicionais Serviços da AWS ou de terceiros, recomendamos que você revise a seção sobre a aplicação de permissões de privilégios mínimos na documentação do IAM.

- Se você tiver vários aplicativos Java, recomendamos criar pipelines de CI/CD separados para cada aplicativo.
- Se você tiver um aplicativo monolítico, recomendamos que você divida o aplicativo em microsserviços sempre que possível. Os microsserviços são mais flexíveis, facilitam a implantação de aplicativos como contêineres e fornecem melhor visibilidade da compilação e implantação gerais do aplicativo.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Para clonar o repositório, execute o comando a seguir. `git clone https://github.com/aws-samples/aws-codepipeline-devsecops-amazoneks`	Desenvolvedor de aplicativos, DevOps engenheiro
Crie um bucket do S3 faça o upload do código.	1. Faça login no AWS Management Console, abra o console do Amazon S3 e, em seguida, crie um bucket S3 no local em Região da AWS que você planeja implantar essa solução. Para obter mais informações, consulte Criar um bucket na documentação do Amazon S3 2. No bucket do S3, crie uma pasta chamada `code`. 3. Navegue até onde você clonou o repositório.	AWS DevOps, administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	Para criar uma versão compactada do código inteiro com a extensão. zip (`cicdstack.zip`) e validar o arquivo.zip, execute os comandos a seguir na ordem.
	
	`cd aws-codepipeline-devsecops-amazoneks`
	`python -m zipfile -c cicdstack.zip *`
	`python -m zipfile -t cicdstack.zip`
	
	Note
	Se o `python` comando falhar e indicar que o Python não foi encontrado, use `python3` em vez disso.
	
	4. Faça upload do arquivo `cicdstack.zip` para a pasta de código que você criou anteriormente no bucket S3.	

Tarefa	Descrição	Habilidades necessárias
Crie uma AWS CloudFormation pilha.	1. Abra o console do AWS CloudFormation e escolha Create stack (Criar pilha). 2. Em Especificar modelo, escolha Fazer upload de um arquivo de modelo, faça o upload do arquivo `cf_templates/codecommit_ecr.yaml` e escolha Avançar. 3. Em Especificar detalhes da pilha, insira o nome da pilha e, em seguida, forneça os seguintes valores de parâmetros de entrada: • `CodeCommitRepositoryBranchName` : o nome da agência em que seu código residirá (o padrão é `main`) • `CodeCommitRepositoryName` : O nome do a CodeCommitrepository ser criado • `CodeCommitRepositoryS3Bucket` : o nome do bucket do S3 em que você criou a pasta de código • `CodeCommitRepositoryS3BucketObjKey` : `code/cicdstack.zip`	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• `ECRRepositoryName` : O nome do repositór io Amazon ECR a ser criado 4. Escolha Próximo, use as configurações padrão para Configurar opções de pilha e, em seguida, escolha Próximo. 5. Na seção Revisão, verifique os detalhes do modelo e da pilha e escolha Criar pilha. A pilha é então criada, incluindo os repositórios Amazon ECR CodeCommit e Amazon. 6. Anote os nomes dos repositórios CodeCommit e do Amazon ECR, que serão necessários para configurar o pipeline Java CI/CD.	
Valide a implantação da CloudFormation pilha.	1. Em Pilhas no CloudForm ation console, verifique o status da CloudFormation pilha que você implantou. O status da pilha deve ser CREATE COMPLETE. 2. No console, confirme se os repositórios CloudForm ation e o Amazon ECR foram provisionados e estão prontos.	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Exclua o bucket do S3.	Esvazie e exclua o bucket do S3 criado anteriormente. Para obter mais informações, consulte Excluir um bucket na documentação do Amazon S3	AWS DevOps, DevOps engenheiro

Configurar os charts do Helm

Tarefa	Descrição	Habilidades necessárias

Configure os charts do Helm do seu aplicativo Java.	1. No local em que você clonou o GitHub repositório, navegue até a pasta. `helm_charts/aws-proserve-java-greeting` Nessa pasta, o arquivo `values.dev.yaml` contém informações sobre a configuração dos recursos do Kubernetes que você pode modificar para suas implantações de contêineres no Amazon EKS. Atualize o parâmetro do repositório Docker fornecendo seu Conta da AWS ID e nome do repositório Amazon ECR. Região da AWS
	`image:`
	`  repository:`
	`  <account-id>.dkr.ecr.<region>.amazon`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	aws.com/<app-ecr-repo-name>
	2. O tipo de serviço do pod Java está definido como `LoadBalancer` .
	`service:`
	`type: LoadBalancer`
	`port: 80`
	`targetPort: 8080`
	`path: /hello`
	`initialDelaySeconds: 60`
	`periodSeconds: 30`
	Para usar um serviço diferente (por exemplo,`NodePort`), você pode alterar esse parâmetro. Para obter mais informações, consulte a documentação do Kubernetes.
	3. Você pode ativar o Ajustador de escala automático do pod horizontal do Kubernetes alterando o parâmetro `autoscaling` para `enabled: true`.
	`autoscaling:`
	`enabled: true`
	`minReplicas: 1`
	`maxReplicas: 100`	

Tarefa	Descrição	Habilidades necessárias
	<pre> targetCPUUtilizati onPercentage: 80 # targetMem oryUtilizationPerc entage: 80</pre> 4. Você pode habilitar recursos diferentes para as cargas de trabalho do Kubernetes alterando os valores no `values.<ENV>.yaml` arquivo, onde <ENV> está seu ambiente de desenvolvimento, produção, UAT ou QA.	

Tarefa	Descrição	Habilidades necessárias

Valide os charts do Helm em busca de erros de sintaxe.	1. No terminal, verifique se o Helm v3 está instalado em sua estação de trabalho local executando o seguinte comando.
	`helm --version`
	Se o Helm v3 não estiver instalado, instale-o.
	2. No terminal, navegue até o diretório de charts do Helm (`helm_charts/aws-proserve-java-greeting`) e execute o comando a seguir.
	`helm lint . -f values.dev.yaml`
	Ele verificará se há erros de sintaxe nos charts do Helm.
		DevOps engenheiro

Configure o pipeline Java CI/CD

Tarefa	Descrição	Habilidades necessárias
Crie o pipeline de CI/CD.	1. Abra o console do AWS CloudFormation e escolha Create stack (Criar pilha). 2. Em Especificar modelo, escolha Carregar um arquivo de modelo, carregue o modelo	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`cf_templates/build_deployment.yaml` e escolha Próximo. 3. Em Especificar detalhes da pilha, especifique o Nome da pilha e, em seguida, forneça os seguintes valores de parâmetros de entrada: • `CodeBranchName` : nome da ramificação do CodeCommit repositório em que seu código reside • `EKSClusterName` : nome do seu cluster EKS (não o `EKSCluster` ID) • `EKSCodeBuildAppName` : Nome do aplicativo Helm chart () `aws-proserve-java-greeting` • `EKSWorkerNodeRoleARN` : ARN da função do IAM atribuída aos nós de trabalho do Amazon EKS • `EKSWorkerNodeRoleName` : nome da função do IAM atribuída aos nós de trabalho do Amazon EKS • `EcrDockerRepository` : Nome do repositório Amazon ECR onde as imagens Docker do seu	

Tarefa	Descrição	Habilidades necessárias
	código serão armazenadas • `EmailRecipient` : Endereço de e-mail para o qual as notificações de criação devem ser enviadas • `EnvType`: Ambiente (por exemplo, desenvolvimento, teste ou produção) • `SourceRepoName` : nome do CodeCommit repositório em que seu código reside 4. Escolha Próximo. use as configurações padrão em Configurar opções de pilha e, em seguida, escolha Avançar. 5. Na seção Revisão, verifique os detalhes do CloudFormation modelo e da pilha e escolha Avançar. 6. Selecione Criar pilha. 7. Durante a implantação da CloudFormation pilha, o proprietário do endereço de e-mail que você forneceu nos parâmetros receberá uma mensagem para se inscrever em um tópico do SNS. Para assinar o	

Tarefa	Descrição	Habilidades necessárias
	Amazon SNS, o proprietá rio deve escolher o link na mensagem. 8. Depois que a pilha for criada, abra a guia Saídas da pilha e registre o valor do ARN para a chave de saída `EksCodeBu ildkubeRoleARN` . Esse valor do ARN do IAM será exigido posteriormente quando você fornecer permissões para a função do CodeBuild IAM implantar cargas de trabalho no cluster Amazon EKS.	

Ative a integração entre o Security Hub e o Aqua Security

Tarefa	Descrição	Habilidades necessárias
Ative a integração com o Aqua Security.	Essa etapa é necessária para fazer o upload das descobert as da vulnerabilidade de imagem do Docker relatadas pela Trivy para o Security Hub. Como AWS CloudForm ation não oferece suporte às integrações do Security Hub, esse processo deve ser feito manualmente.	Administrador e DevOps engenheiro da AWS

Tarefa	Descrição	Habilidades necessárias
	1. Abra o AWS Security Hub console e navegue até Integrações. 2. Procure por Aqua Security e selecione Aqua Security: Aqua Security. 3. Escolha Aceitar descobertas.	

Configure CodeBuild para executar os comandos Helm ou kubectl

Tarefa	Descrição	Habilidades necessárias
Permita CodeBuild a execução de comandos Helm ou kubectl no cluster Amazon EKS.	CodeBuild Para ser autenticado para usar o Helm ou `kubectl` comandos com o cluster Amazon EKS, você deve adicionar as funções do IAM ao. `aws-auth ConfigMap` Nesse caso, adicione o ARN da função do IAM `EksCodeBuildkubeRoleARN`, que é a função do IAM criada para que o CodeBuild serviço acesse o cluster do Amazon EKS e implante cargas de trabalho nele. Essa é uma atividade feita uma única vez. **Important** O procedimento a seguir deve ser	DevOps

Tarefa	Descrição	Habilidades necessárias

	concluído antes do estágio de aprovação da implantação em CodePipeline.
	
	1. Abra o script de shell `cf_templates/kube_aws_auth_configmap_patch.sh` em seu ambiente Amazon Linux ou macOS.
	2. Autentique-se no cluster do Amazon EKS executando o comando a seguir.
	
	`aws eks --region <aws-region> update-kubeconfig --name <eks-cluster-name>`
	
	3. Execute o script de shell usando o comando a seguir, substituindo `<rolearn-eks-codebuild-kubectl>` pelo valor ARN de `EksCodeBuildkubeRoleARN` que você registrou anteriormente.
	
	`bash cf_templates/kube_aws_auth_configmap_patch.sh <rolearn-eks-codebuild-kubectl>`	

Tarefa	Descrição	Habilidades necessárias
	O `aws_authConfigMap` está configurado e o acesso é concedido.	

Valide o pipeline de CI/CD.

Tarefa	Descrição	Habilidades necessárias

Verifique se o pipeline de CI/CD é inicializado automaticamente.	1. O estágio de CodeSecurity verificação no pipeline geralmente falhará se o Checkov detectar vulnerabilidades nos gráficos do Dockerfile ou do Helm. No entanto, o objetivo deste exemplo é estabelecer um processo de identificação de possíveis vulnerabilidades de segurança em vez de corrigi-las por meio do pipeline de CI/CD, normalmente um processo. DevSecOps No arquivo `buildspec/buildspec_secscan.yaml` , o comando `checkov` usa o sinalizador `--soft-fail` para evitar falhas no pipeline.
	
	`- echo -e "\n Running Dockerfile Scan"`
	`- checkov -f code/app/Dockerfile --framework dockerfile --`
		DevOps

Tarefa	Descrição	Habilidades necessárias
	soft-fail --summary-position bottom - echo -e "\n Running Scan of Helm Chart files" - cp -pv helm_charts/$EKS_CODEBUILD_APP_NAME/values.dev.yaml helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml - checkov -d helm_charts/$EKS_CODEBUILD_APP_NAME --framework helm --soft-fail --summary-position bottom - rm -rfv helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml Para que o pipeline falhe quando vulnerabilidades forem relatadas no Dockerfile e nos charts do Helm, a opção `--soft-fail` deve ser removida do comando `checkov`. Os desenvolvedores ou engenheiros podem então corrigir as vulnerabilidades e confirmar as alterações no repositório do CodeCommit código-fonte. 2. Semelhante ao CodeSecurity Scan, o estágio Build	

Tarefa	Descrição	Habilidades necessárias
	usa o Aqua Security Trivy para identificar `HIGH` vulnerabilidades de imagem do `CRITICAL` Docker antes de enviar o aplicativo para o Amazon ECR. `- AWS_REGION=$AWS_DEFAULT_REGION AWS_ACCOUNT_ID=$AWS_ACCOUNT_ID trivy -d image --no-progress --ignore-unfixed --exit-code 0 --severity HIGH,CRITICAL --format template --template "@securityhub/asff.tpl" -o securityhub/report.asff $AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/$IMAGE_REPO_NAME:$CODEBUILD_RESOLVED_SOURCE_VERSION`  Neste exemplo, o pipeline não falha quando as vulnerabilidades da imagem do Docker são relatadas, porque o `trivy` comando no `buildspec/buildspec.yml` arquivo inclui o sinalizador **`--exit-code`** com um valor de. `0` Para que o pipeline falhe quando `CRTICAL`	

Tarefa	Descrição	Habilidades necessárias
	as vulnerabilidades forem relatadas, `HIGH` altere o valor de `--exit-code` para`1`. Os desenvolvedores ou engenheiros podem então corrigir as vulnerabilidades e confirmar as alterações no repositório do CodeCommit código-fonte. 3. As vulnerabilidades de imagem do Docker relatadas pelo Aqua Security Trivy são enviadas para o Security Hub. No console do Security Hub, navegue até Findings. Filtre as descobertas com Record State = Active e Product = Aqua Security. Isso lista as vulnerabilidades da imagem do Docker no Security Hub. Pode levar de 15 minutos a uma hora para que as vulnerabilidades apareçam no Security Hub. Para obter mais informações sobre como iniciar o pipeline usando CodePipeline, consulte Iniciar um pipeline emCodePipeline, Iniciar um pipeline manualmente e Iniciar um pipeline em um cronogram	

Tarefa	Descrição	Habilidades necessárias
	a na CodePipeline documentação.	
Aprove a implantação.	1. Depois que a fase de compilação estiver concluída, haverá um portão de aprovação de implantação. O revisor ou gerente de lançamento deve inspecionar a compilação e, se todos os requisitos forem atendidos, aprová-la. Essa é a abordagem recomendada para equipes que usam entrega contínua para implantação de aplicativos. 2. Após a aprovação, o pipeline inicia o estágio de implantação. 3. Depois que o estágio de implantação for bem-sucedido, o CodeBuild log desse estágio fornecerá a URL do aplicativo. Use o URL para validar a disponibilidade do aplicativo.	DevOps

Tarefa	Descrição	Habilidades necessárias
Valide o perfil do aplicativo.	Depois que a implantação for concluída e o pod do aplicativo for implantado no Amazon EKS, o agente do Amazon CodeGuru Profiler que está configurado no aplicativo tentará enviar dados de perfil do aplicativo (CPU, resumo da pilha, latência e gargalos) para o Profiler. CodeGuru Para a implantação inicial de um aplicativo, o CodeGuru Profiler leva cerca de 15 minutos para visualizar os dados de criação de perfil.	AWS DevOps

Recursos relacionados

- AWS CodePipeline documentação
- Digitalizando imagens com o Trivy em uma AWS CodePipeline (postagem AWS do blog)
- Melhorando seus aplicativos Java usando o Amazon CodeGuru Profiler (postagem AWS no blog)
- AWS Sintaxe do Security Finding Format (ASFF)
- Padrões de EventBridge eventos da Amazon
- Atualização do Helm

Mais informações

- AWS CodeCommit não está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais. Essa solução também funcionará com qualquer provedor Git de sistema de controle de versão (VCS), GitHub como GitLab ou com alterações mínimas.

- CodeGuru O Profiler não deve ser confundido com o AWS X-Ray serviço em termos de funcionalidade. Recomendamos que você use o CodeGuru Profiler para identificar as linhas de código mais caras que podem causar gargalos ou problemas de segurança e corrigi-las antes que se tornem um risco potencial. O serviço X-Ray serve para monitoramento do desempenho de aplicativos.
- Neste padrão, as regras de eventos são associadas ao barramento de eventos padrão. Se necessário, você pode estender o padrão para usar um barramento de eventos personalizado.
- Esse padrão usa o CodeGuru Reviewer como uma ferramenta estática de teste de segurança de aplicativos (SAST) para o código do aplicativo. Você também pode usar esse pipeline para outras ferramentas, como SonarQube o Checkmarx. Você pode adicionar as instruções de configuração de escaneamento de qualquer uma dessas ferramentas `buildspec/buildspec_secscan.yaml` para substituir as instruções de CodeGuru escaneamento.

Crie uma definição de tarefa do Amazon ECS e monte um sistema de arquivos em EC2 instâncias usando o Amazon EFS

Criado por Durga Prasad Cheepuri (AWS)

Resumo

Esse padrão fornece exemplos de código e etapas para criar uma definição de tarefa do Amazon Elastic Container Service (Amazon ECS) que é executada em instâncias do Amazon Elastic Compute Cloud (EC2Amazon) na Amazon Web Services (AWS) Cloud, enquanto usa o Amazon Elastic File System (Amazon EFS) para montar um sistema de arquivos nessas instâncias. EC2 As tarefas do Amazon ECS que usam o Amazon EFS montam automaticamente os sistemas de arquivos que você especifica na definição de tarefa e disponibilizam esses sistemas de arquivos para os contêineres da tarefa em todas as zonas de disponibilidade em uma região da AWS.

Para atender aos seus requisitos de armazenamento persistente e armazenamento compartilhado, você pode usar o Amazon ECS e o Amazon EFS juntos. Por exemplo, você pode usar o Amazon EFS para armazenar dados persistentes de usuários e dados de aplicações para suas aplicações com pares de contêineres ECS ativos e em espera em execução em diferentes zonas de disponibilidade para alta disponibilidade. Você também pode usar o Amazon EFS para armazenar dados compartilhados que podem ser acessados paralelamente por contêineres do ECS e workloads distribuídas.

Para usar o Amazon EFS com o Amazon ECS, você pode adicionar uma ou mais definições de volume a uma definição de tarefa. Uma definição de volume inclui um ID do sistema de arquivos do Amazon EFS, ID do ponto de acesso e uma configuração para autorização do AWS Identity and Access Management (IAM) ou criptografia Transport Layer Security (TLS) em trânsito. Você pode usar as definições de contêiner nas definições de tarefas para especificar os volumes de definição de tarefas que são montados quando o contêiner é executado. Quando uma tarefa que usa um sistema de arquivos do Amazon EFS é executada, o Amazon ECS garante que o sistema de arquivos esteja montado e disponível para os contêineres que precisam acessá-lo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) com um endpoint de rede privada virtual (VPN) ou um roteador

- (Recomendado) Agente de contêiner do Amazon ECS 1.38.0 ou superior para compatibilidade com pontos de acesso do Amazon EFS e atributos de autorização do IAM (Para obter mais informações, consulte a postagem do blog da AWS Novo para Amazon EFS – Autorização do IAM e Pontos de acesso).

Limitações

- As versões do agente de contêiner do Amazon ECS anteriores à 1.35.0 não oferecem suporte aos sistemas de arquivos do Amazon EFS para tarefas que usam o EC2 tipo de execução.

Arquitetura

O diagrama a seguir mostra um exemplo de um aplicativo que usa o Amazon ECS para criar uma definição de tarefa e montar um sistema de arquivos do Amazon EFS em EC2 instâncias em contêineres do ECS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Criar um sistema de arquivos do Amazon EFS.
2. Crie uma definição de tarefa com um contêiner.
3. Configure as instâncias do contêiner para montar o sistema de arquivos do Amazon EFS. As definições de tarefa referenciam montagens de volume de modo que a instância de contêiner possa usar o sistema de arquivos Amazon EFS. As tarefas do ECS têm acesso ao mesmo sistema de arquivos do Amazon EFS, independentemente da instância de contêiner em que essas tarefas foram criadas.
4. Crie um serviço Amazon ECS com três instâncias da definição de tarefa.

Pilha de tecnologia

- Amazon EC2
- Amazon ECS
- Amazon EFS

Ferramentas

- Amazon EC2 — A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode usar EC2 a Amazon para lançar quantos servidores virtuais precisar e pode expandir ou aumentar a escala.
- Amazon ECS: o Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido para execução, interrupção e gerenciamento de contêineres em um cluster. Você pode executar tarefas e serviços em uma infraestrutura com tecnologia gerenciada pelo AWS Fargate. Como alternativa, para ter mais controle sobre sua infraestrutura, você pode executar suas tarefas e serviços em um cluster de EC2 instâncias que você gerencia.
- Amazon EFS: o Amazon Elastic File System (Amazon EFS) fornece um sistema de arquivos NFS elástico simples, escalável, totalmente gerenciável e pronto para uso com serviços de Nuvem AWS e atributos on-premises.
- AWS CLI: o AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto para interagir com serviços da AWS por meio de comandos em seu shell de linha de comando. Com configuração mínima, você pode executar comandos da AWS CLI que implementam funcionalidade equivalente àquela fornecida pelo Console de Gerenciamento da AWS baseado em navegador a partir de um prompt de comando.

Épicos

Criar um sistema de arquivos do Amazon EFS

Tarefa	Descrição	Habilidades necessárias
Crie um sistema de arquivos do Amazon EFS usando o Console de Gerenciamento da AWS.	1. **Note** Crie um sistema de arquivos do Amazon EFS e escolha a VPC que inclui seus contêineres. : se você usa uma VPC diferente, configure	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	uma conexão de emparelhamento de VPC. 2. Anote o ID do sistema de arquivos.	

Crie uma definição de tarefa do Amazon ECS usando um sistema de arquivos do Amazon EFS ou a AWS CLI

Tarefa	Descrição	Habilidades necessárias
Crie uma definição de tarefa usando um sistema de arquivos do Amazon EFS.	Crie uma definição de tarefa usando o novo console do Amazon ECS ou o console clássico do Amazon ECS com as seguintes configurações: • Se você usa o novo console, escolha EC2 instâncias da Amazon para o ambiente de aplicativos. Se você usa o console clássico, escolha EC2como o tipo de lançamento. • Adicione um volume. Insira um nome para o volume, escolha EFS para o tipo de volume e, em seguida, escolha a ID do sistema de arquivos que você anotou anteriormente. Para o diretório raiz, escolha o caminho do sistema de	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	arquivos do Amazon EFS que você deseja hospedar no host de contêineres do Amazon ECS.	

Tarefa	Descrição	Habilidades necessárias

Crie uma definição de tarefa usando a AWS CLI.	1. Para criar um modelo JSON com espaços reservados para parâmetros de entrada para a definição de tarefa, execute o seguinte comando:
	`aws ecs register-task-definition --generate-cli-skeleton`
	2. Execute o seguinte comando para criar a definição de tarefa com o modelo JSON:
	`aws ecs register-task-definition --cli-input-json file://<path_to_your_json_file>`
	3. **Note**
	Insira os parâmetros de entrada em seu modelo JSON com base no arquivo `task_definition_parameters.json` (anexado). : Para obter mais informações sobre parâmetros de entrada, consulte
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Parâmetros de definição de tarefas (documentação do Amazon ECS) e register-task-definition(AWS CLI Command Reference).	

Recursos relacionados

- Definições de tarefa do Amazon ECS
- Volumes do Amazon EFS

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Implantar funções do Lambda com imagens de contêiner

Criado por Ram Kandaswamy (AWS)

Resumo

AWS Lambda oferece suporte a imagens de contêineres como modelo de implantação. Esse padrão mostra como implantar funções do Lambda por meio de imagens de contêiner.

O Lambda é um serviço de computação com tecnologia sem servidor e orientado a eventos que você pode usar para executar código para praticamente qualquer tipo de aplicativo ou serviço de backend sem provisionar ou gerenciar servidores. Com o suporte a imagens de contêiner para funções do Lambda, você obtém os benefícios de até 10 GB de armazenamento para o artefato do seu aplicativo e a capacidade de usar ferramentas familiares de desenvolvimento de imagens de contêiner.

O exemplo desse padrão usa Python como linguagem de programação subjacente, mas você pode usar outras linguagens, como Java, Node.js ou Go. Para a fonte, considere um sistema baseado em Git GitHub, como, ou Bitbucket GitLab, ou use o Amazon Simple Storage Service (Amazon S3).

Pré-requisitos e limitações

Pré-requisitos

- Amazon Elastic Container Registry (Amazon ECR) ativado
- Código do aplicativo
- Imagens do Docker com o cliente de interface de runtime e a versão mais recente do Python
- Conhecimento prático do Git

Limitações

- O tamanho máximo de imagem suportado é 10 GB.
- O runtime máximo para uma implantação de contêiner baseado em Lambda é de 15 minutos.

Arquitetura

Arquitetura de destino

1. Você cria um repositório Git e confirma o código do aplicativo no repositório.
2. O AWS CodeBuild projeto é acionado por alterações de confirmação.
3. O CodeBuild projeto cria a imagem do Docker e publica a imagem criada no Amazon ECR.
4. Você cria a função Lambda usando a imagem no Amazon ECR.

Automação e escala

Esse padrão pode ser automatizado usando AWS CloudFormation AWS Cloud Development Kit (AWS CDK), ou operações de API de um SDK. O Lambda pode ser escalado automaticamente com base no número de solicitações, e você pode ajustá-lo usando os parâmetros de simultaneidade. Para obter mais informações, consulte a documentação do Lambda.

Ferramentas

Serviços da AWS

- AWS CloudFormationNa AWS, CloudFormationhelps você configura AWS recursos, os provisiona de forma rápida e consistente e os gerencia durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS Esse padrão usa o AWS CloudFormation Application Composer, que ajuda você a visualizar e editar AWS CloudFormation modelos visualmente.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- GitHub, GitLab, e o Bitbucket são alguns dos sistemas de controle de código-fonte baseados em Git comumente usados para acompanhar as alterações no código-fonte.

Práticas recomendadas

- Torne sua função o mais eficiente e reduzida possível para evitar o carregamento de arquivos desnecessários.
- Esforce-se para ter camadas estáticas no topo da sua lista de arquivos do Docker e coloque as camadas que mudam com mais frequência na parte inferior. Isso melhora o armazenamento em cache, o que aumenta o desempenho.
- O proprietário da imagem é responsável por atualizar e corrigir a imagem. Adicione essa cadência de atualização aos seus processos operacionais. Para obter mais informações, consulte a documentação do AWS Lambda.

Épicos

Crie um projeto em CodeBuild

Tarefa	Descrição	Habilidades necessárias
Crie um repositório Git.	Crie um repositório Git que conterá o código-fonte do aplicativo, o Dockerfile e o arquivo. `buildspec.yaml`	Desenvolvedor
Crie um CodeBuild projeto.	Para usar um CodeBuild projeto para criar a imagem Lambda personalizada, faça o seguinte: 1. Faça login no e abra AWS Management Console o CodeBuild console em https://console.aws.amazon.com/codesuite/codebuild/. 2. Criar um novo projeto da . Como fonte, escolha o repositório Git que você criou. Para obter informaçõ	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	es sobre os diferentes tipos de integração do repositório Git, consulte a documenta ção Como trabalhar com conexões. 3. Confirme se o modo privilegiado está ativado. Isso é necessário para criar imagens do Docker. Caso contrário, a imagem não será criada com êxito. 4. Forneça valores para o nome e a descrição do projeto.	
Edite o Dockerfile.	O Dockerfile deve estar localizado no diretório de nível superior em que você está desenvolvendo o aplicativo. O código Python deve estar na pasta `src`. Ao criar imagens, use as imagens oficiais suportadas pelo Lambda. Caso contrário, ocorrerá um erro de bootstrap , dificultando o processo de empacotamento. Para obter detalhes, consulte a seção Informações adicionais.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Crie um repositório do Amazon ECR.	Crie um repositório de contêineres no Amazon ECR. No exemplo de comando a seguir, o nome do repositório criado é `cf-demo`: `aws ecr create-repository --cf-demo` O repositório será referenciado no `buildspec.yaml` arquivo.	Administrador da AWS, desenvolvedor
Envie a imagem para o Amazon ECR.	Você pode usar CodeBuild para realizar o processo de criação de imagens. CodeBuild precisa de permissão para interagir com o Amazon ECR e trabalhar com o S3. Como parte do processo, a imagem do Docker é criada e enviada para o registro do Amazon ECR. Para obter detalhes sobre o modelo e o código, consulte a seção Informações adicionais.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Verifique se a imagem está no repositório.	Para verificar se a imagem está no repositório, selecione Repositórios no console do Amazon ECR. A imagem deve ser listada, com tags e com os resultados de um relatório de verificação de vulnerabilidade, caso esse atributo tenha sido ativado nas configurações do Amazon ECR. Para obter mais informações, consulte a documentação da AWS.	Desenvolvedor

Crie a função do Lambda para executar a imagem

Tarefa	Descrição	Habilidades necessárias
Criar a função do Lambda.	No console do Lambda, selecione Criar função e, em seguida, selecione Imagem do contêiner. Insira o nome da função e o URI da imagem que está no repositório do Amazon ECR e selecione Criar função. Para obter mais informações, consulte a documentação do AWS Lambda.	Desenvolvedor de aplicativos
Testar a função do Lambda.	Para invocar e testar a função, escolha Testar. Para obter mais informações, consulte a documentação do AWS Lambda.	Desenvolvedor de aplicativos

Solução de problemas

Problema	Solução
A construção não está sendo bem-sucedida.	1. Verifique se o modo privilegiado está ativado para o CodeBuild projeto. 2. Certifique-se de que os comandos relacionados ao Docker tenham as permissões necessárias. Tente adicionar `sudo` aos comandos. 3. Verifique se a função do IAM associada à CodeBuild tem uma política com ações apropriadas para interagir com o Amazon ECR, o Amazon S3 e os registros. CloudWatch

Recursos relacionados

- Imagens de base para o Lambda
- Amostra do Docker para CodeBuild
- Passe credenciais temporárias

Mais informações

Edite o Dockerfile

O código a seguir mostra os comandos que você edita no Dockerfile:

```
FROM public.ecr.aws/lambda/python:3.xx

# Copy function code
COPY app.py ${LAMBDA_TASK_ROOT}
COPY requirements.txt  ${LAMBDA_TASK_ROOT}

# install dependencies
RUN pip3 install --user -r requirements.txt
```

```
# Set the CMD to your handler (could also be done as a parameter override outside of
 the Dockerfile)
CMD [ "app.lambda_handler" ]
```

No FROM comando, use o valor apropriado para a versão do Python compatível com o Lambda (por exemplo,). 3.12 Essa será a imagem base que estará disponível no repositório público de imagens do Amazon ECR.

O comando COPY app.py ${LAMBDA_TASK_ROOT} copia o código para o diretório raiz da tarefa, que a função do Lambda usará. Esse comando usa a variável de ambiente para que não precisemos nos preocupar com o caminho real. A função a ser executada é passada como argumento para o comando CMD ["app.lambda_handler"].

O comando COPY requirements.txt captura as dependências necessárias para o código.

O comando RUN pip install --user -r requirements.txt instala as dependências no diretório local do usuário.

Para construir sua imagem, execute o seguinte comando.

```
docker build -t <image name> .
```

Adicione a imagem no Amazon ECR

No código a seguir, substitua aws_account_id pelo número da conta e substitua us-east-1 se você estiver usando uma região diferente. O buildspec arquivo usa o número da CodeBuild compilação para identificar de forma exclusiva as versões da imagem como um valor de tag. Você pode alterar isso de acordo com as suas necessidades.

O código personalizado do buildspec

```
phases:
  install:
    runtime-versions:
       python: 3.xx
  pre_build:
    commands:
      - python3 --version
      - pip3 install --upgrade pip
      - pip3 install --upgrade awscli
      - sudo docker info
```

```
  build:
    commands:
      - echo Build started on `date`
      - echo Building the Docker image...
      - ls
      - cd app
      - docker build -t cf-demo:$CODEBUILD_BUILD_NUMBER .
      - docker container ls
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker image...
      - aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.us-east-1.amazonaws.com
      - docker tag cf-demo:$CODEBUILD_BUILD_NUMBER aws_account_id.dkr.ecr.us-
east-1.amazonaws.com/cf-demo:$CODEBUILD_BUILD_NUMBER
      - docker push aws_account_id.dkr.ecr.us-east-1.amazonaws.com/cf-demo:
$CODEBUILD_BUILD_NUMBER
```

Implante microsserviços Java no Amazon ECS usando o AWS Fargate

Criado por Vijay Thompson (AWS) e Sandeep Bondugula (AWS)

Resumo

Esse padrão fornece orientação para implantar microsserviços Java em contêineres no Amazon Elastic Container Service (Amazon ECS) usando o AWS Fargate. O padrão não usa o Amazon Elastic Container Registry (Amazon ECR) para gerenciamento de contêineres; em vez disso, as imagens do Docker são extraídas do hub do Docker.

Pré-requisitos e limitações

Pré-requisitos

- Um aplicativo de microsserviços Java existente em um hub do Docker
- Um repositório público do Docker
- Uma conta AWS ativa
- Familiaridade com os serviços da AWS, incluindo Amazon ECS e Fargate
- Estrutura Docker, Java e Spring Boot
- Amazon Relational Database Service (Amazon RDS) instalado e em execução (opcional)
- Uma nuvem privada virtual (VPC) se o aplicativo exigir o Amazon RDS (opcional)

Arquitetura

Pilha de tecnologia de origem

- Microsserviços Java (por exemplo, implementados no Spring Boot) e implantados no Docker

Arquitetura de origem

Pilha de tecnologias de destino

- Um cluster do Amazon ECS que hospeda cada microsserviço usando o Fargate
- Uma rede VPC para hospedar o cluster do Amazon ECS e os grupos de segurança associados
- Uma definição de cluster/tarefa para cada microsserviço que gera contêineres usando o Fargate

Arquitetura de destino

Ferramentas

Ferramentas

- O Amazon ECS elimina a necessidade de instalar e operar seu próprio software de orquestração de contêineres, gerenciar e escalar um cluster de máquinas virtuais ou programar contêineres nessas máquinas virtuais.
- O AWS Fargate ajuda você a executar contêineres sem precisar gerenciar servidores ou instâncias do Amazon Elastic Compute Cloud (Amazon). EC2 É usado em conjunto com o Amazon Elastic Container Service (Amazon ECS).
- Docker é uma plataforma de software que permite criar, testar e implantar aplicativos rapidamente. O Docker empacota o software em unidades padronizadas chamadas contêineres que têm tudo o que o software precisa para ser executado, incluindo bibliotecas, ferramentas do sistema, código e runtime.

Código Docker

O Dockerfile a seguir especifica a versão do Java Development Kit (JDK) usada, onde o arquivo Java (JAR) existe, o número da porta exposta e o ponto de entrada do aplicativo.

```
FROM openjdk:11
ADD target/Spring-docker.jar Spring-docker.jar
EXPOSE 8080
ENTRYPOINT ["java","-jar","Spring-docker.jar"]
```

Épicos

Criar novas definições de tarefa

Tarefa	Descrição	Habilidades necessárias
Crie uma definição de tarefa.	É necessária uma definição de tarefa para executar contêineres do Docker no Amazon ECS. Abra o console do	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Amazon ECS em https://console.aws.amazon.com/ecs/, escolha Definições de tarefas e, em seguida, crie uma nova definição de tarefa. Para obter mais informações, consulte a documentação do Amazon ECS.	
Escolha o tipo de inicialização.	Escolha Fargate como o tipo de inicialização.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Configure a tarefa.	Defina um nome de tarefa e configure o aplicativo com a quantidade adequada de memória de tarefa e CPU.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Defina o contêiner.	Especifique o nome do contêiner. Para a imagem, insira o nome do site do Docker, o nome do repositório e o nome da tag da imagem do Docker (`docker.io/sample-repo/sample-application:sample-tag-name`). Defina limites de memória para o aplicativo e configure mapeamentos de portas (`8080, 80`) para as portas permitidas.	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Crie a tarefa.	Quando as configurações da tarefa e do contêiner estiverem prontas, crie a tarefa. Para obter instruções detalhadas, consulte os links na seção Recursos relaciona dos.	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Configurar o cluster

Tarefa	Descrição	Habilidades necessárias
Criar e configurar um cluster.	Escolha Rede somente como o tipo de cluster, configure o nome e, em seguida, crie o cluster ou use um cluster existente, se disponível. Para obter mais informações, consulte a documentação do Amazon ECS.	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Configurar tarefa

Tarefa	Descrição	Habilidades necessárias
Crie uma tarefa do .	Dentro do cluster, escolha Executar nova tarefa.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Escolha o tipo de inicialização.	Escolha Fargate como o tipo de inicialização.	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Escolha a definição da tarefa, a revisão e a versão da plataforma.	Escolha a tarefa que você deseja executar, a revisão da definição da tarefa e a versão da plataforma.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Selecione o cluster.	Escolha o cluster do qual você deseja executar a tarefa.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Especifique o número de tarefas.	Configure o número de tarefas que devem ser executada s. Se você estiver iniciando com duas ou mais tarefas, é necessário um balanceador de carga para distribuir o tráfego entre as tarefas.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Especifique o grupo de tarefas.	(Opcional) Especifique um nome de grupo de tarefas para identificar um conjunto de tarefas relacionadas como um grupo de tarefas.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Configure as sub-redes e os grupos de segurança da VPC do cluster.	Configure a VPC do cluster e as sub-redes nas quais você deseja implantar a aplicação . Crie ou atualize grupos de segurança (HTTP, HTTPS e porta 8080) para fornecer acesso às conexões de entrada e saída.	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Defina as configurações de IP público.	Ative ou desative o IP público, dependendo da sua necessidade de em usar um endereço IP público para tarefas do Fargate. Por padrão, a opção recomendada é Ativado.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Revise as configurações e crie a tarefa.	Revise as configurações e, em seguida, escolha Concluir.	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Substituir

Tarefa	Descrição	Habilidades necessárias
Copie o URL do aplicativo.	Quando o status da tarefa for atualizado para Em execução, selecione a tarefa. Na seção Rede, copie o IP público.	Administrador de sistemas da AWS, desenvolvedor de aplicativos
Testar seu aplicativo	No seu navegador, insira o IP público para testar o aplicativo.	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Recursos relacionados

- Noções básicas do Docker para Amazon ECS (documentação do Amazon ECS)
- Amazon ECS no AWS Fargate (documentação do Amazon ECS)
- Criação de uma definição de tarefa (documentação do Amazon ECS)
- Criação de um cluster (documentação do Amazon ECS)
- Configurando parâmetros básicos de serviço (documentação do Amazon ECS)
- Configurando uma rede (documentação do Amazon ECS)
- Implantação de microsserviços Java no Amazon ECS (postagem do blog)

Implante recursos e pacotes do Kubernetes usando o Amazon EKS e um repositório de charts do Helm no Amazon S3

Criado por Sagar Panigrahi (AWS)

Resumo

Esse padrão ajuda você a gerenciar aplicativos Kubernetes com eficiência, independentemente de sua complexidade. O padrão integra o Helm aos pipelines existentes de integração e entrega contínuas (CI/CD) para implantar aplicativos em um cluster do Kubernetes. Helm é um gerenciador de pacotes Kubernetes que ajuda a gerenciar aplicativos Kubernetes. Os charts do Helm ajudam a definir, instalar e atualizar aplicativos Kubernetes complexos. Os gráficos (charts) podem ser versionados e armazenados nos repositórios do Helm, o que melhora o tempo médio de restauração (MTTR) durante interrupções.

Esse padrão usa o Amazon Elastic Kubernetes Service (Amazon EKS) para o cluster do Kubernetes. Ele usa o Amazon Simple Storage Service (Amazon S3) como um repositório de charts do Helm, para que os gráficos possam ser gerenciados e acessados centralmente por desenvolvedores em toda a organização.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS) com uma nuvem privada virtual (VPC)
- Um cluster do Amazon EKS
- Nós de trabalho configurados dentro do cluster do Amazon EKS e prontos para receber workloads
- Kubectl para configurar o arquivo kubeconfig do Amazon EKS para o cluster de destino na máquina cliente
- Acesso ao AWS Identity and Access Management (IAM) para criar o bucket S3
- Acesso por IAM (programático ou por perfil) ao Amazon S3 a partir da máquina cliente
- Gerenciamento de código-fonte e pipeline de CI/CD

Limitações

- No momento, não há suporte para atualizar, excluir ou gerenciar definições de recursos personalizados ()CRDs.

- Se você estiver usando um recurso que se refere a um CRD, o CRD deverá ser instalado separadamente (fora do gráfico).

Versões do produto

- Helm v3.6.3

Arquitetura

Pilha de tecnologias de destino

- Amazon EKS
- Amazon VPC
- Amazon S3
- Gerenciamento de código-fonte
- Helm
- Kubectl

Arquitetura de destino

Automação e escala

- A AWS CloudFormation pode ser usada para automatizar a criação da infraestrutura. Para obter mais informações, consulte Criação de recursos do Amazon EKS com a AWS CloudFormation na documentação do Amazon EKS.
- O Helm deve ser incorporado à sua ferramenta de automação de CI/CD existente para automatizar o empacotamento e o versionamento dos charts do Helm (fora do escopo desse padrão).
- GitVersion ou os números de compilação do Jenkins podem ser usados para automatizar o controle de versão dos gráficos.

Ferramentas

Ferramentas

- Amazon EKS: o Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço gerenciado para executar o Kubernetes na AWS sem a necessidade de criar ou manter seu próprio ambiente de gerenciamento do Kubernetes. O Kubernetes é um sistema de código aberto para automatizar a implantação, a escalabilidade e o gerenciamento de aplicações em contêineres.
- Helm: é um gerenciador de pacotes Helm para o Kubernetes que ajuda a instalar e gerenciar aplicações em seu cluster do Kubernetes.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.
- Kubectl: o Kubectl é um utilitário de linha de comando para executar comandos em clusters do Kubernetes.

Código

O código de exemplo está anexado.

Épicos

Configurar e inicializar o Helm

Tarefa	Descrição	Habilidades necessárias
Instale o cliente Helm.	Para baixar e instalar o cliente do Helm em seu sistema local, use o comando a seguir. `sudo curl https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 | bash`	DevOps engenheiro
Valide a instalação do Helm.	Para validar se o Helm é capaz de se comunicar com o servidor da API Kubernetes dentro do cluster do	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Amazon EKS, execute `helm version`.	

Crie e instale um chart do Helm no cluster do Amazon EKS

Tarefa	Descrição	Habilidades necessárias
Crie um chart do Helm para o NGINX.	Para criar um chart do Helm nomeado `my-nginx` na máquina cliente, execute `helm create my-nginx`.	DevOps engenheiro
Analise a estrutura do gráfico.	Para revisar a estrutura do gráfico, execute o comando de árvore `tree my-nginx/` .	DevOps engenheiro
Desative a criação de contas de serviço no gráfico.	Em `values.yaml` , abaixo da seção `serviceAccount` , defina a chave `create` como `false`. Essa opção está desativada porque não há necessidade de criar uma conta de serviço para esse padrão.	DevOps engenheiro
Valide (lint) o gráfico modificado em busca de erros sintáticos.	Para validar o gráfico em busca de qualquer erro sintático antes de instalá-lo no cluster de destino, execute `helm lint my-nginx/` .	DevOps engenheiro
Instale o gráfico para implantar recursos do Kubernetes.	Para executar a instalação do chart do Helm, use o comando a seguir.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`helm install --name my-nginx-release --debug my-nginx/ --namespace helm-space` O sinalizador opcional `debug` gera todas as mensagens de depuração durante a instalação. O sinalizador `namespace` especifica o namespace no qual a parte de recursos desse gráfico será criada.	
Revise os recursos no cluster do Amazon EKS.	Para revisar os recursos que foram criados como parte do chart do Helm no namespace `helm-space`, use o comando a seguir. `kubectl get all -n helm-space`	DevOps engenheiro

Reverta para uma versão anterior de um aplicativo do Kubernetes

Tarefa	Descrição	Habilidades necessárias
Modifique e atualize a versão.	Para modificar o gráfico, em `values.yaml`, altere o valor de `replicaCount` para 2. Em seguida, atualize a versão já instalada executando o seguinte comando.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`helm upgrade my-nginx-release my-nginx/ --namespace helm-space`	
Analise o histórico de versões do Helm.	Para listar todas as revisões de uma versão específica que foram instaladas usando o Helm, execute o comando a seguir. `helm history my-nginx-release`	DevOps engenheiro
Revise os detalhes de uma revisão específica.	Antes de mudar ou reverter para uma versão funcional e para obter uma camada adicional de validação antes de instalar uma revisão, veja quais valores foram passados para cada uma das revisões usando o comando a seguir. `helm get --revision=2 my-nginx-release`	DevOps engenheiro
Reverta para uma versão anterior.	Para reverter para uma revisão anterior, use o comando a seguir. `helm rollback my-nginx-release 1` Este exemplo está revertendo para a revisão número 1.	DevOps engenheiro

Inicializar um bucket do S3 como um repositório do Helm

Tarefa	Descrição	Habilidades necessárias
Crie um bucket do S3 para charts do Helm.	Crie um bucket exclusivo do S3. No bucket, crie uma pasta denominada `charts`. O exemplo desse padrão usa `s3://my-helm-charts/charts` como repositório do gráfico de destino.	Administrador de nuvem
Instale o plug-in do Helm para o Amazon S3.	Para instalar o plug-in helm-s3 na máquina cliente, use o comando a seguir. `helm plugin install https://github.com/hypnoglow/helm-s3.git --version 0.10.0` Observação: o suporte ao Helm V3 está disponível com a versão 0.9.0 e superior do plugin.	DevOps engenheiro
Inicialize o repositório do Helm no Amazon S3.	Para inicializar a pasta de destino como um repositório do Helm, use o comando a seguir. `helm S3 init s3://my-helm-charts/charts` O comando cria um arquivo `index.yaml` no destino para rastrear todas as	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	informações do gráfico armazenadas nesse local.	
Adicione o repositório do Amazon S3 ao Helm.	Para adicionar o repositór io na máquina cliente, use o comando a seguir. `helm repo add my-helm-charts s3://my-helm-charts/charts` Esse comando adiciona um alias ao repositório de destino na máquina cliente do Helm.	DevOps engenheiro
Revise a lista de repositórios.	Para ver a lista de repositórios na máquina cliente do Helm, execute `helm repo list`.	DevOps engenheiro

Empacote e armazene gráficos no repositório do Helm no Amazon S3

Tarefa	Descrição	Habilidades necessárias
Embalar o gráfico.	Para empacotar o gráfico `my-nginx` que você criou, execute `helm package ./my-nginx/` . O comando empacota todo o conteúdo da pasta do gráfico `my-nginx` em um arquivo, que é nomeado usando o número da versão mencionado no arquivo `Chart.yaml` .	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Armazene o pacote no repositório do Helm no Amazon S3.	Para fazer o upload do pacote para o repositório do Helm no Amazon S3, execute o comando a seguir, usando o nome correto do arquivo `.tgz`. `helm s3 push ./my-nginx-0.1.0.tgz my-helm-charts`	DevOps engenheiro
Pesquise pelo chart do Helm.	Para confirmar se o gráfico aparece localmente e no repositório do Helm no Amazon S3, execute o comando a seguir. `helm search repo my-nginx`	DevOps engenheiro

Modificar, criar versões e empacotar um gráfico

Tarefa	Descrição	Habilidades necessárias
Modificar e embalar o gráfico.	Em `values.yaml` , defina o valor `replicaCount` como `1`. Em seguida, empacote o gráfico executando `helm package ./my-nginx/` , desta vez alterando a versão de `Chart.yaml` para `0.1.1`.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	O controle de versão é idealmente atualizado por meio da automação usando ferramentas como GitVersion números de compilação do Jenkins em um pipeline de CI/CD. A automação do número da versão está fora do escopo desse padrão.	
Envie a nova versão para o repositório do Helm no Amazon S3.	Para enviar o novo pacote com a versão 0.1.1 para o repositório `my-helm-charts` do Helm no Amazon S3, execute o comando a seguir. `helm s3 push ./my-nginx-0.1.1.tgz my-helm-charts`	DevOps engenheiro

Pesquise e instale um gráfico do repositório do Helm no Amazon S3

Tarefa	Descrição	Habilidades necessárias
Pesquise todas as versões do gráfico my-nginx.	Para ver todas as versões disponíveis de um gráfico, execute o comando a seguir com o sinalizador `--versions` . `helm search repo my-nginx --versions`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Sem o sinalizador, o Helm, por padrão, exibe a versão mais recente carregada de um gráfico.	
Instale um gráfico do repositório do Helm no Amazon S3.	Os resultados da pesquisa da tarefa anterior mostram as várias versões do gráfico `my-nginx`. Para instalar a nova versão (0.1.1) do repositório do Helm no Amazon S3, use o comando a seguir. `helm upgrade my-nginx-release my-helm-charts/my-nginx --version 0.1.1 --namespace helm-space`	DevOps engenheiro

Recursos relacionados

- Documentação do HELM
- Plug-in helm-s3 (licença MIT)
- Binário do cliente do HELM
- Documentação do Amazon EKS

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Implante um exemplo de microsserviço Java no Amazon EKS e exponha o microsserviço usando um Application Load Balancer

Criado por Vijay Thompson (AWS) e Akkamahadevi Hiremath (AWS)

Resumo

Esse padrão descreve como implantar um microsserviço Java de exemplo como uma aplicação em contêiner no Amazon Elastic Kubernetes Service (Amazon EKS) usando o utilitário de linha de comando `eksctl` e o Amazon Elastic Container Registry (Amazon ECR). Você pode usar um Application Load Balancer para balancear a carga do tráfego do aplicativo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) versão 1.7 ou mais recente, instalada e configurada no macOS, Linux ou Windows
- Um daemon do Docker em execução
- O utilitário de linha de comando `eksctl`, instalado e configurado no macOS, Linux ou Windows (para obter mais informações, consulte Conceitos básicos do Amazon EKS – eksctl na documentação do Amazon EKS.)
- O utilitário de linha de comando `kubectl`, instalado e configurado no macOS, Linux ou Windows (para obter mais informações, consulte Instalar ou atualizar kubectl na documentação do Amazon EKS.)

Limitações

- Esse padrão não abrange a instalação de um certificado SSL para o Application Load Balancer.

Arquitetura

Pilha de tecnologias de destino

- Amazon ECR

- Amazon EKS
- Elastic Load Balancing

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para a conteinerização de um microsserviço Java no Amazon EKS.

Ferramentas

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O Elastic Load Balancing distribui automaticamente seu tráfego de entrada entre vários destinos, como instâncias, contêineres e endereços IP do EC2 Amazon Elastic Compute Cloud (Amazon), em uma ou mais zonas de disponibilidade.
- O eksctl ajuda você a criar clusters no Amazon EKS.
- O kubectl possibilita a execução de comandos nos clusters do Kubernetes.
- O Docker ajuda você a criar, testar e entregar aplicativos em pacotes chamados contêineres.

Épicos

Crie de um cluster do Amazon EKS usando eksctl

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do Amazon EKS.	Para criar um cluster do Amazon EKS que usa duas EC2 instâncias t2.small da Amazon como nós, execute o seguinte comando:	Desenvolvedor, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
	`eksctl create cluster --name <your-cluster-name> --version <version-number> --nodes=1 --node-type=t2.small` **Note** O processo pode levar de 15 a 20 minutos. Depois que o cluster é criado, a configuração apropriada do Kubernetes é adicionada ao seu arquivo kubeconfig. Você pode usar o arquivo `kubeconfig` com `kubectl` para implantar o aplicativo em etapas posteriores.	
Verifique o cluster do Amazon EKS.	Para verificar se o cluster foi criado e se você pode se conectar a ele, execute o comando `kubectl get nodes`.	Desenvolvedor, administrador do sistema

Crie um repositório Amazon ECR e envie a imagem do Docker.

Tarefa	Descrição	Habilidades necessárias
Crie um repositório do Amazon ECR.	Siga as instruções em Criar um repositório privado na	Desenvolvedor, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
	documentação do Amazon ECR.	
Crie um arquivo XML POM.	Crie um arquivo `pom.xml` com base no código de arquivo POM de exemplo na seção Additional information desse padrão.	Desenvolvedor, administrador do sistema

Tarefa	Descrição	Habilidades necessárias

Criar um arquivo de origem.	Crie um arquivo de origem chamado `HelloWorld.java` no caminho `src/main/java/eksExample` com base no exemplo a seguir:
	`package eksExample;`
	`import static spark.Spark.get;`
	`public class HelloWorld {`
	`  public static void main(String[] args) {`
	`  get("/", (req, res) -> {`
	`  return "Hello World!";`
	`  });`
	`  }`
	`}`
	Certifique-se de usar a seguinte estrutura de diretório:
	`### Dockerfile`
	`### deployment.yaml`
	`### ingress.yaml`
	`### pom.xml`
	`### service.yaml`
	`### src`
	`  ### main`
	`  ### java`
	`  ### eksExample`
	`  ### HelloWorld.java`	

Tarefa	Descrição	Habilidades necessárias
Crie um Dockerfile.	Crie um `Dockerfile` com base no código de Exemplo de Dockerfile na seção Informações adicionais desse padrão.	Desenvolvedor, administrador do sistema

Tarefa	Descrição	Habilidades necessárias

Compilar e enviar por push uma imagem do Docker	No diretório em que você deseja criar, marcar e enviar a imagem `Dockerfile` para o Amazon ECR, execute os seguintes comandos:
	`aws ecr get-login -password --region <region>| docker login --username <username> --password-stdin <account_number>.dkr.ecr.<region>.amazonaws.com`
	`docker buildx build --platform linux/amd64 -t hello-world-java:v1 .`
	`docker tag hello-world-java:v1 <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	`docker push <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	Note
	Modifique a região da AWS, o número da conta e os detalhes do repositório nos comandos anteriores. Certifique-se de anotar	

Tarefa	Descrição	Habilidades necessárias
	a URL da imagem para uso posterior. **Important** Um sistema macOS com um chip M1 tem problemas ao criar uma imagem compatível com o Amazon EKS executado em uma plataforma. AMD64 Para resolver esse problema, use o docker buildx para criar uma imagem do Docker que funcione no Amazon EKS.	

Implemente os microsserviços Java

Tarefa	Descrição	Habilidades necessárias
Crie um arquivo de implantação.	Crie um arquivo YAML chamado `deployment.yaml` com base no código de arquivo de exemplo de implantação na seção Informações adicionais desse padrão.	Desenvolvedor, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
	Note Use o URL da imagem que você copiou anteriormente como o caminho do arquivo de imagem para o repositório Amazon ECR.	
Implante os microsserviços Java no cluster Amazon EKS.	Para criar uma implantação em seu cluster Amazon EKS, execute o comando `kubectl apply -f deploymen t.yaml .`	Desenvolvedor, administrador do sistema
Verifique o status dos pods.	1. Para verificar o status dos pods, execute o comando `kubectl get pods`. 2. Aguarde até que o status mude para Pronto.	Desenvolvedor, administrador do sistema
Crie um serviço.	1. Crie um arquivo chamado `service.yaml` com base no código de arquivo de exemplo de serviço na seção Informações adicionais desse padrão. 2. Execute o comando `kubectl apply -f service.yaml .`	Desenvolvedor, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
Instale o complemento Load Balancer Controller da AWS.	Siga as instruções de Instalar o complemento AWS Load Balancer Controller na documentação do Amazon EKS. **Note** Você precisa ter o complemento instalado para criar um Application Load Balancer ou Network Load Balancer para um serviço Kubernetes.	Desenvolvedor, administrador do sistema
Crie um recurso de entrada.	Crie um arquivo YAML chamado `ingress.yaml` com base no código de arquivo de exemplo de recurso de ingresso na seção Informações adicionais desse padrão.	Desenvolvedor, administrador do sistema
Criar um Application Load Balancer.	Para implantar o recurso de entrada e criar um Application Load Balancer, execute o comando `kubectl apply -f ingress.yaml` .	Desenvolvedor, administrador do sistema

Teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Teste e verifique a aplicação.	1. Para obter o nome DNS do balanceador de carga no campo ADDRESS (ENDEREÇO), execute o comando `kubectl get ingress.networking.k8s.io/java-microservice-ingress` . 2. Em uma EC2 instância na mesma VPC dos seus nós do Amazon EKS, execute o `curl -v <DNS address from previous command>` comando.	Desenvolvedor, administrador do sistema

Recursos relacionados

- Criar um repositório privado (documentação do Amazon ECR)
- Enviar por push uma imagem do Docker (documentação do Amazon ECR)
- Controladores de entrada (Amazon EKS Workshop)
- Docker buildx (documentos do Docker)

Mais informações

Example POM file

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/
maven-4.0.0.xsd">
```

```
  <modelVersion>4.0.0</modelVersion>


  <groupId>helloWorld</groupId>
  <artifactId>helloWorld</artifactId>
  <version>1.0-SNAPSHOT</version>


  <dependencies>
    <dependency>
      <groupId>com.sparkjava</groupId><artifactId>spark-core</
artifactId><version>2.0.0</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-jar-plugin</
artifactId><version>2.4</version>
        <configuration><finalName>eksExample</finalName><archive><manifest>
              <addClasspath>true</addClasspath><mainClass>eksExample.HelloWorld</
mainClass><classpathPrefix>dependency-jars/</classpathPrefix>
            </manifest></archive>
        </configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-compiler-plugin</
artifactId><version>3.1</version>
        <configuration><source>1.8</source><target>1.8</target></configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-assembly-plugin</
artifactId>
        <executions>
          <execution>
            <goals><goal>attached</goal></goals><phase>package</phase>
            <configuration>
              <finalName>eksExample</finalName>
              <descriptorRefs><descriptorRef>jar-with-dependencies</descriptorRef></
descriptorRefs>
              <archive><manifest><mainClass>eksExample.HelloWorld</mainClass></
manifest></archive>
            </configuration>
          </execution>
```

```
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

Example Dockerfile

```
FROM bellsoft/liberica-openjdk-alpine-musl:17

RUN apk add maven
WORKDIR /code

# Prepare by downloading dependencies
ADD pom.xml /code/pom.xml
RUN ["mvn", "dependency:resolve"]
RUN ["mvn", "verify"]

# Adding source, compile and package into a fat jar
ADD src /code/src
RUN ["mvn", "package"]

EXPOSE 4567
CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]
```

Example deployment file

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      containers:
      - name: java-microservice-container
```

```
        image: .dkr.ecr.amazonaws.com/:
        ports:
        - containerPort: 4567
```

Example service file

```
apiVersion: v1
kind: Service
metadata:
  name: "service-java-microservice"
spec:
  ports:
    - port: 80
      targetPort: 4567
      protocol: TCP
  type: NodePort
  selector:
    app.kubernetes.io/name: java-microservice
```

Example ingress resource file

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: "java-microservice-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/load-balancer-name: apg2
    alb.ingress.kubernetes.io/target-type: ip
  labels:
    app: java-microservice
spec:
  rules:
    - http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: "service-java-microservice"
                port:
                  number: 80
```

Implante um aplicativo em cluster no Amazon ECS usando o AWS Copilot

Criado por Jean-Baptiste Guillois (AWS), Mathew George (AWS) e Thomas Scott (AWS)

Resumo

Esse padrão mostra como implantar contêineres em um cluster do Amazon Elastic Container Service (Amazon ECS) de duas maneiras: usando o console de gerenciamento do Amazon Web Services (AWS) e usando o AWS Copilot, para demonstrar como o AWS Copilot simplifica as tarefas de implantação.

O Amazon ECS é um serviço de gerenciamento de contêineres altamente escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster. Os contêineres são definidos em uma definição de tarefa que você usa para executar tarefas individuais ou tarefas em um serviço. Você pode executar tarefas e serviços em uma infraestrutura com tecnologia gerenciada pelo AWS Fargate. Como alternativa, para ter mais controle sobre sua infraestrutura, você pode executar suas tarefas e serviços em um cluster de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que você gerencia.

A interface de linha de comandos (CLI) do AWS Copilot simplifica a criação, o lançamento e o funcionamento de aplicações em contêineres prontas para produção no Amazon ECS em um ambiente de desenvolvimento local. A CLI do AWS Copilot se alinha aos fluxos de trabalho do desenvolvedor que oferecem suporte a práticas recomendadas de aplicações modernas: do uso da infraestrutura como código à criação de um pipeline de integração contínua e oferta contínua (CI/CD) provisionado em nome de um usuário. Use a CLI do AWS Copilot como parte do ciclo diário de desenvolvimento e testes como uma alternativa ao Console de Gerenciamento da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) instalada e configurada localmente para usar sua conta da AWS (consulte as instruções de instalação e as instruções de configuração na documentação da AWS CLI)
- AWS Copilot instalado localmente (consulte as instruções de instalação na documentação do Amazon ECS)
- Docker instalado em sua máquina local (consulte a documentação do Docker)

Limitações

- O Docker impõe limites de extração de 100 imagens de contêiner por 6 horas por endereço IP no plano gratuito.

Arquitetura

Pilha de tecnologias de destino

- Ambiente da AWS configurado com uma nuvem privada virtual (VPC), sub-redes públicas e privadas e grupos de segurança
- Cluster do Amazon ECS
- Definição de serviços e tarefas do Amazon ECS
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon DynamoDB
- Application Load Balancer
- AWS Fargate
- Amazon Identity and Access Management (IAM)
- Amazon CloudWatch
- AWS CloudTrail

Arquitetura de destino

Quando você implanta o aplicativo de amostra para esse padrão, várias tarefas são criadas e implantadas em zonas de disponibilidade separadas. Cada tarefa armazena dados no Amazon DynamoDB. Ao acessar a página da Web de uma tarefa, você pode visualizar os dados de todas as outras tarefas.

Ferramentas

Serviços da AWS

- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um serviço de registro de imagem de contêiner, seguro, escalável e confiável. O Amazon ECR oferece suporte a repositórios privados com permissões baseadas em recursos usando o IAM.

- Amazon ECS: o Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido para execução, interrupção e gerenciamento de contêineres em um cluster. Você pode executar tarefas e serviços em uma infraestrutura com tecnologia gerenciada pelo AWS Fargate. Como alternativa, para ter mais controle sobre sua infraestrutura, você pode executar suas tarefas e serviços em um cluster de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que você gerencia.
- AWS Copilot: o AWS Copilot fornece uma interface de linha de comando que ajuda você a lançar e gerenciar aplicativos em contêineres na AWS, incluindo envio para um registro, criação de uma definição de tarefa e criação de um cluster.
- AWS Fargate — O AWS Fargate é um mecanismo de pay-as-you-go computação sem servidor que permite que você se concentre na criação de aplicativos sem gerenciar servidores. O AWS Fargate é compatível com o Amazon ECS e com o Amazon Elastic Kubernetes Service (Amazon EKS). Ao executar suas tarefas e serviços do Amazon ECS com o tipo de inicialização do Fargate ou um provedor de capacidade do Fargate, empacote a aplicação em contêineres, especifique os requisitos de CPU e memória, defina as políticas de rede e do IAM e inicie a aplicação. Cada tarefa do Fargate tem seu próprio limite de isolamento e não compartilha o kernel subjacente, os recursos de CPU, os recursos de memória nem a interface de rede elástica com outra tarefa.
- Amazon DynamoDB: o Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade integrada.
- Elastic Load Balancing (ELB) — O Elastic Load Balancing distribui automaticamente seu tráfego de entrada em vários destinos, EC2 como instâncias, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Ele monitora a integridade dos destinos registrados e roteia o tráfego apenas para os destinos íntegros. O Elastic Load Balancing escala seu balanceador de carga conforme seu tráfego de entrada muda com o tempo. Ele pode ser dimensionado automaticamente para a vasta maioria das cargas de trabalho.

Ferramentas

- Command Line Interface do Docker
- AWS Command Line Interface (AWS CLI)
- Interface de linha de comando do AWS Copilot

Código

O código do aplicativo de amostra usado nesse padrão está disponível no GitHub repositório Cluster Sample Application. Siga as instruções da próxima seção para usar os arquivos de amostra.

Épicos

Implemente a pilha de aplicativos: opção 1 (Console de Gerenciamento da AWS)

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Clone o repositório de códigos de exemplo usando o comando: `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	Desenvolvedor de aplicativos, AWS DevOps
Crie o repositório do Amazon ECR.	1. Faça login no AWS Management Console e abra o console do Amazon ECR nos https://console.aws.amazon.com/ecr/repositórios. 2. Escolha Criar repositório. 3. Para o nome do repositório, insira cluster-sample-app. 4. Para todas as outras configurações, mantenha os valores predefinidos. 5. Escolha Criar repositório. Para obter mais informações, consulte Criar um repositório	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	privado na documentação do Amazon ECR.	

Tarefa	Descrição	Habilidades necessárias

Crie, marque e envie sua imagem do Docker para o repositório do Amazon ECR.	1. Selecione o repositório que você acabou de criar e escolha Exibir comandos push.
	2. Copie os comandos exibidos e execute-os localmente para criar, marcar e enviar sua imagem do Docker. Estes comandos serão semelhantes ao mostrado a seguir.
	
	Para autenticar seu cliente do Docker no registro:
	
	`aws ecr get-login -password --region <YOUR_AWS_REGION> | docker login --username AWS --password-stdin <YOUR_AWS_ACCOUNT>.dkr.ecr.<YOUR_AWS_REGION>.amazonaws.com`
	
	Para criar sua imagem do Docker:
	
	`docker build -t cluster-sample-app .`
	
	Para marcar sua imagem do Docker:
	
	`docker tag cluster-sample-app:latest`
		Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	<YOUR_AWS_ACCOUNT> .dkr.ecr.<YOUR_AWS _REGION>.amazonaws .com/cluster-sample- app:latest Para enviar sua imagem do Docker ao seu repositório: docker push <YOUR_AWS _ACCOUNT>.dkr.ecr. <YOUR_AWS_REGION>. amazonaws.com/clus ter-sample-app:latest	

Tarefa	Descrição	Habilidades necessárias
Implante a pilha do aplicativo.	1. Abra o CloudFormation console da AWS em https://console.aws.amazon.com/cloudformation/. 2. Selecione Criar pilha. 3. Na seção Prepare template (Preparar modelo), selecione Template is ready (O modelo está pronto). 4. Na seção Especificar modelo escolha Fazer carregar um arquivo de modelo. 5. Escolha o arquivo local **`cluster-sample-app-stack.yml`** que você clonou do GitHub repositório como CloudFormation modelo e, em seguida, escolha Avançar. 6. Insira um nome para a pilha e escolha Avançar. 7. Mantenha as opções padrão, escolha Avançar. 8. Analise todas as opções, reconheça a criação dos recursos do IAM e escolha Criar pilha. 9. Quando sua pilha de aplicativos tiver sido implantada, escolha a guia Saída, copie a URL e a	AWS DevOps, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	abra em seu navegador para acessar o aplicativo. Para obter mais informaçõ es sobre a implantação de CloudFormation modelos, consulte Como criar uma pilha na documentação da AWS CloudFormation .	

Implemente a pilha de aplicativos: opção 2 (CLI do AWS Copilot)

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Clone o repositório de códigos de exemplo usando o comando: `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	Desenvolvedor de aplicativos, AWS DevOps
Implante sua imagem de contêiner na AWS usando a CLI do AWS Copilot.	Implante o aplicativo em uma única etapa usando o seguinte comando no diretório raiz do seu projeto: `copilot init --app cluster-sample-app --name demo --type "Load Balanced Web Service" --dockerfile ./Dockerf`	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`ile --port 8080 --deploy` Em seguida, você poderá acessar o aplicativo usando o nome DNS fornecido como saída.	

Exclua os recursos criados

Tarefa	Descrição	Habilidades necessárias
Excluir os recursos criados por meio do Console de Gerenciamento da AWS.	Se você usou a opção 1 (o Console de Gerenciamento da AWS) para implantar a pilha de aplicativos, siga estas etapas quando estiver pronto para excluir os recursos que você criou: 1. Abra o CloudFormation console em https://console.aws.amazon.com/cloudformation/. 2. Selecione a pilha que você criou e escolha Excluir. 3. Abra o console do Amazon ECR nos https://console.aws.amazon.com/ecr/repositórios. 4. Selecione o repositório que você criou e escolha Excluir.	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Exclua os recursos criados pelo AWS Copilot.	Se você usou a opção 2 (a CLI do AWS Copilot) para implantar a pilha de aplicativos, execute o seguinte comando no diretório raiz do seu projeto quando estiver pronto para excluir os recursos que você criou: `copilot app delete`	Desenvolvedor de aplicativos, AWS DevOps

Recursos relacionados

- Instalar ou atualizar a versão mais recente da AWS CLI (documentação da AWS CLI)
- Usando a interface de linha de comando do AWS Copilot (documentação do Amazon ECS)
- Amazon ECS no AWS Fargate (documentação do Amazon ECR)
- Documentação do Amazon ECS
- Documentação do Amazon ECR
- CloudFormation Documentação da Amazon
- Docker Desktop (documentação do Docker)

Implemente um aplicativo baseado em gRPC em um cluster Amazon EKS e acesse-o com um Application Load Balancer

Criado por Kirankumar Chandrashekar (AWS) e Huy Nguyen (AWS)

Resumo

Esse padrão descreve como hospedar um aplicativo baseado em gRPC em um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) e acessá-lo com segurança por meio de um Application Load Balancer.

gRPC é uma estrutura de chamada de procedimento remoto (RPC) de código aberto que pode ser executada em qualquer ambiente. Você pode usá-lo para integrações de microsserviços e comunicações cliente-servidor. Para obter mais informações sobre o gRPC, consulte a postagem do blog da AWS Application Load Balancer support for end-to-end HTTP/2 e gRPC.

Esse padrão mostra como hospedar um aplicativo baseado em gRPC executado em pods do Kubernetes no Amazon EKS. O cliente gRPC se conecta a um Application Load Balancer por meio do protocolo HTTP/2 com uma conexão criptografada SSL/TLS. O Application Load Balancer encaminha o tráfego para o aplicativo gRPC que é executado nos pods do Amazon EKS. O número de pods gRPC pode ser escalado automaticamente com base no tráfego usando o autoescalador horizontal de pods do Kubernetes. O grupo-alvo do Application Load Balancer realiza verificações de saúde nos nós do Amazon EKS, avalia se o destino está íntegro e encaminha o tráfego somente para nós íntegros.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Docker, instalado e configurado no Linux, macOS ou Windows
- AWS Command Line Interface (AWS CLI) versão 2, instalado e configurado no Linux, macOS ou Windows.
- eksctl, instalado e configurado no Linux, macOS ou Windows.
- `kubectl`, instalado e configurado para acessar recursos em seu cluster Amazon EKS. Para obter mais informações, consulte Instalação ou atualização do kubectl na documentação do Amazon EKS.
- g RPCurl, instalado e configurado.

- Um cluster Amazon EKS novo ou existente. Para obter mais informações, consulte Introdução ao Amazon EKS.
- Seu terminal de computador configurado para acessar o cluster Amazon EKS. Para obter mais informações, consulte Configurar seu computador para se comunicar com seu cluster na documentação do Amazon EKS.
- Controlador do AWS Load Balancer, provisionado no cluster Amazon EKS.
- Um nome de host DNS existente com um certificado SSL ou SSL/TLS válido. É possível obter um certificado para seu domínio usando o AWS Certificate Manager (ACM) ou fazendo upload de um certificado existente para o ACM. Para obter mais informações sobre essas duas opções, consulte Solicitação de um certificado público e Importação de certificados para o AWS Certificate Manager na documentação do ACM.

Arquitetura

O diagrama a seguir mostra a arquitetura implementada por esse padrão.

O diagrama a seguir mostra um fluxo de trabalho em que o tráfego SSL/TLS é recebido de um cliente gRPC que é transferido para um Application Load Balancer. O tráfego é encaminhado em texto simples para o servidor gRPC porque é proveniente de uma nuvem privada virtual (VPC).

Ferramentas

Serviços da AWS

- O AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.

Ferramentas

- eksctl é uma ferramenta CLI simples para criar clusters no Amazon EKS.
- O Kubectl: é um utilitário de linha de comando para executar comandos em clusters do Kubernetes.
- O AWS Load Balancer Controller ajuda a gerenciar AWS Elastic Load Balancers para um cluster do Kubernetes.
- g RPCurl é uma ferramenta de linha de comando que ajuda você a interagir com os serviços gRPC.

Repositório de código

O código desse padrão está disponível no repositório GitHub grpc-traffic-on-alb-to-eks.

Épicos

Crie e envie a imagem do Docker do servidor gRPC para o Amazon ECR

Tarefa	Descrição	Habilidades necessárias
Crie um repositório do Amazon ECR.	Faça login no AWS Management Console, abra o console do Amazon ECR e crie um repositório do Amazon ECR. Para obter mais informações, consulte Criação de um repositório na documentação do Amazon ECR. Certifique-se de registrar a URL do repositório Amazon ECR. Você também pode criar um repositório Amazon ECR com a AWS CLI executando o seguinte comando:	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	`aws ecr create-repository --repository-name helloworld-grpc`	

Crie a imagem do Docker.	1. Clone o repositório GitHub grpc-traffic-on-alb-to-eks.
	`git clone https://github.com/aws-samples/grpc-traffic-on-alb-to-eks.git`
	2. No diretório raiz do repositório, verifique se o Dockerfile existe e execute o seguinte comando para criar a imagem do Docker:
	`docker build -t <amazon_ecr_repository_url>:<Tag> .`
	Important
	Certifique-se de `<amazon_ecr_repository_url>` substituir pela URL do repositório Amazon ECR que você criou anteriormente.
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Envie a imagem do Docker para o Amazon ECR.	1. Execute o seguinte comando para fazer login no repositório Amazon ECR:
	`aws ecr get-login -password --region us-east-1 --no-cli-auto-prompt | docker login --username AWS --password-stdin <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com`
	2. Envie a imagem do Docker para o repositório do Amazon ECR executando o comando a seguir:
	`docker push <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-grpc:1.0`
	Important
	Certifique-se de substituir pelo `<your_aws_account_id>` ID da sua conta da AWS.
		DevOps engenheiro

Implemente os manifestos do Kubernetes no cluster Amazon EKS

Tarefa	Descrição	Habilidades necessárias
Modifique os valores no arquivo de manifesto do Kubernetes.	1. Modifique o arquivo de manifesto do `grpc-sample.yaml` Kubernetes na pasta Kubernetes do repositório de acordo com seus requisitos. Você deve modificar as anotações e o nome do host no recurso de entrada. Para obter um exemplo de recurso de entrada, consulte a seção Informações adicionais. Para obter mais informações consulte Ingress annotations na documentação do Kubernetes. 2. No recurso de implantação do Kubernetes, altere o recurso de implantação `image` para o identificador uniforme de recursos (URI) do repositório Amazon ECR para o qual você enviou a imagem do Docker. Para obter um exemplo de recurso de implantação, consulte a seção Informações adicionais.	DevOps engenheiro
Implemente o arquivo manifesto do Kubernetes.	Implante o `grpc-sample.yaml` arquivo no cluster Amazon EKS executando o seguinte `kubectl` comando:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`kubectl apply -f ./kubernetes/grpc-sample.yaml`	

Crie o registro DNS para o FQDN do Application Load Balancer

Tarefa	Descrição	Habilidades necessárias
Registre o FQDN do Application Load Balancer	1. Execute o `kubectl` comando a seguir para descrever o recurso de entrada do Kubernetes que gerencia o Application Load Balancer: `kubectl get ingress -n grpcserver` O exemplo de saída é fornecido na seção Informações adicionais. Na saída, o `HOSTS` campo exibe o nome do host DNS para o qual os certificados SSL foram criados. 2. Registre o nome de domínio totalmente qualificado (FQDN) do Application Load Balancer no `Address` campo da saída. 3. Crie um registro DNS que aponte para o FQDN do Application Load Balancer. Se o seu provedor de	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	DNS for o Amazon Route 53, você poderá criar um registro de alias que aponte para o FQDN do Applicati on Load Balancer. Para obter mais informações sobre essa opção, consulte Escolha entre registros de alias e sem alias na documentação do Route 53.	

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Teste o servidor gRPC.	Use g RPCurl para testar o endpoint executando o seguinte comando: `grpcurl grpc.exam ple.com:443 list grpc.reflection.v 1alpha.ServerRefle ction helloworld.helloworld` **Note** `grpc.exam ple.com` Substitua pelo seu nome DNS.	DevOps engenheiro
Teste o servidor gRPC usando um cliente gRPC.	No `helloworld_client_ ssl.py` exemplo de cliente	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	gRPC, substitua o nome do host de pelo nome do `grpc.example.com` host usado para o servidor gRPC.
	
	O exemplo de código a seguir mostra a resposta do servidor gRPC para a solicitação do cliente:
	
	`python ./app/helloworld_client_ssl.py`
	`message: "Hello to gRPC server from Client"`
	
	`message: "Thanks for talking to gRPC server!! Welcome to hello world. Received message is \"Hello to gRPC server from Client\""`
	`received: true`
	
	Isso mostra que o cliente pode conversar com o servidor e que a conexão foi bem-sucedida.	

Limpeza

Tarefa	Descrição	Habilidades necessárias
Remova o registro DNS.	Remova o registro DNS que aponta para o FQDN do	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Application Load Balancer que você criou anteriormente.	
Remova o balanceador de carga.	No EC2 console da Amazon, escolha Load Balancers e, em seguida, remova o balancead or de carga que o controlad or Kubernetes criou para seu recurso de entrada.	Administrador de nuvem
Exclua o cluster Amazon EKS.	Exclua o cluster Amazon EKS usando`eksctl`: `eksctl delete cluster -f ./eks.yaml`	AWS DevOps

Recursos relacionados

- Balanceamento de carga da rede no Amazon EKS
- Grupos de destino para seus Application Load Balancers

Mais informações

Exemplo de recurso de entrada:

```
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  annotations:
    alb.ingress.kubernetes.io/healthcheck-protocol: HTTP
    alb.ingress.kubernetes.io/ssl-redirect: "443"
    alb.ingress.kubernetes.io/backend-protocol-version: "GRPC"
    alb.ingress.kubernetes.io/listen-ports: '[{"HTTP": 80}, {"HTTPS":443}]'
    alb.ingress.kubernetes.io/scheme: internet-facing
    alb.ingress.kubernetes.io/target-type: ip
```

```
    alb.ingress.kubernetes.io/certificate-arn: arn:aws:acm:<AWS-
Region>:<AccountId>:certificate/<certificate_ID>
  labels:
    app: grpcserver
    environment: dev
  name: grpcserver
  namespace: grpcserver
spec:
  ingressClassName: alb
  rules:
  - host: grpc.example.com # <----- replace this as per your host name for which the
 SSL certtficate is available in ACM
    http:
      paths:
      - backend:
          service:
            name: grpcserver
            port:
              number: 9000
        path: /
        pathType: Prefix
```

Exemplo de recurso de implantação:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: grpcserver
  namespace: grpcserver
spec:
  selector:
    matchLabels:
      app: grpcserver
  replicas: 1
  template:
    metadata:
      labels:
        app: grpcserver
    spec:
      containers:
      - name: grpc-demo
        image: <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-
grpc:1.0   #<------- Change to the URI that the Docker image is pushed to
```

```
        imagePullPolicy: Always
        ports:
        - name: grpc-api
          containerPort: 9000
        env:
        - name: POD_IP
          valueFrom:
            fieldRef:
              fieldPath: status.podIP
      restartPolicy: Always
```

Exemplo de saída:

```
NAME             CLASS           HOSTS                          Address
 PORTS          AGE
 grpcserver      <none>      <DNS-HostName>                 <ELB-address>
 80            27d
```

Implantar e depure clusters do Amazon EKS

Criado por Svenja Raether (AWS) e Mathew George (AWS)

Resumo

Os contêineres estão se tornando uma parte essencial do desenvolvimento de aplicativos nativos de nuvem. O Kubernetes fornece uma maneira eficiente de gerenciar e orquestrar contêineres. O Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço totalmente gerenciado e certificado em conformidade com o Kubernetes para compilar, proteger, operar e manter clusters do Kubernetes na Amazon Web Services (AWS). Ele é compatível com a execução de pods no AWS Fargate para fornecer capacidade computacional sob demanda do tamanho certo.

É importante que desenvolvedores e administradores conheçam as opções de depuração ao executar workloads em contêineres. Este padrão orienta você na implantação e depuração de contêineres no Amazon EKS com o AWS Fargate. Isso inclui criar, implantar, acessar, depurar e limpar as workloads do Amazon EKS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Perfil do AWS Identity and Access Management (IAM) configurado com permissões suficientes para criar e interagir com o Amazon EKS, perfis do IAM e funções vinculadas a serviços
- AWS Command Line Interface (AWS CLI) instalada na máquina local.
- eksctl
- kubectl
- Helm

Limitações

- Esse padrão fornece aos desenvolvedores práticas úteis de depuração para ambientes de desenvolvimento. Ele não indica as práticas recomendadas para ambientes de produção.
- Se você estiver executando o Windows, use os comandos específicos do sistema operacional para definir as variáveis de ambiente.

Versões do produto usadas

- AWS CLI versão 2
- Versão kubectl dentro de uma pequena diferença de versão do ambiente de gerenciamento do Amazon EKS que você está usando
- versão mais recente do eksctl
- Helm v3

Arquitetura

Pilha de tecnologia

- Application Load Balancer
- Amazon EKS
- AWS Fargate

Arquitetura de destino

Todos os recursos mostrados no diagrama são provisionados usando comandos `eksctl` e `kubectl` emitidos de uma máquina local. Clusters privados devem ser executados a partir de uma instância que esteja dentro da VPC privada.

A arquitetura de destino consiste em um cluster EKS usando o tipo de inicialização Fargate. Ele fornece capacidade computacional sob demanda do tamanho certo, sem a necessidade de especificar tipos de servidor. O cluster EKS tem um ambiente de gerenciamento, que é usado para gerenciar os nós e as workloads do cluster. Os pods são provisionados em sub-redes VPC privadas que abrangem várias zonas de disponibilidade. A Galeria pública do Amazon ECR é referenciada para recuperar e implantar uma imagem do servidor web NGINX nos pods do cluster.

O diagrama mostra como acessar o ambiente de gerenciamento do Amazon EKS usando os comandos `kubectl` e como acessar o aplicativo usando o Application Load Balancer.

.

1. Uma máquina local fora da Nuvem AWS envia comandos para o ambiente de gerenciamento do Kubernetes dentro de uma VPC gerenciada pelo Amazon EKS.

2. O Amazon EKS agenda pods com base nos seletores no perfil do Fargate.
3. A máquina local abre a URL do Application Load Balancer no navegador.
4. O Application Load Balancer divide o tráfego entre os pods do Kubernetes nos nós do cluster Fargate implantados em sub-redes privadas abrangendo várias zonas de disponibilidade.

Ferramentas

Serviços da AWS

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes. Esse padrão também usa a ferramenta de linha de comando eksctl para trabalhar com clusters Kubernetes no Amazon EKS.
- O AWS Fargate ajuda você a executar contêineres sem precisar gerenciar servidores ou instâncias do Amazon Elastic Compute Cloud (Amazon). EC2 É usado em conjunto com o Amazon Elastic Container Service (Amazon ECS).
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade. Esse padrão usa o componente de controle do AWS Load Balancer Controller para criar o Application Load Balancer quando uma entrada do Kubernetes é provisionada. O Application Load Balancer distribui o tráfego de entrada entre vários destinos.

Outras ferramentas

- O Helm é um gerenciador de pacotes de código aberto para o Kubernetes. Nesse padrão, o Helm é usado para instalar o AWS Load Balancer Controller.
- O Kubernetes é um sistema de código aberto para automatizar a implantação, a escalabilidade e o gerenciamento de aplicações em contêineres.
- O NGINX é um servidor web e proxy reverso de alto desempenho.

Épicos

Crie um cluster do EKS

Tarefa	Descrição	Habilidades necessárias
Criar os arquivos.	Usando o código na seção Informações adicionais, crie os seguintes arquivos: • `clusterconfig-fargate.yaml` • `nginx-deployment.yaml` • `nginx-service.yaml` • `nginx-ingress.yaml` • `index.html`	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps
Definição de variáveis de ambiente.	**Note** Se um comando falhar devido a tarefas anteriores não concluídas, aguarde alguns segundos e execute o comando novamente. Esse padrão usa a região da AWS e o nome do cluster definidos no arquivo `clusterconfig-fargate.yaml` . Defina os mesmos valores das variáveis de ambiente para referenciá-los em outros comandos.	Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	`export AWS_REGION="us-east-1"` `export CLUSTER_NAME="my-fargate"`	
Crie um cluster do EKS.	Para criar um cluster EKS que usa as especificações do arquivo `clusterconfig-fargate.yaml`, execute o comando a seguir. `eksctl create cluster -f clusterconfig-fargate.yaml` O arquivo contém `ClusterConfig`, que provisiona um novo cluster EKS chamado `my-fargate-cluster` na Região `us-east-1` e um perfil Fargate padrão (`fp-default`). O perfil Fargate padrão é configurado com dois seletores (`default` e `kube-system`).	Desenvolvedor de aplicativos, AWS DevOps, administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Verifique o cluster criado.	Para verificar o cluster criado, execute o seguinte comando.
	`eksctl get cluster --output yaml`
	A saída deve ser a seguinte.
	`- Name: my-fargate`
	`  Owned: "True"`
	`  Region: us-east-1`
	Verifique o perfil Fargate criado usando `CLUSTER_NAME` .
	`eksctl get fargatepr ofile --cluster $CLUSTER_NAME --output yaml`
	Esse comando exibe informações sobre os recursos. Você pode usar as informações para verificar o cluster criado. A saída deve ser a seguinte.
	`- name: fp-default`
	`  podExecutionRoleAR N: arn:aws:iam::<YOUR -ACCOUNT-ID>:role/ eksctl-my-fargate- cluster-FargatePod ExecutionRole-xxx`
	`  selectors:`
	`  - namespace: default`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>- namespace: kube-system
	status: ACTIVE
	subnets:
	- subnet-aaa
	- subnet-bbb
	- subnet-ccc</pre>	

Implantar um contêiner

Tarefa	Descrição	Habilidades necessárias
Implante o servidor web NGINX.	Para aplicar a implantação do servidor web NGINX no cluster, execute o comando a seguir. <pre>kubectl apply -f ./nginx-deployment.yaml</pre>A saída deve ser a seguinte. <pre>deployment.apps/nginx-deployment created</pre>A implantação inclui três réplicas da imagem do NGINX tiradas da Galeria pública do Amazon ECR. A imagem é implantada no namespace padrão e exposta na porta 80 nos pods em execução.	Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS
Verifique a implantação e os pods.	(Opcional) Verifique a implantação. Você pode	Desenvolvedor de aplicativos, AWS DevOps, administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	verificar o status da implantação com o comando a seguir.
	`kubectl get deployment`
	A saída deve ser a seguinte.
	`NAME READY UP-TO-DATE AVAILABLE AGE nginx-deployment 3/3 3 3 7m14s`
	Um pod é um objeto implantável no Kubernetes, contendo um ou mais contêineres. Para listar todos os pods, execute o seguinte comando.
	`kubectl get pods`
	A saída deve ser a seguinte.
	`NAME READY STATUS RESTARTS AGE nginx-deployment-xxxx-aaa 1/1 Running 0 94s nginx-deployment-xxxx-bbb 1/1 Running 0 94s nginx-deployment-xxxx-ccc 1/1 Running 0 94s`	

Tarefa	Descrição	Habilidades necessárias

Escale a implantação.	Para escalar a implantação das três réplicas especificadas em `deployment.yaml` para quatro réplicas, use o comando a seguir.
	`kubectl scale deploymen t nginx-deployment -- replicas 4`
	A saída deve ser a seguinte.
	`deployment.apps/nginx- deployment scaled`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Implante um AWS Load Balancer Controller

Tarefa	Descrição	Habilidades necessárias

Definição de variáveis de ambiente.	Descreva a CloudFormation pilha do cluster para recuperar informações sobre sua VPC.
	`aws cloudformation describe-stacks -- stack-name eksctl-$C LUSTER_NAME-cluste r --query "Stacks[0 ].Outputs[?OutputK ey==\`VPC\`].Outpu tValue"`
	A saída deve ser a seguinte.
	`[`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	`"vpc-<YOUR-VPC-ID>"`
	`]`
	
	Copie o ID da VPC e exporte-o como uma variável de ambiente.
	
	`export VPC_ID="vpc-<YOUR-VPC-ID>"`	

Configurar o IAM para a conta de serviço do cluster.	Use o `AWS_REGION` e `CLUSTER_NAME` do épico anterior para criar um provedor IAM Open ID Connect para o cluster.
	
	`eksctl utils associate-iam-oidc-provider \`
	`--region $AWS_REGION \`
	`--cluster $CLUSTER_NAME \`
	`--approve`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

Faça download e crie a política do IAM.	Baixe a política do IAM para o AWS Load Balancer Controller, que permite que ele faça chamadas para a AWS APIs em seu nome.
	`curl -o iam-policy.json https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/main/docs/install/iam_policy.json`
	Crie a política em sua conta da AWS usando a CLI da AWS.
	`aws iam create-policy \ --policy-name AWSLoadBalancerControllerIAMPolicy \ --policy-document file://iam-policy.json`
	Você verá a saída a seguir.
	`{ "Policy": { "PolicyName": "AWSLoadBalancerControllerIAMPolicy", "PolicyId": "<YOUR_POLICY_ID>", "Arn": "arn:aws:iam::<YOUR-ACCOUNT`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>-ID>:policy/AWSLoa
	dBalancerControlle
	rIAMPolicy",
	"Path": "/",
	"DefaultV
	ersionId": "v1",
	"Attachme
	ntCount": 0,
	"Permissi
	onsBoundaryUsageCo
	unt": 0,
	"IsAttachable":
	true,
	"CreateDate":
	"<YOUR-DATE>",
	"UpdateDate":
	"<YOUR-DATE>"
	}
	}</pre> Salve o nome do recurso da Amazon (ARN) da política como `$POLICY_ARN` . <pre>export POLICY_AR
	N=”arn:aws:iam::<Y
	OUR-ACCOUNT-ID>:po
	licy/AWSLoadBalanc
	erControllerIAMPol
	icy”</pre>	

Tarefa	Descrição	Habilidades necessárias

Crie uma conta de serviço do IAM.	Uma conta de serviço do IAM chamada `aws-load-balancer-controller` no namespace `kube-system`. Use `CLUSTER_NAME`, `AWS_REGION` e `POLICY_ARN` que você configurou anteriormente.
	`eksctl create iamserviceaccount \ --cluster=$CLUSTER_NAME \ --region=$AWS_REGION \ --attach-policy-arn=$POLICY_ARN \ --namespace=kube-system \ --name=aws-load-balancer-controller \ --override-existing-serviceaccounts \ --approve`
	Verifique a criação.
	`eksctl get iamserviceaccount \ --cluster $CLUSTER_NAME \ --name aws-load-balancer-controller \ --namespace kube-system \ --output yaml`
	A saída deve ser a seguinte.
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	`- metadata:`
	`    name: aws-load-balancer-controller`
	`    namespace: kube-system`
	`  status:`
	`    roleARN: arn:aws:iam::<YOUR-ACCOUNT-ID>:role/eksctl-my-fargate-addon-iam serviceaccount-ku-Role1-<YOUR-ROLE-ID>`
	`  wellKnownPolicies:`
	`    autoScaler: false`
	`    awsLoadBalancerController: false`
	`    certManager: false`
	`    ebsCSIController: false`
	`    efsCSIController: false`
	`    externalDNS: false`
	`    imageBuilder: false`	

Tarefa	Descrição	Habilidades necessárias

Instale o Load Balancer Controller da AWS.	Atualize o repositório do Helm.
	`helm repo update`
	Adicione o repositório de gráficos do Amazon EKS ao repositório Helm.
	`helm repo add eks https://aws.github.io/eks-charts`
	Aplique as definições de recursos personalizadas do Kubernetes (CRDs) que são usadas pelo AWS Load Balancer Controller eks-chart em segundo plano.
	`kubectl apply -k "github.com/aws/eks-charts/stable/aws-load-balancer-controller//crds?ref=master"`
	A saída deve ser a seguinte.
	`customresourcedefinition.apiextensions.k8s.io/ingressclassparams.elbv2.k8s.aws created customresourcedefinition.apiextensions.k8s.io/targetgro`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	upbindings.elbv2.k8s.aws created
	
	Instale o chart do Helm usando as variáveis de ambiente que você definiu anteriormente.
	
	`helm install aws-load-balancer-controller eks/aws-load-balancer-controller \ --set clusterName=$CLUSTER_NAME \ --set serviceAccount.create=false \ --set region=$AWS_REGION \ --set vpcId=$VPC_ID \ --set serviceAccount.name=aws-load-balancer-controller \ -n kube-system`
	
	A saída deve ser a seguinte.
	
	`NAME: aws-load-balancer-controller LAST DEPLOYED: <YOUR-DATE> NAMESPACE: kube-system STATUS: deployed REVISION: 1 TEST SUITE: None NOTES: AWS Load Balancer controller installed!`	

Tarefa	Descrição	Habilidades necessárias

Crie um serviço NGINX.	Crie um serviço para expor os pods do NGINX usando o arquivo `nginx-service.yaml` .
	`kubectl apply -f nginx-service.yaml`
	A saída deve ser a seguinte.
	`service/nginx-service created`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Crie o recurso de entrada do Kubernetes.	Crie um serviço para expor o ingresso dos Kubernetes do NGINX usando o arquivo `nginx-ingress.yaml` .
	`kubectl apply -f nginx-ingress.yaml`
	A saída deve ser a seguinte.
	`ingress.networking.k8s.io/nginx-ingress created`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

Obtenha a URL do balancead or de carga.	Para recuperar as informaçõ es de entrada, use o comando a seguir.
	`kubectl get ingress nginx-ingress`
	A saída deve ser a seguinte.
	`NAME CLASS HOSTS ADDRESS PORTS AGE nginx-ingress <none> * k8s-defau lt-nginxing-xxx.us -east-1.elb.amazon aws.com 80 80s`
	Copie ADDRESS (por exemplo, `k8s-default-nginxi ng-xxx.us-east-1.e lb.amazonaws.com`) da saída e cole-o em seu navegador para acessar o arquivo `index.html` .
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Depure contêineres em execução

Tarefa	Descrição	Habilidades necessárias
Selecione um pod.	Liste todos os pods e copie o nome do pod desejado.	Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	`kubectl get pods`
	
	A saída deve ser a seguinte.
	
	`NAME READY STATUS RESTARTS AGE nginx-deployment-xxxx-aaa 1/1 Running 0 55m nginx-deployment-xxxx-bbb 1/1 Running 0 55m nginx-deployment-xxxx-ccc 1/1 Running 0 55m nginx-deployment-xxxx-ddd 1/1 Running 0 42m`
	
	Esse comando lista os pods existentes e as informações adicionais.
	
	Se você estiver interessado em um pod específico, preencha o nome do pod em que você está interessado para a variável `POD_NAME` ou defina-o como uma variável de ambiente. Caso contrário, omita esse parâmetro para pesquisar todos os recursos.	

Tarefa	Descrição	Habilidades necessárias
	`export POD_NAME="nginx-deployment-<YOUR-POD-NAME>"`	
Acesse os logs.	Obtenha os logs do pod que você deseja depurar. `kubectl logs $POD_NAME`	Desenvolvedor de aplicativos, administrador de sistemas da AWS, AWS DevOps

Encaminhe a porta NGINX.	Use o encaminhamento de porta para mapear a porta do pod para acessar o servidor web NGINX em uma porta na sua máquina local.
	`kubectl port-forward deployment/nginx-deployment 8080:80`
	No seu navegador, abra o seguinte URL.
	`http://localhost:8080`
	O comando `port-forward` fornece acesso ao arquivo `index.html` sem disponibilizá-lo publicamente por meio de um balanceador de carga. Isso é útil para acessar o aplicativo em execução durante a depuração. Você pode interromper o encaminhamento de portas pressionando o comando do teclado Ctrl+C.
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Execute comandos dentro do pod.	Para examinar o arquivo `index.html` atual, use o comando a seguir. `kubectl exec $POD_NAME -- cat /usr/share/nginx/html/index.html` Você pode usar o comando `exec` para emitir qualquer comando diretamente no pod. Isso é útil para depurar os aplicativos em execução.	Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Copie arquivos para um pod.	Remova o arquivo `index.html` padrão desse pod.
	`kubectl exec $POD_NAME -- rm /usr/share/nginx/html/index.html`
	Faça o upload do arquivo local personalizado `index.html` para o pod.
	`kubectl cp index.html $POD_NAME:/usr/share/nginx/html/`
	Você pode usar o comando `cp` para alterar ou adicionar arquivos diretamente a qualquer um dos pods.
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

Use o encaminhamento de porta para exibir a alteração.	Use o encaminhamento de portas para verificar as alterações que você fez nesse pod.
	`kubectl port-forward pod/$POD_NAME 8080:80`
	Abra o seguinte URL no seu navegador.
	`http://localhost:8080`
	As alterações aplicadas ao arquivo `index.html` devem estar visíveis no navegador.
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Excluir recursos

Tarefa	Descrição	Habilidades necessárias

Exclui o balanceador de carga.	Exclua a entrada.
	`kubectl delete ingress/nginx-ingress`
	A saída deve ser a seguinte.
	`ingress.networking.k8s.io "nginx-ingress" deleted`
	Exclua o serviço.
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	`kubectl delete service/nginx-service`
	
	A saída deve ser a seguinte.
	
	`service "nginx-service" deleted`
	
	Exclua o controlador do balanceador de carga.
	
	`helm delete aws-load-balancer-controller -n kube-system`
	
	A saída deve ser a seguinte.
	
	`release "aws-load-balancer-controller" uninstalled`
	
	Exclua a conta do serviço.
	
	`eksctl delete iamserviceaccount --cluster $CLUSTER_NAME --namespace kube-system --name aws-load-balancer-controller`	

Tarefa	Descrição	Habilidades necessárias

Exclua a implantação.	Para excluir os recursos de implantação, use o seguinte comando.
	`kubectl delete deploy/nginx-deployment`
	A saída deve ser a seguinte.
	`deployment.apps "nginx-deployment" deleted`
		Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS

Excluir o cluster.	Exclua o cluster EKS usando o comando a seguir, onde `my-fargate` é o nome do cluster. `eksctl delete cluster --name $CLUSTER_NAME` Esse comando exclui todo o cluster, incluindo todos os recursos associados.	Desenvolvedor de aplicativos, AWS DevOps, administrador de sistemas da AWS
Excluir a política do IAM.	Exclua a política criada anteriormente usando a CLI da AWS. `aws iam delete-policy --policy-arn $POLICY_ARN`	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Solução de problemas

Problema	Solução
Você recebe uma mensagem de erro na criação do cluster informando que sua zona de disponibilidade de destino não tem capacidad e suficiente para oferecer suporte ao cluster. Você verá uma mensagem semelhante à mensagem abaixo. `Cannot create cluster 'my-fargate' because us-east-1e, the targeted availability zone, does not currently have sufficient capacity to support the cluster. Retry and choose from these availability zones: us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1f`	Crie o cluster novamente usando as zonas de disponibilidade recomendadas a partir da mensagem de erro. Especifique uma lista de zonas de disponibilidade na última linha do seu arquivo `clusterconfig-fargate.yaml` (por exemplo, `availabilityZones: ["us-east-1a", "us-east-1b", "us-east-1c"]`).

Recursos relacionados

- Documentação do Amazon EKS
- Application Load Balancer no Amazon EKS
- Guias de práticas recomendadas do EKS
- Documentação do AWS Load Balancer Controller
- eksctl documentation
- Imagem NGINX da Galeria Pública do Amazon ECR
- Documentação do Helm
- Debug Running Pods (Depurar pods em execução) (documentação do Kubernetes)
- Workshop do Amazon EKS
- Erros de criação do cluster EKS

Mais informações

clusterconfig-fargate.yaml

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-fargate
  region: us-east-1

fargateProfiles:
  - name: fp-default
    selectors:
      - namespace: default
      - namespace: kube-system
```

nginx-deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: "nginx-deployment"
  namespace: "default"
spec:
  replicas: 3
  selector:
    matchLabels:
      app: "nginx"
  template:
    metadata:
      labels:
        app: "nginx"
    spec:
      containers:
      - name: nginx
        image: public.ecr.aws/nginx/nginx:latest
        ports:
        - containerPort: 80
```

nginx-service.yaml

```
apiVersion: v1
```

```
kind: Service
metadata:
  annotations:
    alb.ingress.kubernetes.io/target-type: ip
  name: "nginx-service"
  namespace: "default"
spec:
  ports:
  - port: 80
    targetPort: 80
    protocol: TCP
  type: NodePort
  selector:
    app: "nginx"
```

nginx-ingress.yaml

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  namespace: "default"
  name:  "nginx-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/scheme: internet-facing
spec:
  rules:
    - http:
        paths:
        - path: /
          pathType: Prefix
          backend:
            service:
              name: "nginx-service"
              port:
                number: 80
```

index.html

```
<!DOCTYPE html>
<html>

<body>
```

```
    <h1>Welcome to your customized nginx!</h1>
    <p>You modified the file on this running pod</p>
</body>

</html>
```

Implantar contêineres usando o Elastic Beanstalk

Criado por Thomas Scott (AWS) e Jean-Baptiste Guillois (AWS)

Resumo

Na Nuvem da Amazon Web Services (AWS), o AWS Elastic Beanstalk oferece suporte ao Docker como uma plataforma disponível, para que os contêineres possam ser executados com o ambiente criado. Esse padrão mostra como implantar contêineres usando o serviço Elastic Beanstalk. A implantação desse padrão usará o ambiente de servidor web baseado na plataforma Docker.

Para usar o Elastic Beanstalk para implantar e escalar aplicativos e serviços web, você carrega seu código e a implantação é tratada automaticamente. Provisionamento de capacidade, balanceamento de carga, ajuste de escala automático e monitoramento da integridade do aplicativo também estão incluídos. Ao usar o Elastic Beanstalk, você pode assumir o controle total sobre os recursos da AWS que ele cria em seu nome. Não há custo adicional para o Elastic Beanstalk. Você paga apenas pelos recursos da AWS que são usados para armazenar e executar seus aplicativos.

Esse padrão inclui instruções para implantação usando a Interface de linhas de comandos do AWS Elastic Beanstalk (EB CLI) e o Console de Gerenciamento da AWS.

Casos de uso

Os casos de uso do Elastic Beanstalk incluem:

- Implementar um ambiente de protótipo para demonstrar um aplicativo de frontend. (Esse padrão usa um Dockerfile como exemplo.)
- Implantar uma API para lidar com solicitações de API para um determinado domínio.
- Implante uma solução de orquestração usando o Docker-Compose (`docker-compose.yml` não é usado como exemplo prático nesse padrão).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da AWS
- AWS EB CLI instalada localmente
- Docker instalado em uma máquina local

Limitações

- Há um limite de extração do Docker de 100 pulls por seis horas por endereço IP no plano gratuito.

Arquitetura

Pilha de tecnologias de destino

- Instâncias do Amazon Elastic Compute Cloud (Amazon EC2)
- Grupo de segurança
- Application Load Balancer
- Auto Scaling group (Grupo do Auto Scaling)

Arquitetura de destino

Automação e escala

O AWS Elastic Beanstalk pode escalar automaticamente com base no número de solicitações feitas. Os recursos da AWS criados para um ambiente incluem um Application Load Balancer, um grupo de Auto Scaling e uma ou mais instâncias da Amazon. EC2

O balanceador de carga fica na frente das EC2 instâncias da Amazon, que fazem parte do grupo Auto Scaling. O Amazon EC2 Auto Scaling inicia automaticamente EC2 instâncias adicionais da Amazon para acomodar o aumento da carga em seu aplicativo. Se a carga em seu aplicativo diminuir, o Amazon EC2 Auto Scaling interrompe as instâncias, mas mantém pelo menos uma instância em execução.

Triggers de ajuste de escala automático

O grupo Auto Scaling em seu ambiente do Elastic Beanstalk usa dois CloudWatch alarmes da Amazon para iniciar operações de escalabilidade. Os triggers padrão são dimensionados quando a média de tráfego de rede de saída de cada instância é mais alta que 6 MB ou mais baixa que 2 MB durante um período de cinco minutos. Para usar o Amazon EC2 Auto Scaling de forma eficaz, configure gatilhos apropriados para seu aplicativo, tipo de instância e requisitos de serviço. Você pode dimensionar com base em várias estatísticas, incluindo latência, E/S de disco, utilização de CPU e a contagem de solicitações. Para obter mais informações, consulte Triggers de ajuste de escala automático.

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- A AWS EB Command Line Interface (EB CLI) é um cliente de linha de comando que você pode usar para criar, configurar e gerenciar ambientes do Elastic Beanstalk.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade.

Outros serviços

- O Docker empacota o software em unidades padronizadas chamadas contêineres que incluem bibliotecas, ferramentas do sistema, código e runtime.

Código

O código desse padrão está disponível no repositório GitHub Cluster Sample Application.

Épicos

Compile com um Dockerfile

Tarefa	Descrição	Habilidades necessárias
Clone o repositório remoto.	• Para clonar o repositório, execute o comando `git clone https://github.com/aws-samples/cluster-sample-app.git .</p>`	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps
Inicialize o projeto Elastic Beanstalk Docker.	1. Crie um arquivo chamado `aws.json` na raiz. 2. No `aws.json` arquivo, adicione o código a seguir.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	"AWSEBDoc
	kerrunVersion":"1",
	"Image":{
	"Name":"c
	luster-sample-app"
	},
	"Ports":[
	{
	"ContainerPort":80
	,
	"HostPort":8080
	}
	]
	}</pre> 3. Execute o comando `eb init -p docker` na raiz do projeto.	

Teste o projeto localmente	1. Execute o comando `eb local run` na raiz do projeto. 2. Teste o aplicativo ao navegar até `http://localhost` .	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Implante usando a EB CLI

Tarefa	Descrição	Habilidades necessárias
Execute o comando de implantação	1. Execute o comando `eb create docker-sa`	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`mple-cluster-app` na raiz do projeto.	
Acesse a versão implantada.	Depois que o comando de implantação for concluído, acesse o projeto usando o comando `eb open`.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Implante usando o console

Tarefa	Descrição	Habilidades necessárias
Implante o aplicativo usando o navegador.	1. Abra o console de . 2. Navegue até o console do Elastic Beanstalk. 3. Escolha Criar aplicativo. 4. Em Nome do aplicativo, insira Cluster-Sample-App. 5. Escolha o Docker como plataforma. 6. Escolha Carregar seu código. 7. Escolha seu arquivo .zip local (na raiz do projeto clonado) ou uma URL pública do Amazon Simple Storage Service (Amazon S3).	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps
Acesse a versão implantada.	Após a implantação, acesse o aplicativo implantado e escolha a URL fornecida.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Recursos relacionados

- Ambientes de servidor da web
- Instalar a EB CLI no macOS
- Instalar a CLI do EB manualmente

Mais informações

Vantagens de usar o Elastic Beanstalk

- Provisionamento automático da infraestrutura
- Gerenciamento automático da plataforma subjacente
- Correções e atualizações automáticas para oferecer suporte ao aplicativo
- Ajuste de escala automático da aplicação
- Capacidade de personalizar o número de nós
- Capacidade de acessar os componentes da infraestrutura, se necessário
- Facilidade de implantação em relação a outras soluções de implantação de contêineres

Gere um endereço IP de saída estático usando uma função do Lambda, Amazon VPC e uma arquitetura de tecnologia sem servidor

Criado por Thomas Scott (AWS)

Resumo

Esse padrão descreve como gerar um endereço IP de saída estático na Nuvem da Amazon Web Services (AWS) usando uma arquitetura de tecnologia sem servidor. Sua organização pode se beneficiar dessa abordagem se quiser enviar arquivos para uma entidade comercial separada usando o Secure File Transfer Protocol (SFTP). Isso significa que a entidade comercial deve ter acesso a um endereço IP que permita que os arquivos passem pelo firewall.

A abordagem do padrão ajuda você a criar uma função do AWS Lambda que usa um endereço IP elástico como endereço IP de saída. Seguindo as etapas desse padrão, você pode criar uma função do Lambda e uma nuvem privada virtual (VPC) que roteia o tráfego de saída por meio de um gateway da Internet com um endereço IP estático. Para usar o endereço IP estático, você anexa a função do Lambda à VPC e suas sub-redes.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões do AWS Identity and Access Management (IAM) para criar e implementar uma função do Lambda e criar uma VPC e suas sub-redes. Para obter mais informações, consulte Função de execução e permissões de usuário na documentação da AWS Lambda.
- Se você planeja usar a infraestrutura como código (IaC) para implementar a abordagem desse padrão, você precisa de um ambiente de desenvolvimento integrado (IDE), como o AWS Cloud9. Para obter mais informações sobre isso, consulte O que é o AWS Cloud9? na documentação do AWS Cloud9.

Arquitetura

O diagrama a seguir mostra a arquitetura de tecnologia sem servidor desse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. O tráfego de saída de `NAT gateway 1` em `Public subnet 1`.
2. O tráfego de saída de `NAT gateway 2` em `Public subnet 2`.
3. A função do Lambda pode ser executada em `Private subnet 1` ou `Private subnet 2`.
4. `Private subnet 1` e `Private subnet 2` roteiam o tráfego para os gateways NAT nas sub-redes públicas.
5. Os gateways NAT enviam tráfego de saída para o gateway da Internet a partir das sub-redes públicas.
6. Os dados de saída são transferidos do gateway da Internet para o servidor externo.

Pilha de tecnologia

- Lambda
- Amazon Virtual Private Cloud (Amazon VPC)

Automação e escala

Você pode garantir a alta disponibilidade (HA) usando duas sub-redes públicas e duas privadas em diferentes zonas de disponibilidade. Mesmo que uma zona de disponibilidade fique indisponível, a solução do padrão continua funcionando.

Ferramentas

- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- Amazon VPC: a Amazon Virtual Private Cloud (Amazon VPC) permite provisionar uma seção logicamente isolada da Nuvem AWS, em que é possível executar recursos da AWS em uma rede virtual que você mesmo define. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu datacenter, com os benefícios de usar a infraestrutura dimensionável da AWS.

Épicos

Crie uma nova VPC

Tarefa	Descrição	Habilidades necessárias
Crie uma nova VPC.	Faça login no AWS Management Console, abra o console Amazon VPC e crie uma VPC chamada `Lambda VPC` que tenha `10.0.0.0/25` como intervalo CIDR. IPv4 Para obter mais informações sobre como criar uma VPC, consulte Conceitos básicos da Amazon VPC na documentação da Amazon VPC.	Administrador da AWS

Crie duas sub-redes públicas

Tarefa	Descrição	Habilidades necessárias
Crie a primeira sub-rede pública.	1. No console do Amazon VPC, escolha Sub-redes e, em seguida, escolha Criar sub-rede. 2. Em Nomear tag, insira `public-one` . 3. Em VPC, escolha `Lambda VPC`. 4. Escolha uma zona de disponibilidade e registre-a.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	5. Para bloco IPv4 CIDR, insira `10.0.0.0/28` e escolha Criar sub-rede.	
Crie a segunda sub-rede pública.	1. No console do Amazon VPC, escolha Sub-redes e, em seguida, escolha Criar sub-rede. 2. Em Nomear tag, insira `public-two` . 3. Em VPC, escolha `Lambda` VPC. 4. **Important** Escolha uma zona de disponibilidade e registre-a. : você não pode usar a zona de disponibilidade que contém a `public-one` sub-rede. 5. Para bloco IPv4 CIDR, insira `10.0.0.16/28` e escolha Criar sub-rede.	Administrador da AWS

Criar duas sub-redes privadas

Tarefa	Descrição	Habilidades necessárias
Criar a primeira sub-rede privada.	1. No console do Amazon VPC, escolha Sub-redes e,	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	em seguida, escolha Criar sub-rede. 2. Em Nomear tag, insira `private-one` . 3. Em VPC, escolha `Lambda VPC`. 4. Escolha a zona de disponibilidade que contém a sub-rede `public-one` que você criou anteriormente. 5. Para bloco IPv4 CIDR, insira `10.0.0.32/28` e escolha Criar sub-rede.	
Crie a segunda sub-rede privada.	1. No console do Amazon VPC, escolha Sub-redes e, em seguida, escolha Criar sub-rede. 2. Em Nomear tag, insira `private-two` . 3. Em VPC, escolha `Lambda VPC`. 4. Escolha a mesma zona de disponibilidade que contém a sub-rede `public-two` que você criou anteriormente. 5. Para bloco IPv4 CIDR, insira `10.0.0.64/28` e escolha Criar sub-rede.	Administrador da AWS

Criar um endereço IP elástico para o seu gateway NAT

Tarefa	Descrição	Habilidades necessárias
Crie o primeiro endereço IP elástico.	1. No console da Amazon VPC, escolha Elastic IPs e, em seguida, escolha Alocar novo endereço. 2. Escolha Alocar e registre o ID de alocação para seu endereço IP elástico recém-criado. **Note** Esse endereço IP elástico é usado para seu primeiro gateway NAT.	Administrador da AWS
Crie o segundo endereço IP elástico.	1. No console da Amazon VPC, escolha Elastic IPs e, em seguida, escolha Alocar novo endereço. 2. Escolha Alocar e registre o ID de alocação para esse segundo endereço IP elástico. **Note** Esse endereço IP elástico é usado para	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	seu segundo gateway NAT.	

Criar um gateway da internet

Tarefa	Descrição	Habilidades necessárias
Crie um gateway da Internet.	1. No console da Amazon VPC escolha Gateway da Internet e escolha Criar gateway da Internet. 2. Insira `Lambda internet gateway` como nome e escolha Criar gateway da internet. Certifique-se de registrar o ID do gateway da internet.	Administrador da AWS
Anexar o Gateway da Internet à VPC.	Selecione o gateway da internet criado e escolha Actions, Attach to VPC (Ações, anexar à VPC).	Administrador da AWS

Crie dois gateways NAT

Tarefa	Descrição	Habilidades necessárias
Crie o primeiro gateway NAT.	1. No console do Amazon VPC, escolha NAT Gateways e, em seguida, escolha Create NAT Gateway.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	2. Insira `nat-one` como o nome do gateway NAT. 3. Selecione a `public-one` como a sub-rede na qual o gateway NAT deve ser criado. 4. Em Tipo de conectividade, escolha Público. 5. Em ID de alocação do IP elástico, escolha o ID do endereço IP elástico que você criou anteriormente e o associe ao gateway NAT. 6. Escolha Criar um gateway NAT.	

Tarefa	Descrição	Habilidades necessárias
Crie o segundo gateway NAT.	1. No console do Amazon VPC, escolha NAT Gateways e, em seguida, escolha Create NAT Gateway. 2. Insira `nat-two` como o nome do gateway NAT. 3. Selecione a sub-rede `public-two` na qual o gateway NAT deve ser criado. 4. Em Tipo de conectividade, escolha Público. 5. Em ID de alocação do IP elástico, escolha o ID do endereço IP elástico que você criou anteriormente e associe ao gateway NAT. 6. Escolha Criar um gateway NAT.	Administrador da AWS

Crie tabelas de rotas para suas sub-redes públicas e privadas

Tarefa	Descrição	Habilidades necessárias
Crie a tabela de rotas para a sub-rede pública.	1. No console do Amazon VPC, escolha Tabela de rotas e, em seguida, escolha Criar tabela de rotas. 2. Insira `public-one-subnet` como nome da	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	tabela de rotas e escolha Criar tabela de rotas. 3. Escolha a tabela de rotas `public-one-subnet` , escolha Editar rotas e, em seguida, escolha Adicionar rota. 4. Especifique `0.0.0.0` na caixa de Destino e selecione o ID do gateway da internet na lista Target. 5. Na guia Associações de sub-rede, escolha Editar associações de sub-rede, marque a caixa de seleção da sub-rede `public-one` com o `10.0.0.0/28` intervalo CIDR e, em seguida, escolha Salvar associações. 6. Escolha Salvar alterações.	

Tarefa	Descrição	Habilidades necessárias
Crie a tabela de rotas para a sub-rede pública dois.	1. No console do Amazon VPC, escolha Tabela de rotas e, em seguida, escolha Criar tabela de rotas. 2. Insira `public-two-subnet` como nome da tabela de rotas e escolha Criar tabela de rotas. 3. Escolha a tabela de rotas `public-two-subnet` , escolha Editar rotas e, em seguida, escolha Adicionar rota. 4. Especifique `0.0.0.0` na caixa de Destino e selecione o ID do gateway da internet na lista Target. 5. Na guia Associações de sub-rede, escolha Editar associações de sub-rede, marque a `public-two` sub-rede com o `10.0.0.16/28` intervalo CIDR e, em seguida, escolha Salvar associaçõ es. 6. Escolha Salvar alterações.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Crie a tabela de rotas para a sub-rede privada-um.	1. No console do Amazon VPC, escolha Tabela de rotas e, em seguida, escolha Criar tabela de rotas. 2. Insira `private-one-subnet` como nome da tabela de rotas e escolha Criar tabela de rotas. 3. Escolha a tabela de rotas `private-one-subnet`, escolha Editar rotas e, em seguida, escolha Adicionar rota. 4. Especifique `0.0.0.0` na caixa Destino e selecione o gateway NAT da internet na sub-rede `public-one` na lista do Target. 5. Na guia Associações de sub-rede, escolha Editar associações de sub-rede, marque a `10.0.0.32/28` sub-rede **`private-one`** com o intervalo CIDR e, em seguida, escolha Salvar associações. 6. Escolha Salvar alterações.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Crie a tabela de rotas para a sub-rede privada.	1. No console do Amazon VPC, escolha Tabela de rotas e, em seguida, escolha Criar tabela de rotas. 2. Insira `private-two-subnet` como nome da tabela de rotas e escolha Criar tabela de rotas. 3. Escolha a tabela de rotas `private-two-subnet`, escolha Editar rotas e, em seguida, escolha Adicionar rota. 4. Especifique `0.0.0.0` na caixa Destino e selecione o gateway NAT da internet na sub-rede `public-two` na lista do Target. 5. Na guia Associações de sub-rede, escolha Editar associações de sub-rede, marque a sub-rede `private-two` com o intervalo CIDR `10.0.0.64/28` e, em seguida, escolha Salvar associações. 6. Escolha Salvar alterações.	Administrador da AWS

Crie a função do Lambda, adicione-a à VPC e teste a solução

Tarefa	Descrição	Habilidades necessárias
Crie uma nova função do Lambda.	1. Abra o console do AWS Lambda e escolha Criar função. 2. Em Informações básicas, insira `Lambda test` em Nome da função e escolha o idioma de sua preferência em Runtime. 3. Escolha a opção Criar função.	Administrador da AWS
Adicione a função do Lambda ao seu VPC.	1. Abra a página Funções do console do AWS Lambda, escolha a função que você criou anteriormente. 2. Escolha Configuration (Configuração) e, em seguida, escolha VPC. 3. Escolha Editar e, em seguida, escolha `Lambda` VPC as duas sub-redes privadas. 4. Escolha Grupo de segurança padrão para fins de teste e, em seguida, escolha Salvar.	Administrador da AWS
Escreva o código para chamar um serviço externo.	1. Na linguagem de programação de sua escolha, escreva um código para chamar um serviço	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	externo que retorna seu endereço IP. 2. Verifique se o endereço IP retornado corresponde a um dos seus endereços IP elásticos.	

Recursos relacionados

- Configurar uma função do Lambda para acessar recursos em uma VPC

Identifique automaticamente imagens de contêineres duplicadas ao migrar para um repositório Amazon ECR

Criado por Rishabh Yadav (AWS) e Rishi Singla (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

O padrão fornece uma solução automatizada para identificar se as imagens armazenadas em diferentes repositórios de contêineres são duplicatas. Essa verificação é útil quando você planeja migrar imagens de outros repositórios de contêineres para o Amazon Elastic Container Registry (Amazon ECR).

Para obter informações básicas, o padrão também descreve os componentes de uma imagem de contêiner, como o resumo da imagem, o manifesto e as tags. Ao planejar uma migração para o Amazon ECR, você pode decidir sincronizar suas imagens de contêiner em todos os registros de contêineres comparando os resumos das imagens. Antes de migrar suas imagens de contêiner, você precisa verificar se essas imagens já existem no repositório Amazon ECR para evitar duplicações. No entanto, pode ser difícil detectar duplicações comparando resumos de imagens, o que pode causar problemas na fase inicial de migração. Esse padrão compara os resumos de duas imagens semelhantes que estão armazenadas em diferentes registros de contêineres e explica por que os resumos variam, para ajudar você a comparar imagens com precisão.

Pré-requisitos e limitações

- Um ativo Conta da AWS
- Acesso ao registro público do Amazon ECR
- Familiaridade com o seguinte: Serviços da AWS
  - AWS CodeCommit
  - AWS CodePipeline
  - AWS CodeBuild
  - AWS Identity and Access Management (IAM)
  - Amazon Simple Storage Service (Amazon S3)
- CodeCommit Credenciais configuradas (consulte as instruções)

Arquitetura

Componentes de imagem de contêiner

O diagrama a seguir ilustra alguns dos componentes de uma imagem de contêiner. Esses componentes são descritos após o diagrama.

Termos e definições

Os termos a seguir são definidos na Especificação de Imagem da Open Container Initiative (OCI).

- Registro: um serviço para armazenamento e gerenciamento de imagens.
- Cliente: Uma ferramenta que se comunica com registros e trabalha com imagens locais.
- Push: O processo de upload de imagens para um registro.
- Pull: O processo para baixar imagens de um registro.
- Blob: a forma binária de conteúdo que é armazenada por um registro e pode ser tratada por um resumo.
- Índice: uma construção que identifica vários manifestos de imagem para diferentes plataformas de computador (como x86-64 ou ARM de 64 bits) ou tipos de mídia. Para obter mais informações, consulte a Especificação do Índice de Imagem OCI.
- Manifesto: um documento JSON que define uma imagem ou artefato que é carregado por meio do endpoint do manifesto. Um manifesto pode fazer referência a outros blobs em um repositório usando descritores. Para obter mais informações, consulte a Especificação do manifesto de imagem OCI.
- Camada do sistema de arquivos: bibliotecas do sistema e outras dependências de uma imagem.
- Configuração: um blob que contém metadados de artefatos e é referenciado no manifesto. Para obter mais informações, consulte a Especificação de configuração de imagem OCI.
- Objeto ou artefato: um item de conteúdo conceitual armazenado como um blob e associado a um manifesto anexo com uma configuração.
- Resumo: um identificador exclusivo criado a partir de um hash criptográfico do conteúdo de um manifesto. O resumo da imagem ajuda a identificar de forma exclusiva uma imagem de contêiner imutável. Ao extrair uma imagem usando seu resumo, você baixará a mesma imagem todas as vezes em qualquer sistema operacional ou arquitetura. Para obter mais informações, consulte a Especificação de imagem OCI.

- Tag: Um identificador de manifesto legível por humanos. Em comparação com os resumos de imagens, que são imutáveis, as tags são dinâmicas. Uma tag que aponta para uma imagem pode mudar e passar de uma imagem para outra, embora o resumo da imagem subjacente permaneça o mesmo.

Arquitetura de destino

O diagrama a seguir mostra a arquitetura de alto nível da solução fornecida por esse padrão para identificar imagens de contêineres duplicadas comparando imagens armazenadas no Amazon ECR e em repositórios privados.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeCommité um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar as alterações de software continuamente.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.

Código

O código desse padrão está disponível na solução automatizada do GitHub repositório para identificar imagens de contêineres duplicadas entre repositórios.

Práticas recomendadas

- AWS CloudFormation melhores práticas

- AWS CodePipeline melhores práticas

Épicos

Extraia imagens de contêineres dos repositórios públicos e privados do Amazon ECR

Tarefa	Descrição	Habilidades necessárias

Extraia uma imagem do repositório público do Amazon ECR.	No terminal, execute o comando a seguir para extrair a imagem `amazonlinux` do repositório público do Amazon ECR.
	`$~ % docker pull public.ecr.aws/amazonlinux/amazonlinux:2018.03`
	Quando a imagem for transferida para sua máquina local, você verá o seguinte resumo, que representa o índice da imagem.
	`2018.03: Pulling from amazonlinux/amazonlinux`
	`4ddc0f8d367f: Pull complete`
	`Digest: sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5`
	`Status: Downloaded newer image for public.ecr.aws/ama`
		Desenvolvedor de aplicativos, AWS DevOps, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	zonlinux/amazonlin ux:2018.03 public.ecr.aws/a mazonlinux/amazonl inux:2018.03	

Tarefa	Descrição	Habilidades necessárias

Envie a imagem para um repositório privado do Amazon ECR.	1. Crie um repositório privado do Amazon ECR chamado `test_ecr_repository` na região Leste dos EUA (Norte da Virgínia) (`us-east-1`).
	`$~ % aws ecr get-login -password --region us-east-1 | docker login --username AWS --password-stdin <account-id>.dkr.ecr.us-east-1.amazonaws.com`
	`Login Succeeded`
	onde `<account-id>` se refere ao seu Conta da AWS.
	2. Marque a imagem local que você extraiu anteriormente. Use o valor `public.ecr.aws/amazonlinux/amazonlinux:2018.03` e envie-o para o repositório privado do Amazon ECR.
	`$~ % docker tag public.ecr.aws/amazonlinux/amazonlinux:2018.03 <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
		Administrador da AWS, AWS DevOps, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	`$~ % docker push <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	Quando você envia a imagem para o repositório Amazon ECR, o Docker envia a imagem subjacente e não o índice da imagem.
	
	`The push refers to repository [<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository] d5655967c2c4: Pushed latest: digest: sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02 size: 529`	

Tarefa	Descrição	Habilidades necessárias

Extraia a mesma imagem do repositório privado do Amazon ECR.	1. No terminal, execute o comando a seguir para extrair a imagem que você enviou anteriormente para o repositório privado do Amazon ECR.
	`$~ % docker pull <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	`latest: Pulling from test_ecr_repository`
	`Digest: sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02`
	`Status: Image is up to date for <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	`<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	O resumo dessa imagem corresponde ao resumo da imagem que você enviou para o repositório privado do Amazon ECR e representa a imagem subjacente. Esse valor não corresponde ao índice de
		Desenvolvedor de aplicativos, AWS DevOps, administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	imagens que você extraiu do repositório público.
	2. Para verificar, recupere o índice da imagem por resumo.
	
	`curl -k -H “Authorization: Bearer $TOKEN” https://public.ecr.aws/v2/amazonlinux/amazonlinux/manifests/sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b55`
	`{`
	`“schemaVersion”: 2,`
	`“mediaType”: “application/vnd.docker.distribution.manifest.list.v2+json”,`
	`“manifests”: [`
	`{`
	`“mediaType”: “application/vnd.docker.distribution.manifest.v2+json”,`
	`“size”: 529,`
	`“digest”: “sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02”,`
	`“platform”: {`	

Tarefa	Descrição	Habilidades necessárias

	<pre>“architec
	ture”: “amd64”,
	“os”:
	“linux”
	}
	}
	]
	}</pre>	

Compare os manifestos de imagem

Tarefa	Descrição	Habilidades necessárias

Encontre o manifesto da imagem armazenada no repositório público do Amazon ECR.	No terminal, execute o comando a seguir para extrair o manifesto da imagem `public.ecr.aws/amazonlinux/amazonlinux:2018.03` do repositório público do Amazon ECR.
	<pre>$~ % docker manifest
	inspect public.ec
	r.aws/amazonlinux/
	amazonlinux:2018.03
	{
	"schemaVersion": 2,
	"mediaType":
	"application/vnd.d
	ocker.distribution
	.manifest.list.v2+
	json",
	"manifests": [
	{
	"mediaType":
	"application/vnd.d
	ocker.distribution
	.manifest.v2+json",</pre>
		Administrador da AWS, AWS DevOps, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	"size": 529,
	"digest":
	"sha256:52db900007
	3d93b9bdee6a7246a6
	8c35a741aaade05a8f
	4febba0bf795cdac02",
	"platform": {
	"architec
	ture": "amd64",
	"os":
	"linux"
	}
	}
	]
	}	

Tarefa	Descrição	Habilidades necessárias

Encontre o manifesto da imagem armazenada no repositório privado do Amazon ECR.	No terminal, execute o comando a seguir para extrair o manifesto da imagem `<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest` do repositório privado do Amazon ECR.
	
	`$~ % docker manifest inspect <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	`{`
	`"schemaVersion": 2,`
	`"mediaType": "application/vnd.docker.distribution.manifest.v2+json",`
	`"config": {`
	`"mediaType": "application/vnd.docker.container.image.v1+json",`
	`"size": 1477,`
	`"digest": "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68"`
	`},`
	`"layers": [`
	`{`
		AWS DevOps, administrador de sistemas da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	"mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip", "size": 62267075, "digest": "sha256:4ddc0f8d367f424871a060e2067749f32bd36a91085e7140dcb159952f2d71453" }] }	

Tarefa	Descrição	Habilidades necessárias
Compare o resumo obtido pelo Docker com o resumo do manifesto da imagem no repositório privado do Amazon ECR.	Outra questão é por que o resumo fornecido pelo comando docker pull difere do resumo do manifesto para a imagem. `<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest` O resumo usado para docker pull representa o resumo do manifesto da imagem, que é armazenado em um registro. Esse resumo é considerado a raiz de uma cadeia de hash, porque o manifesto contém o hash do conteúdo que será baixado e importado para o Docker. O ID da imagem usado no Docker pode ser encontrado neste manifesto como `config.digest` . Isso representa a configuração de imagem que o Docker usa. Então, você poderia dizer que o manifesto é o envelope e a imagem é o conteúdo do envelope. O resumo do manifesto é sempre diferente do ID da imagem. No entanto, um manifesto específico deve sempre produzir o mesmo ID	AWS DevOps, administrador de sistemas da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	de imagem. Como o resumo do manifesto é uma cadeia de hash, não podemos garantir que sempre será o mesmo para um determinado ID de imagem. Na maioria dos casos, ele produz o mesmo resumo, embora o Docker não possa garantir isso. A possível diferença no resumo do manifesto decorre do fato de o Docker não armazenar localmente os blobs que são compactados com o gzip. Portanto, a exportação de camadas pode produzir um resumo diferente, embora o conteúdo não compactado permaneça o mesmo. O ID da imagem verifica se o conteúdo não compactado é o mesmo; ou seja, o ID da imagem agora é um identificador de conteúdo endereçável (). `chainID` Para confirmar essas informações, você pode comparar a saída do comando docker inspect nos repositór ios públicos e privados do Amazon ECR: 1. Execute o seguinte comando em seu terminal para a imagem armazenad	

Tarefa	Descrição	Habilidades necessárias

	a no repositório público do Amazon ECR.
	
	`$~ % docker inspect public.ecr.aws/amazonlinux/amazonlinux:2018.03`
	
	Para ver a saída do comando, consulte a seção Informações adicionais.
	2. Execute o seguinte comando em seu terminal para a imagem armazenada no repositório privado do Amazon ECR.
	
	`$~ % docker inspect <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	Para ver a saída do comando, consulte a seção Informações adicionais.
	
	Os resultados verificam se as duas imagens têm o mesmo resumo de ID de imagem e resumo de camada.
	
	ID: `f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68`	

Tarefa	Descrição	Habilidades necessárias
	Camadas: `d5655967c 2c4e8d68f8ec7cf753 218938669e6c16ac13 24303c073c736a2e2a2` Além disso, os resumos são baseados nos bytes do objeto gerenciado localment e (o arquivo local é um tar da camada de imagem do contêiner) ou no blob enviado ao servidor de registro. No entanto, quando você envia o blob para um registro, o tar é compactado e o resumo é computado no arquivo tar compactado. Portanto, a diferença no valor do resumo do docker pull surge da compactação aplicada no nível do registro (Amazon ECR privado ou público). **Note** Essa explicação é específica para o uso de um cliente Docker. Você não verá esse comportamento com outros clientes, como nerdctl ou Finch, porque eles não compactam automatic amente a imagem	

Tarefa	Descrição	Habilidades necessárias
	durante as operações de push e pull.	

Identifique automaticamente imagens duplicadas entre os repositórios públicos e privados do Amazon ECR

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Clone o repositório Github desse padrão em uma pasta local: `$git clone https://github.com/aws-samples/automated-solution-to-identify-duplicate-container-images-between-repositories`	Administrador da AWS, AWS DevOps
Configure um pipeline de CI/CD.	O GitHub repositório inclui um `.yaml` arquivo que cria uma AWS CloudFormation pilha para configurar um pipeline. AWS CodePipeline 1. Faça login no AWS Management Console e abra o AWS CloudFormation console. 2. Crie uma pilha usando o `pipeline.yaml` arquivo de modelo, que está na `code` pasta no repositório clonado.	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	3. Aceite ou altere os valores padrão dos parâmetros. Especifique valores para os seguintes campos: • Nome da pilha • `ArtifactStoreBucketName` — Um bucket S3 existente que será usado para armazenar artefatos AWS CodePipeline • `OutputBucket` — Um bucket S3 existente que será usado para armazenar as URIs imagens duplicadas • `SourceImageFile` — Um arquivo de texto existente chamado `input.txt` que contém a imagem URIs do repositório público que será verificada no repositório privado do Amazon ECR para detectar duplicações 4. Revise e ajuste as opções de pilha e, em seguida, escolha Enviar para executar o modelo. O pipeline será configura do com dois estágios (CodeCommit e CodeBuild	

Tarefa	Descrição	Habilidades necessárias
	, conforme mostrado no diagrama da arquitetura) para identificar imagens no repositório privado que também existem no repositório público. O pipeline é configura do com os seguintes recursos: • CodePipeline para a orquestração do pipeline de implantação. • Um CodeCommit repositór io para armazenar o script bash e o arquivo de entrada. O script bash é usado para comparar a imagem do contêiner IDs nos repositórios público e privado para encontrar duplicações. Essa verificaç ão é realizada em todos os repositórios especificados Conta da AWS em um único Região da AWS. • Um CodeBuild projeto para invocar o script bash para identificar imagens que já estão presentes no repositór io Amazon ECR. • Funções necessárias do IAM para permitir o acesso. • Um bucket do S3 para armazenar o arquivo de	

Tarefa	Descrição	Habilidades necessárias
	saída que contém a imagem URIs. • Outro bucket S3 para armazenar CodePipeline artefatos.	

Tarefa	Descrição	Habilidades necessárias
Preencha o CodeCommit repositório.	Para preencher o CodeCommit repositório, execute estas etapas: 1. Abra o CodeCommit console e navegue até o Região da AWS local onde você criou a CloudFormation pilha. 2. Encontre o repositório que você provisionou usando o CloudFormation script da lista, escolha Clone URL e, em seguida, copie o protocolo de URL HTTPS para se conectar ao repositório. 3. Abra um prompt de comando e execute o comando git clone com a URL HTTPS que você copiou na etapa anterior. 4. Navegue até o diretório raiz. Crie um arquivo chamado `input.txt` e preencha esse arquivo com o registro público de imagens do Amazon ECR URIs que você gostaria de pesquisar no repositório privado do Amazon ECR. 5. Copie os arquivos `script.sh buildspec.yml` , e `input.txt`	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	de sua cópia local do GitHub repositório Solução automatizada para identificar imagens de contêiner duplicadas entre repositórios para o repositório clonado. CodeCommit
	6. Faça upload dos arquivos CodeCommit usando estes comandos:
	`git add .`
	`git commit -m “added input files”`
	`git push`	

Limpeza.	Para evitar cobranças futuras, exclua os recursos seguindo estas etapas: 1. Navegue até o bucket do S3 que armazena os CodePipeline artefatos e esvazie o bucket. 2. Navegue até o bucket do S3 que armazena a imagem URIs duplicada e esvazie o bucket. 3. Navegue até o CloudFormation console e exclua a pilha que você criou para configurar o pipeline.	Administrador da AWS

Solução de problemas

Problema	Solução
Ao tentar enviar, extrair ou interagir de outra forma com um CodeCommit repositório a partir do terminal ou da linha de comando, você é solicitado a fornecer um nome de usuário e uma senha, além de fornecer as credenciais do Git para seu usuário do IAM.	As causas mais comuns desse erro são as seguintes: • Seu computador local está executando um sistema operacional que não oferece suporte ao gerenciamento de credenciais ou não tem um utilitário de gerenciamento de credenciais instalado. • As credenciais do Git para seu usuário do IAM não foram salvas em um desses sistemas de gerenciamento de credenciais. Dependendo de seu sistema operacional e ambiente local, talvez seja necessário instalar um gerenciador de credenciais, configurar o gerenciador de credenciais incluído no sistema operacional ou personalizar o ambiente local para usar o armazenamento de credencia is. Por exemplo, se seu computador estiver executando o macOS, você pode usar o utilitári o Acesso às Chaves para armazenar suas credenciais. Se seu computador for Windows, você pode usar o Git Credential Manager que é instalado com o Git para Windows. Para obter mais informações, consulte Configuração para usuários HTTPS usando credenciais do Git na CodeCommit documentação e Armazenamento de credenciais na documentação do Git.
Você encontra erros de HTTP 403 ou “sem credenciais básicas de autenticação” ao enviar uma imagem para o repositório Amazon ECR.	Você pode encontrar essas mensagens de erro do comando docker push ou docker pull, mesmo que tenha se autenticado com sucesso

Problema	Solução
	no Docker usando o comando aws ecr. get-login-password As causas conhecidas são: • Você se autenticou em uma região diferente . Para obter mais informações, consulte Autenticação de registro privado na documentação do Amazon ECR. • Você se autenticou para enviar para um repositório para o qual não tem permissões. Para obter mais informações, consulte Políticas de repositório privado na documentação do Amazon ECR. • Seu token expirou. O período de expiração padrão para tokens obtidos usando a `GetAuthorizationToken` operação é de 12 horas.

Recursos relacionados

- Solução automatizada para identificar imagens de contêineres duplicadas entre repositórios (GitHub repositório)
- Galeria pública do Amazon ECR
- Imagens privadas no Amazon ECR (documentação do Amazon ECR)
- AWS::CodePipeline::Pipeline recurso (AWS CloudFormation documentação)
- Especificação do formato de imagem OCI

Mais informações

Saída da inspeção Docker para imagem no repositório público do Amazon ECR

```
[
    {
        "Id":
 "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68",
```

```
        "RepoTags": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest",
            "public.ecr.aws/amazonlinux/amazonlinux:2018.03"
        ],
        "RepoDigests": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/
test_ecr_repository@sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",
            "public.ecr.aws/amazonlinux/
amazonlinux@sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5"
        ],
        "Parent": "",
        "Comment": "",
        "Created": "2023-02-23T06:20:11.575053226Z",
        "Container":
 "ec7f2fc7d2b6a382384061247ef603e7d647d65f5cd4fa397a3ccbba9278367c",
        "ContainerConfig": {
            "Hostname": "ec7f2fc7d2b6",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/sh",
                "-c",
                "#(nop) ",
                "CMD [\"/bin/bash\"]"
            ],
            "Image":
 "sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": {}
        },
        "DockerVersion": "20.10.17",
        "Author": "",
```

```
        "Config": {
            "Hostname": "",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image":
 "sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": null
        },
        "Architecture": "amd64",
        "Os": "linux",
        "Size": 167436755,
        "VirtualSize": 167436755,
        "GraphDriver": {
            "Data": {
                "MergedDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/merged",
                "UpperDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/diff",
                "WorkDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/work"
            },
            "Name": "overlay2"
        },
        "RootFS": {
            "Type": "layers",
            "Layers": [

 "sha256:d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2"
```

```
            ]
        },
        "Metadata": {
            "LastTagTime": "2023-03-02T10:28:47.142155987Z"
        }
    }
]
```

Saída da inspeção do Docker para imagem no repositório privado do Amazon ECR

```
[
    {
        "Id":
 "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68",
        "RepoTags": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest",
            "public.ecr.aws/amazonlinux/amazonlinux:2018.03"
        ],
        "RepoDigests": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/
test_ecr_repository@sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",
            "public.ecr.aws/amazonlinux/
amazonlinux@sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5"
        ],
        "Parent": "",
        "Comment": "",
        "Created": "2023-02-23T06:20:11.575053226Z",
        "Container":
 "ec7f2fc7d2b6a382384061247ef603e7d647d65f5cd4fa397a3ccbba9278367c",
        "ContainerConfig": {
            "Hostname": "ec7f2fc7d2b6",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
```

```
                "/bin/sh",
                "-c",
                "#(nop) ",
                "CMD [\"/bin/bash\"]"
            ],
            "Image":
"sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": {}
        },
        "DockerVersion": "20.10.17",
        "Author": "",
        "Config": {
            "Hostname": "",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image":
"sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": null
        },
        "Architecture": "amd64",
        "Os": "linux",
        "Size": 167436755,
        "VirtualSize": 167436755,
        "GraphDriver": {
```

```
            "Data": {
                "MergedDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/merged",
                "UpperDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/diff",
                "WorkDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/work"
            },
            "Name": "overlay2"
        },
        "RootFS": {
            "Type": "layers",
            "Layers": [

 "sha256:d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2"
            ]
        },
        "Metadata": {
            "LastTagTime": "2023-03-02T10:28:47.142155987Z"
        }
    }
]
```

Instale o agente SSM nos nós de trabalho do Amazon EKS usando o Kubernetes DaemonSet

Criado por Mahendra Revanasiddappa (AWS)

Resumo

Observação, setembro de 2021: a última versão otimizada do Amazon EKS AMIs instala o SSM Agent automaticamente. Para obter mais informações, consulte as notas de lançamento de junho de 2021 AMIs.

No Amazon Elastic Kubernetes Service (Amazon EKS), devido às diretrizes de segurança, os nós de processamento não têm pares de chaves Secure Shell (SSH) anexados a eles. Esse padrão mostra como você pode usar o tipo de DaemonSet recurso Kubernetes para instalar o AWS Systems Manager Agent (SSM Agent) em todos os nós de trabalho, em vez de instalá-lo manualmente ou substituir a Amazon Machine Image (AMI) pelos nós. DaemonSet usa um cron job no nó de trabalho para agendar a instalação do SSM Agent. Você também pode usar esse padrão para instalar outros pacotes nos nós de processamento.

Quando você está solucionando problemas no cluster, a instalação do SSM Agent sob demanda permite estabelecer uma sessão SSH com o nó de processamento, coletar logs ou examinar a configuração da instância, sem pares de chaves SSH.

Pré-requisitos e limitações

Pré-requisitos

- Um cluster Amazon EKS existente com nós de trabalho do Amazon Elastic Compute Cloud (Amazon EC2).
- As instâncias de contêiner devem ter as permissões necessárias para se comunicar com o serviço SSM. A função gerenciada do AWS Identity and Access Management (IAM), a Amazon SSMManaged InstanceCore fornece as permissões necessárias para que o SSM Agent seja executado em EC2 instâncias. Para obter mais informações, consulte a documentação do AWS Systems Manager.

Limitações

- Esse padrão não é aplicável ao AWS Fargate, porque DaemonSets não são compatíveis com a plataforma Fargate.

- Esse padrão se aplica somente aos nós de processamento baseados em Linux.
- Os DaemonSet pods funcionam em modo privilegiado. Se o cluster do Amazon EKS tiver um webhook que bloqueia pods no modo privilegiado, o SSM Agent não será instalado.

Arquitetura

O diagrama a seguir ilustra a arquitetura desse padrão.

Ferramentas

Ferramentas

- O kubectl é um utilitário de linha de comando que é usado para interagir com um cluster do Amazon EKS. Esse padrão é usado `kubectl` para implantar um DaemonSet no cluster Amazon EKS, que instalará o SSM Agent em todos os nós de trabalho.
- O Amazon EKS facilita para você a execução do Kubernetes na AWS, eliminando a necessidade de instalar, operar e manter seu próprio ambiente de gerenciamento ou nós do Kubernetes. O Kubernetes é um sistema de código aberto para automatizar a implantação, a escalabilidade e o gerenciamento de aplicações em contêineres.
- O AWS Systems Manager Session Manager permite que você gerencie suas EC2 instâncias, instâncias locais e máquinas virtuais (VMs) por meio de um shell interativo baseado em navegador com um clique ou por meio da AWS Command Line Interface (AWS CLI).

Código

Use o código a seguir para criar um arquivo DaemonSet de configuração que instalará o SSM Agent no cluster Amazon EKS. Siga as instruções na seção Épicos.

```
cat << EOF > ssm_daemonset.yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  labels:
    k8s-app: ssm-installer
  name: ssm-installer
  namespace: kube-system
spec:
  selector:
```

```
    matchLabels:
      k8s-app: ssm-installer
  template:
    metadata:
      labels:
        k8s-app: ssm-installer
    spec:
      containers:
      - name: sleeper
        image: busybox
        command: ['sh', '-c', 'echo I keep things running! && sleep 3600']
      initContainers:
      - image: amazonlinux
        imagePullPolicy: Always
        name: ssm
        command: ["/bin/bash"]
        args: ["-c","echo '* * * * * root yum install -y https://s3.amazonaws.com/
ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm & rm -rf /etc/
cron.d/ssmstart' > /etc/cron.d/ssmstart"]
        securityContext:
          allowPrivilegeEscalation: true
        volumeMounts:
        - mountPath: /etc/cron.d
          name: cronfile
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      volumes:
      - name: cronfile
        hostPath:
          path: /etc/cron.d
          type: Directory
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      terminationGracePeriodSeconds: 30
EOF
```

Épicos

Configurar o kubectl

Tarefa	Descrição	Habilidades necessárias
Instale e configure o kubectl para acessar o cluster do EKS.	Se o `kubectl` ainda não estiver instalado e configurado para acessar o cluster do Amazon EKS, consulte Instalação do kubectl na documentação do Amazon EKS.	DevOps

Implemente o DaemonSet

Tarefa	Descrição	Habilidades necessárias
Crie o arquivo DaemonSet de configuração.	Use o código na seção Código no início desse padrão para criar um arquivo de DaemonSet configuração chamado `ssm_daemonset.yaml`, que será implantado no cluster Amazon EKS. O pod lançado por DaemonSet tem um contêiner principal e um `init` contêiner. O contêiner principal tem um comando `sleep`. O contêiner `init` inclui uma seção `command` que cria um arquivo de trabalho cron para instalar o SSM Agent no caminho `/etc/cron.d/`. O trabalho	DevOps

Tarefa	Descrição	Habilidades necessárias
	cron é executado somente uma vez, e o arquivo que ele cria é automaticamente excluído após a conclusão do trabalho. Quando o contêiner inicial terminar, o contêiner principal espera 60 minutos antes de sair. Após 60 minutos, um novo pod é lançado. Esse pod instala o SSM Agent, se estiver ausente, ou atualiza o SSM Agent para a versão mais recente. Se necessário, você pode modificar o comando `sleep` para reiniciar o pod uma vez por dia ou para executá-lo com mais frequência.	
Implemente o DaemonSet no cluster Amazon EKS.	Para implantar o arquivo de DaemonSet configuração que você criou na etapa anterior no cluster Amazon EKS, use o seguinte comando: `kubectl apply -f ssm_daemonset.yaml` Esse comando cria um DaemonSet para executar os pods nos nós de trabalho para instalar o SSM Agent.	DevOps

Recursos relacionados

- Instalação do kubectl (documentação do Amazon EKS)
- Configurando o Session Manager (documentação do AWS Systems Manager)

Instale o agente SSM e o CloudWatch agente nos nós de trabalho do Amazon EKS usando preBootstrapCommands

Criado por Akkamahadevi Hiremath (AWS)

Resumo

Esse padrão fornece exemplos de código e etapas para instalar o AWS Systems Manager Agent (SSM Agent) e o CloudWatch agente Amazon nos nós de trabalho do Amazon Elastic Kubernetes Service (Amazon EKS) na nuvem Amazon Web Services (AWS) durante a criação do cluster Amazon EKS. Você pode instalar o agente SSM e o CloudWatch agente usando a `preBootstrapCommands` propriedade do esquema do arquivo de `eksctl` configuração (documentação da Weaveworks). Em seguida, você pode usar o SSM Agent para se conectar aos seus nós de trabalho sem usar um par de chaves do Amazon Elastic Compute Cloud EC2 (Amazon). Além disso, você pode usar o CloudWatch agente para monitorar a utilização da memória e do disco nos nós de trabalho do Amazon EKS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- O utilitário de linha de comando eksctl, instalado e configurado no macOS, Linux ou Windows
- O utilitário de linha de comando kubectl, instalado e configurado no macOS, Linux ou Windows

Limitações

- Recomendamos que você evite adicionar scripts de longa execução à propriedade `preBootstrapCommands`, pois isso impede o nó se junte ao cluster do Amazon EKS durante as atividades de escalabilidade. Em vez disso, recomendamos que você crie uma imagem de máquina da Amazon (AMI) personalizada.
- Esse padrão se aplica somente às instâncias do Amazon EC2 Linux.

Arquitetura

Pilha de tecnologia

- Amazon CloudWatch
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Systems Manager Parameter Store

Arquitetura de destino

O diagrama a seguir mostra um exemplo de um usuário se conectando aos nós de processamento do Amazon EKS usando o SSM Agent, que foi instalado usando `preBootstrapCommands`.

O diagrama mostra o seguinte fluxo de trabalho:

1. O usuário cria um cluster Amazon EKS usando o arquivo de `eksctl` configuração com a `preBootstrapCommands` propriedade, que instala o agente e CloudWatch o agente SSM.
2. Todas as novas instâncias que ingressam no cluster posteriormente devido a atividades de escalabilidade são criadas com o agente e o agente SSM pré-instalados. CloudWatch
3. O usuário se conecta à Amazon EC2 usando o agente SSM e, em seguida, monitora a utilização da memória e do disco usando o CloudWatch agente.

Ferramentas

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- O AWS Systems Manager Parameter Store oferece armazenamento hierárquico seguro para o gerenciamento de dados de configuração e gerenciamento de segredos.
- O AWS Systems Manager Session Manager ajuda você a gerenciar suas EC2 instâncias, instâncias locais e máquinas virtuais por meio de um shell interativo, com um clique e baseado em navegador, ou por meio da AWS Command Line Interface (AWS CLI).
- O eksctl é utilitário de linha de comando para criar e gerenciar clusters do Kubernetes no Amazon EKS.
- O kubectl é um utilitário de linha de comando para se comunicar com o servidor da API do cluster.

Épicos

Criar um cluster do Amazon EKS.

Tarefa	Descrição	Habilidades necessárias
Armazene o arquivo de configuração do CloudWatch agente.	Armazene o arquivo de configuração do CloudWatch agente no AWS Systems Manager Parameter Store na região da AWS onde você deseja criar seu cluster Amazon EKS. Para fazer isso, crie um parâmetro no AWS Systems Manager Parameter Store e anote o nome do parâmetro (por exemplo, `AmazonCloudwatch-linux`). Para obter mais informações, consulte o exemplo de código do arquivo de configuração do CloudWatch agente na seção Informações adicionais desse padrão.	DevOps engenheiro
Criar o arquivo de configuração e o cluster eksctl.	1. Crie um arquivo `eksctl` de configuração que inclua as etapas de instalação do CloudWatch agente e do SSM Agent. Para obter mais informações, consulte o exemplo do código do arquivo de configuração ekcstl na seção de Informações adicionais deste padrão.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	2. Criar o cluster ao executar o comando `eksctl create cluster -f cluster.yaml` .	

Verifique se o agente SSM e o CloudWatch agente funcionam

Tarefa	Descrição	Habilidades necessárias
Testar o SSM Agent.	Use o SSH para se conectar aos nós de cluster do Amazon EKS usando qualquer um dos métodos abordados em Iniciar uma sessão na documentação do AWS Systems Manager.	AWS DevOps
Teste o CloudWatch agente.	Use o CloudWatch console para validar o CloudWatch agente: 1. Faça login no Console de Gerenciamento da AWS e abra o console do CloudWatch . 2. No painel de navegação, expanda Métricas e escolha Todas as métricas. 3. Na caixa de pesquisa na guia Procurar, insira e escolha CWAgent métricas para ver as métricas de memória e disco.	AWS DevOps

Recursos relacionados

- Instalando e executando o CloudWatch agente em seus servidores (CloudWatch documentação da Amazon)
- Criar um parâmetro do Systems Manager (console) (documentação do AWS Systems Manager)
- Crie o arquivo de configuração do CloudWatch agente (CloudWatch documentação da Amazon)
- Iniciar uma sessão (AWS CLI) (documentação do AWS Systems Manager).
- Iniciando uma sessão (EC2 console da Amazon) (documentação do AWS Systems Manager)

Mais informações

Exemplo de arquivo de configuração do CloudWatch agente

No exemplo a seguir, o CloudWatch agente está configurado para monitorar a utilização do disco e da memória nas instâncias do Amazon Linux:

```
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "cwagent"
    },
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "disk": {
                "measurement": [
                    "used_percent"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
```

```
                    "mem_used_percent"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

Exemplo de arquivo de configuração eksctl

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: test
  region: us-east-2
  version: "1.24"
managedNodeGroups:
  - name: test
    minSize: 2
    maxSize: 4
    desiredCapacity: 2
    volumeSize: 20
    instanceType: t3.medium
    preBootstrapCommands:
    - sudo yum install amazon-ssm-agent -y
    - sudo systemctl enable amazon-ssm-agent
    - sudo systemctl start amazon-ssm-agent
    - sudo yum install amazon-cloudwatch-agent -y
    - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-
config -m ec2 -s -c ssm:AmazonCloudwatch-linux
    iam:
      attachPolicyARNs:
        - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
        - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
        - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
        - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Outros detalhes do código

- Na última linha da propriedade `preBootstrapCommands`, `AmazonCloudwatch-linux` é o nome do parâmetro criado no AWS Systems Manager Parameter Store. É necessário incluir `AmazonCloudwatch-linux` no Parameter Store na mesma região da AWS em que o

cluster do Amazon EKS foi criado. Você também pode especificar um caminho de arquivo, mas recomendamos o uso do Systems Manager para facilitar a automação e a reutilização.

- Se você usar `preBootstrapCommands` no arquivo `eksctl` de configuração, verá dois modelos de lançamento no Console de Gerenciamento da AWS. O primeiro modelo de lançamento inclui os comandos especificados em `preBootstrapCommands`. O segundo modelo inclui os comandos especificados em `preBootstrapCommands` e os dados padrão do usuário do Amazon EKS. Esses dados são necessários para que os nós se juntem ao cluster. O grupo do Auto Scaling do grupo de nós usa esses dados do usuário para criar novas instâncias.
- Se você usar o atributo `iam` no arquivo `eksctl` de configuração, deverá listar as políticas padrão do Amazon EKS com todas as políticas adicionais exigidas nas políticas anexadas do AWS Identity and Access Management (IAM). No trecho de código da etapa Criar o arquivo de configuração eksctl e o cluster, `AmazonSSMMangedInstanceCore` são adicionadas políticas adicionais para garantir que o CloudWatch agente `CloudWatchAgentServerPolicy` e o agente SSM funcionem conforme o esperado. As políticas `AmazonEKSWorkerNodePolicy`, `AmazonEKS_CNI_Policy` e `AmazonEC2ContainerRegistryReadOnly` são políticas obrigatórias necessárias para que o cluster Amazon EKS funcione corretamente.

Migre os controladores de entrada NGINX ao ativar o modo automático do Amazon EKS

Criado por Olawale Olaleye (AWS) e Shamanth Devagari (AWS)

Resumo

O EKS Auto Mode para Amazon Elastic Kubernetes Service (Amazon EKS) pode reduzir a sobrecarga operacional da execução de suas cargas de trabalho em clusters Kubernetes. Esse modo também AWS permite configurar e gerenciar a infraestrutura em seu nome. Ao habilitar o EKS Auto Mode em um cluster existente, você deve planejar cuidadosamente a migração das configurações do NGINX Ingress Controller. Isso ocorre porque a transferência direta de balanceadores de carga de rede não é possível.

Você pode usar uma estratégia de implantação azul/verde para migrar uma instância do NGINX Ingress Controller ao habilitar o EKS Auto Mode em um cluster Amazon EKS existente.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um cluster Amazon EKS executando o Kubernetes versão 1.29 ou posterior
- Complementos do Amazon EKS executando versões mínimas
- Versão mais recente de kubectl
- Uma instância existente do NGINX Ingress Controller
- (Opcional) Uma zona hospedada no Amazon Route 53 para mudança de tráfego baseada em DNS

Arquitetura

Uma implantação azul/verde é uma estratégia de implantação na qual você cria dois ambientes separados, mas idênticos. Implantações azul/verdes fornecem recursos de liberação e reversão com tempo de inatividade quase zero. A ideia fundamental é transferir o tráfego entre dois ambientes idênticos que estão executando versões diferentes do seu aplicativo.

A imagem a seguir mostra a migração de balanceadores de carga de rede de duas instâncias diferentes do controlador de entrada NGINX ao ativar o modo automático do EKS. Você usa uma implantação azul/verde para transferir o tráfego entre os dois balanceadores de carga de rede.

O namespace original é o namespace azul. É aqui que o serviço e a instância originais do NGINX Ingress Controller são executados, antes de você ativar o EKS Auto Mode. O serviço e a instância originais se conectam a um Network Load Balancer que tem um nome DNS configurado no Route 53. O AWS Load Balancer Controller implantou esse Network Load Balancer na nuvem privada virtual (VPC) de destino.

O diagrama mostra o seguinte fluxo de trabalho para configurar um ambiente para uma implantação azul/verde:

1. Instale e configure outra instância do NGINX Ingress Controller em um namespace diferente, um namespace verde.
2. No Route 53, configure um nome DNS para um novo Network Load Balancer.

Ferramentas

Serviços da AWS

- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- O Helm é um gerenciador de pacotes de código aberto para Kubernetes que ajuda você a instalar e gerenciar aplicativos em seu cluster Kubernetes.
- kubectl é uma interface de linha de comando que ajuda você na execução de comandos em clusters do Kubernetes.
- O NGINX Ingress Controller conecta aplicativos e serviços do Kubernetes com tratamento de solicitações, autenticação, recursos personalizados de autoatendimento e depuração.

Épicos

Revise o ambiente existente

Tarefa	Descrição	Habilidades necessárias

Confirme se a instância original do NGINX Ingress Controller está operacional.	Digite o comando a seguir para verificar se os recursos no `ingress-nginx` namespace estão operacionais. Se você implantou o NGINX Ingress Controller em outro namespace, atualize o nome do namespace neste comando.
	`kubectl get all -n ingress-nginx`
	Na saída, confirme se os pods do NGINX Ingress Controller estão em execução. Veja a seguir um exemplo de saída:
	`NAME READY STATUS RESTARTS AGE pod/ingress-nginx-admission-create-xqn9d 0/1 Completed 0 88m pod/ingress-nginx-admission-patch-lhk4j 0/1 Completed 1 88m pod/ingress-nginx-controller-68f68f859-xrz74 1/1 Running 2 (10m ago) 72m`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE service/ingress-nginx-controller LoadBalancer 10.100.67.255 k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com 80:30330/TCP,443:31462/TCP 88m service/ingress-nginx-controller-admission ClusterIP 10.100.201.176 <none> 443/TCP 88m NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/ingress-nginx-controller 1/1 1 1 88m NAME DESIRED CURRENT READY AGE	

Tarefa	Descrição	Habilidades necessárias
	`replicaset.apps/ingress-nginx-controller-68f68f859 1 1 1 72m replicaset.apps/ingress-nginx-controller-d8c96cf68 0 0 0 88m NAME STATUS COMPLETIONS DURATION AGE job.batch/ingress-nginx-admission-create Complete 1/1 4s 88m job.batch/ingress-nginx-admission-patch Complete 1/1 5s 88m`	

Implemente uma HTTPd carga de trabalho de amostra para usar o controlador de entrada NGINX

Tarefa	Descrição	Habilidades necessárias
Crie os recursos do Kubernetes.	Insira os comandos a seguir para criar um exemplo de implantação, serviço e entrada do Kubernetes: `kubectl create deployment demo --image=httpd --port=80`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`kubectl expose deployment demo`
	
	`kubectl create ingress demo --class=nginx \ --rule nginxautomode.local.dev/=demo:80`	

Tarefa	Descrição	Habilidades necessárias

Analise os recursos implantados.	Digite o comando a seguir para ver uma lista dos recursos implantados:
	`kubectl get all,ingress`
	Na saída, confirme se o HTTPd pod de amostra está em execução. Veja a seguir um exemplo de saída:
	`NAME READY STATUS RESTARTS AGE pod/demo-7d94f8cb4f-q68wc 1/1 Running 0 59m`
	`NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE service/demo ClusterIP 10.100.78.155 <none> 80/TCP 59m service/kubernetes ClusterIP 10.100.0.1 <none> 443/TCP 117m`
	`NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/demo 1/1 1 1 59m`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	NAME DESIRED CURRENT READY AGE replicaset.apps/ demo-7d94f8cb4f 1 1 1 59m NAME CLASS HOSTS ADDRESS PORTS AGE ingress.networ king.k8s.io/demo nginx nginxauto mode.local.dev k8s-ingre ssn-ingressn-abcde fg-12345.elb.eu-we st-1.amazonaws.com 80 56m	

Tarefa	Descrição	Habilidades necessárias

Confirme se o serviço está acessível.	Digite o comando a seguir para confirmar que o serviço pode ser acessado por meio do nome DNS do Network Load Balancer:
	`curl -H "Host: nginxautomode.local.dev" http://k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com`
	A seguir está a saída esperada:
	`<html><body><h1>It works!</h1></body></html>`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

(Opcional) Crie um registro DNS.	1. Siga as instruções em Criação de registros usando o console do Amazon Route 53 (documentação do Route 53) para criar um registro DNS para o domínio configurado.
	2. Digite o comando a seguir para confirmar que o serviço pode ser acessado por meio do nome de domínio configurado:
	`curl "http://nginxautomode.local.dev/?[1-5]"`
	A seguir está a saída esperada:
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
		DevOps engenheiro, AWS DevOps

Ative o modo automático do EKS no cluster existente

Tarefa	Descrição	Habilidades necessárias
Ative o modo automático do EKS.	Siga as instruções em Ativar o modo automático do EKS em um cluster existente (documentação do Amazon EKS).	AWS DevOps

Instale um novo controlador de entrada NGINX

Tarefa	Descrição	Habilidades necessárias

Configure uma nova instância do NGINX Ingress Controller.	1. Baixe o modelo deploy.yaml.
	2. Abra o modelo deploy.yaml no editor de sua preferência.
	3. Na `kind: Namespace` seção, insira um nome exclusivo para o namespace, como: `ingress-nginx-v2`
	`apiVersion: v1`
	`kind: Namespace`
	`metadata:`
	`labels:`
	`app.kubernetes.io/instance: ingress-nginx`
	`app.kubernetes.io/name: ingress-nginx`
	`name: ingress-nginx-v2`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	4. Para cada seção, atualize o `namespace` valor com o novo nome.
	5. Na seção `kind: Deployment` , faça o seguinte:
	a. Insira um valor exclusivo para`--controller-class` , com`k8s.io/ingress-nginx-v2` .
	b. Insira um valor exclusivo para`--ingress-class`, com`nginx-v2`.
	`apiVersion: apps/v1`
	`kind: Deployment`
	`  name: ingress-nginx-controller`
	`  namespace: ingress-nginx-v2`
	`...`
	`    spec:`
	`      containers:`
	`      - args:`
	`        - /nginx-ingress-controller`
	`        - --publish-service=$(POD_NAMESPACE)/ingress-nginx-controller`
	`        - --election-id=ingress-nginx-leader`
	`        - --controller-class=k8s.io/ingress-nginx-v2`
	`        - --ingress-class=nginx-v2`	

Tarefa	Descrição	Habilidades necessárias

	6. Na `kind: IngressClass` seção, insira os mesmos valores para `--controller-class` e `--ingress-class` que você usou na seção anterior:
	
	`apiVersion: networking.k8s.io/v1`
	`kind: IngressClass`
	`metadata:`
	`  labels:`
	`  app.kubernetes.io/component: controller`
	`  app.kubernetes.io/instance: ingress-nginx`
	`  app.kubernetes.io/name: ingress-nginx`
	`  app.kubernetes.io/part-of: ingress-nginx`
	`  app.kubernetes.io/version: 1.12.0`
	`  name: nginx-v2`
	`spec:`
	`  controller: k8s.io/ingress-nginx-v2`
	
	7. Na seção a seguir, adicione `loadBalancerClass: eks.amazonaws.com/nlb` para provisionar um Network Load Balancer	

Tarefa	Descrição	Habilidades necessárias

	para a instância do NGINX Ingress Controller:
	
	`apiVersion: v1`
	`kind: Service`
	`metadata:`
	`  name: ingress-nginx-controller`
	`  namespace: ingress-nginx-v2`
	`spec:`
	`...`
	`  selector:`
	`  app.kubernetes.io/component: controller`
	`  app.kubernetes.io/instance: ingress-nginx`
	`  app.kubernetes.io/name: ingress-nginx`
	`  type: LoadBalancer`
	`  loadBalancerClass: eks.amazonaws.com/nlb`
	
	8. Salve e feche o modelo deploy.yaml.	

Implante a nova instância do NGINX Instance Controller.	Digite o comando a seguir para aplicar o arquivo de manifesto modificado: `kubectl apply -f deploy.yaml`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Confirme a implantação bem-sucedida.	Insira o comando a seguir para verificar se os recursos no `ingress-nginx-v2` namespace estão operacionais:
	`kubectl get all -n ingress-nginx-v2`
	Na saída, confirme se os pods do NGINX Ingress Controller estão em execução. Veja a seguir um exemplo de saída:
	`NAME READY STATUS RESTARTS AGE pod/ingress-nginx-admission-create-7shrj 0/1 Completed 0 24s pod/ingress-nginx-admission-patch-vkxr5 0/1 Completed 1 24s pod/ingress-nginx-controller-757bfcbc6d-4fw52 1/1 Running 0 24s NAME TYPE CLUSTER-IP EXTERNAL-IP`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	PORT(S) AGE service/ingress- nginx-controller LoadBalancer 10.100.208.114 k8s-ingressn-ingre ssn-2e5e37fab6-848 337cd9c9d520f.elb.eu- west-1.amazonaws.com 80:31469/TCP,443:3 0658/TCP 24s service/ingress- nginx-controller- admission ClusterIP 10.100.150.114 <none> 443/TCP 24s NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/ ingress-nginx-co ntroller 1/1 1 1 24s NAME DESIRED CURRENT READY AGE replicaset.apps/ ingress-nginx-co ntroller-757bfcbc6d 1 1 1 24s	

Tarefa	Descrição	Habilidades necessárias
	`NAME  STATUS  COMPLETIONS  DURATION  AGE job.batch/ingress-nginx-admission-create  Complete  1/1  4s  24s job.batch/ingress-nginx-admission-patch  Complete  1/1  5s  24s`	
Crie uma nova entrada para a carga de HTTPd trabalho de amostra.	Insira o comando a seguir para criar uma nova entrada para a carga de HTTPd trabalho de amostra existente: `kubectl create ingress demo-new --class=nginx-v2 \  --rule nginxautomode.local.dev/=demo:80`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Confirme se a nova entrada funciona.	Digite o comando a seguir para confirmar se a nova entrada funciona:
	`curl -H "Host: nginxautomode.local.dev" k8s-ingressn-ingressn-2e5e37fab6-848337cd9c9d520f.elb.eu-west-1.amazonaws.com`
	A seguir está a saída esperada:
	`<html><body><h1>It works!</h1></body></html>`
		DevOps engenheiro

Substituir

Tarefa	Descrição	Habilidades necessárias
Vá para o novo namespace.	1. (Opcional) Siga as instruções em Edição de registros (documentação do Route 53) para atualizar o registro DNS. 2. Quando você confirmar que a nova instância do NGINX Ingress Controller está operando conforme o esperado, exclua a original. 3. Exclua o controlador de AWS balanceador de carga	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	autogerenciado. Para obter instruções, consulte Migrar aplicativos do ALB Ingress Controller obsoleto (documentação do Amazon EKS). 4. Esvazie os grupos de nós gerenciados. Para obter instruções, consulte Excluindo e drenando grupos de nós (document ação do eksctl).	

Tarefa	Descrição	Habilidades necessárias

Analise as duas entradas.	Insira o comando a seguir para analisar as duas entradas que foram criadas para a carga de HTTPd trabalho de amostra:
	`kubectl get ingress`
	Veja a seguir um exemplo de saída:
	`NAME  CLASS  HOSTS  ADDRESS  PORTS  AGE`
	`demo  nginx  nginxautomode.local.dev  k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com  80  95m`
	`demo-new  nginx-v2  nginxautomode.local.dev  k8s-ingressn-ingressn-2e5e37fab6-848337cd9c9d520f.elb.eu-west-1.amazonaws.com  80  33s`
		DevOps engenheiro

Recursos relacionados

- Ative o EKS Auto Mode em um cluster existente (documentação do Amazon EKS)
- Solucione problemas com balanceadores de carga criados pelo controlador de serviço Kubernetes no Amazon EKS (re:POST Knowledge Center)AWS
- Controlador de entrada NGINX (documentação do NGINX)

Migre suas cargas de trabalho de contêiner do Azure Red Hat OpenShift (ARO) para Serviço Red Hat OpenShift na AWS (ROSA)

Criado por Naveen Ramasamy (AWS), Gireesh Sreekantan (AWS) e Srikanth Rangavajhala (AWS)

Resumo

Esse padrão fornece step-by-step instruções para migrar cargas de trabalho de contêiner do Azure Red Hat OpenShift (ARO) para Serviço Red Hat OpenShift na AWS (ROSA). O ROSA é um serviço gerenciado de Kubernetes fornecido pela Red Hat em colaboração com o. AWS Ele ajuda você a implantar, gerenciar e escalar seus aplicativos em contêineres usando a plataforma Kubernetes e se beneficia da experiência da Red Hat em Kubernetes e na infraestrutura. Nuvem AWS

A migração de cargas de trabalho de contêineres do ARO, de outras nuvens ou do local para o ROSA envolve a transferência de aplicativos, configurações e dados de uma plataforma para outra. Esse padrão ajuda a garantir uma transição suave e, ao mesmo tempo, otimiza os Nuvem AWS serviços, a segurança e a eficiência de custos. Ele abrange dois métodos para migrar suas cargas de trabalho para clusters ROSA: CI/CD e Kit de ferramentas de migração para contêineres (MTC).

Esse padrão abrange os dois métodos. O método escolhido depende da complexidade e da certeza do seu processo de migração. Se você tem controle total sobre o estado do seu aplicativo e pode garantir uma configuração consistente por meio de um pipeline, recomendamos que você use o método CI/CD. No entanto, se o estado do seu aplicativo envolver incertezas, mudanças imprevistas ou um ecossistema complexo, recomendamos que você use o MTC como um caminho confiável e controlado para migrar seu aplicativo e seus dados para um novo cluster. Para uma comparação detalhada dos dois métodos, consulte a seção Informações adicionais.

Benefícios da migração para o ROSA:

- O ROSA se integra perfeitamente AWS como um serviço nativo. É facilmente acessível por meio do AWS Management Console e cobrado por meio de um único Conta da AWS. Ele oferece total compatibilidade com outros Serviços da AWS e fornece suporte colaborativo tanto da Red Hat AWS quanto da Red Hat.
- O ROSA oferece suporte a implantações híbridas e multinuvem. Ele permite que os aplicativos sejam executados de forma consistente em data centers locais e em vários ambientes de nuvem.
- O ROSA se beneficia do foco em segurança da Red Hat e fornece recursos como controle de acesso baseado em funções (RBAC), digitalização de imagens e avaliações de vulnerabilidade para garantir um ambiente de contêiner seguro.

- O ROSA foi projetado para escalar aplicativos com facilidade e fornecer opções de alta disponibilidade. Ele permite que os aplicativos cresçam conforme necessário, mantendo a confiabilidade.
- O ROSA automatiza e simplifica a implantação de um cluster Kubernetes em comparação com os métodos manuais de configuração e gerenciamento. Isso acelera o processo de desenvolvimento e implantação.
- O ROSA se beneficia dos Nuvem AWS serviços e fornece integração perfeita com AWS ofertas como serviços de banco de dados, soluções de armazenamento e serviços de segurança.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Permissões configuradas para Serviços da AWS isso que o ROSA usa para fornecer funcionalidade. Para obter mais informações, consulte Pré-requisitos na documentação do ROSA.
- ROSA ativado no console ROSA. Para obter instruções, consulte a documentação do ROSA.
- O cluster ROSA instalado e configurado. Para obter mais informações, consulte Introdução ao ROSA na documentação do ROSA. Para entender os diferentes métodos para configurar um cluster ROSA, consulte o guia de orientação AWS prescritiva sobre estratégias de implementação do ROSA.
- Conectividade de rede estabelecida a partir da rede local AWS por meio de AWS Direct Connect(preferencial) ou AWS Virtual Private Network (AWS VPN).
- Uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou outro servidor virtual para instalar ferramentas como `aws client` cliente OpenShift CLI `oc` (), cliente ROSA e binário Git.

Pré-requisitos adicionais para o método CI/CD:

- Acesso ao servidor Jenkins local com permissões para criar um novo pipeline, adicionar estágios, adicionar OpenShift clusters e realizar compilações.
- Acesso ao repositório Git onde o código-fonte do aplicativo é mantido, com permissões para criar uma nova ramificação do Git e realizar confirmações na nova ramificação.

Pré-requisitos adicionais para o método MTC:

- Um bucket do Amazon Simple Storage Service (Amazon S3), que será usado como repositório de replicação.
- Acesso administrativo ao cluster ARO de origem. Isso é necessário para configurar a conexão MTC.

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

O ROSA fornece três padrões de implantação de rede: público, privado AWS PrivateLinke. PrivateLinkpermite que as equipes de engenharia de confiabilidade de sites (SRE) da Red Hat gerenciem o cluster usando uma sub-rede privada conectada ao PrivateLink endpoint do cluster em uma VPC existente.

A escolha da PrivateLink opção fornece a configuração mais segura. Por esse motivo, nós o recomendamos para cargas de trabalho confidenciais ou requisitos rígidos de conformidade. Para obter informações sobre as opções de implantação de redes públicas e privadas, consulte a OpenShift documentação da Red Hat.

> **Important**
>
> Você pode criar um PrivateLink cluster somente no momento da instalação. Você não pode alterar um cluster para usar PrivateLink após a instalação.

O diagrama a seguir ilustra a PrivateLink arquitetura de um cluster ROSA usado AWS Direct Connect para se conectar aos ambientes locais e ARO.

AWS permissões para ROSA

Para obter AWS permissões para o ROSA, recomendamos que você use AWS Security Token Service (AWS STS) com tokens dinâmicos de curta duração. Esse método usa funções e políticas predefinidas com privilégios mínimos para conceder ao ROSA permissões mínimas para operar no e

oferece suporte à instalação Conta da AWS, ao plano de controle e à funcionalidade de computação do ROSA.

Reimplantação do pipeline de CI/CD

CI/CD pipeline redeployment is the recommended method for users who have a mature CI/CDoleoduto. Ao escolher essa opção, você pode usar qualquer estratégia de DevOps implantação para transferir gradualmente a carga do aplicativo para implantações no ROSA.

> **Note**
>
> Esse padrão pressupõe um caso de uso comum em que você tem um pipeline Git, JFrog Artifactory e Jenkins locais. Essa abordagem exige que você estabeleça conectividade de rede da sua rede local AWS até AWS Direct Connect a outra e que configure o cluster ROSA antes de seguir as instruções na seção Epics. Consulte a seção Pré-requisitos para obter detalhes.

O diagrama a seguir mostra o fluxo de trabalho desse método.

Método MTC

Você pode usar o Migration Toolkit for Containers (MTC) para migrar suas cargas de trabalho em contêineres entre diferentes ambientes do Kubernetes, como do ARO para o ROSA. O MTC simplifica o processo de migração automatizando várias tarefas importantes e fornecendo uma estrutura abrangente para gerenciar o ciclo de vida da migração.

O diagrama a seguir mostra o fluxo de trabalho desse método.

Ferramentas

Serviços da AWS

- AWS DataSyncé um serviço on-line de transferência e descoberta de dados que ajuda você a mover arquivos ou dados de objetos para, de e entre serviços AWS de armazenamento.
- AWS Direct Connectconecta sua rede interna a um AWS Direct Connect local por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais

diretamente para o público, Serviços da AWS ignorando os provedores de serviços de Internet em seu caminho de rede.

- AWS PrivateLinkajuda você a criar conexões unidirecionais e privadas de suas nuvens privadas virtuais (VPCs) para serviços fora da VPC.
- Serviço Red Hat OpenShift na AWS (ROSA) é um serviço gerenciado que ajuda OpenShift os usuários da Red Hat a criar, escalar e gerenciar aplicativos em contêineres. AWS
- AWS Security Token Service (AWS STS) ajuda você a solicitar credenciais temporárias com privilégios limitados para os usuários.

Outras ferramentas

- O kit de ferramentas de migração para contêineres (MTC) fornece um console e uma API para migrar aplicativos em contêineres do ARO para o ROSA.

Práticas recomendadas

- Para resiliência e se você tiver cargas de trabalho de conformidade de segurança, configure um cluster ROSA Multi-AZ que use. PrivateLink Para obter mais informações, consulte a documentação do ROSA.

> **Note**
>
> PrivateLink não pode ser configurado após a instalação.

- O bucket do S3 que você usa para o repositório de replicação não deve ser público. Use as políticas apropriadas do bucket do S3 para restringir o acesso.
- Se você escolher o método MTC, use a opção Stage migration para reduzir a janela de tempo de inatividade durante a transição.
- Revise suas cotas de serviço antes e depois de provisionar o cluster ROSA. Se necessário, solicite um aumento de cota de acordo com suas necessidades. Para obter mais informações, consulte a documentação do Servie Quotas.
- Revise as diretrizes de segurança do ROSA e implemente as melhores práticas de segurança.
- Recomendamos que você remova o administrador de cluster padrão após a instalação. Para obter mais informações, consulte a OpenShift documentação da Red Hat.

- Use o escalonamento automático do pool de máquinas para reduzir os nós de trabalho não utilizados no cluster ROSA e otimizar os custos. Para obter mais informações, consulte o Workshop ROSA.
- Use o serviço Red Hat Cost Management for OpenShift Container Platform para entender e monitorar melhor os custos de nuvens e containers. Para obter mais informações, consulte o Workshop ROSA.
- Monitore e audite os serviços e aplicativos da infraestrutura do cluster ROSA usando Serviços da AWS. Para obter mais informações, consulte o Workshop ROSA.

Épicos

Opção 1: usar um pipeline de CI/CD

Tarefa	Descrição	Habilidades necessárias
Adicione o novo cluster ROSA ao Jenkins.	1. No console Jenkins, escolha Gerenciar Jenkins, Configurar sistema. 2. Na página Gerenciar Jenkins, na seção OpenShift Plug-in, escolha Adicionar um novo cluster. 3. Forneça as informações necessárias, como nome do cluster, URL do servidor da API e informações de token, para autenticação com o ROSA.	Administrador da AWS, administrador de sistemas da AWS, AWS DevOps
Adicione o `oc` cliente aos seus nós do Jenkins.	1. No console Jenkins, escolha Manage Jenkins, Global Tool Configuration. 2. Na seção Ferramentas do OpenShift cliente, instale a versão do cliente OpenShift	Administrador da AWS, administrador de sistemas da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	CLI (`oc`) que é igual à versão do cluster ROSA.	
Crie uma nova ramificação do Git.	Crie uma nova ramificação no seu repositório Git para. `rosa-dev` Essa ramificação separa as alterações no código ou nos parâmetros de configuração do ROSA do seu pipeline existente.	AWS DevOps
Imagens de tags para ROSA.	Em seu estágio de construção, use uma tag diferente para identificar as imagens que são criadas a partir do pipeline ROSA.	Administrador da AWS, administrador de sistemas da AWS, AWS DevOps
Crie um pipeline.	Crie um novo pipeline do Jenkins que seja semelhante ao seu pipeline existente. Para esse pipeline, use a ramificação do `rosa-dev` Git que você criou anteriormente e certifique-se de incluir o checkout, a verificação de código e os estágios de construção do Git que sejam idênticos ao seu pipeline existente.	Administrador da AWS, administrador de sistemas da AWS, AWS DevOps
Adicione um estágio de implantação do ROSA.	No novo pipeline, adicione um estágio para implantação no cluster ROSA e faça referência ao cluster ROSA que você adicionou à configuração global do Jenkins.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Comece uma nova compilaçã o.	No Jenkins, selecione seu pipeline e escolha Criar agora, ou inicie uma nova compilação confirmando uma alteração na `rosa-dev` ramificação no Git.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS
Verificar a implantação.	Use o comando oc ou o console ROSA para verificar se o aplicativo foi implantado no cluster ROSA de destino.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS
Copie os dados para o cluster de destino.	Para cargas de trabalho com estado, copie os dados do cluster de origem para o cluster de destino usando AWS DataSync ou usando utilitários de código aberto, como rsync, ou você pode usar o método MTC. Para obter mais informações, consulte a documentação do AWS DataSync.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS
Testar seu aplicativo	1. Recupere a URL da rota do seu aplicativo usando o comando oc route ou o console ROSA. 2. Teste seu aplicativo usando o URL da rota.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Corte.	Se o teste for bem-sucedido, use a política apropriada do Amazon Route 53 para mover o tráfego do aplicativo hospedado no ARO para o aplicativo hospedado no ROSA. Quando você concluir essa etapa, a carga de trabalho do seu aplicativo fará a transição completa para o cluster ROSA.	Administrador da AWS, administrador de sistemas da AWS

Opção 2: usar o MTC

Tarefa	Descrição	Habilidades necessárias
Instale o operador MTC.	Instale o operador MTC nos clusters ARO e ROSA: 1. No console ARO ou ROSA, navegue até a OperatorHubpágina Operadores. 2. Na caixa Filtrar por palavra-chave, localize ou digite MTC. 3. Selecione o operador MTC para exibir informações adicionais. 4. Depois de ler as informações sobre o operador, escolha Instalar.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Configure o tráfego de rede para o repositório de replicação.	Se você estiver usando um servidor proxy, configure-o para permitir o tráfego de rede entre o repositório de replicação e os clusters. O repositório de replicação é um objeto de armazenamento intermediário que a MTC usa para migrar dados. Os clusters de origem e de destino devem ter acesso de rede ao repositório de replicação durante a migração.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS
Adicione o cluster de origem ao MTC.	No console web MTC, adicione o cluster de origem ARO.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS
Adicione o Amazon S3 como seu repositório de replicação.	No console web da MTC, adicione o bucket Amazon S3 (consulte Pré-requisitos) como repositório de replicação.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS
Crie um plano de migração.	No console web do MTC, crie um plano de migração e especifique o tipo de transferência de dados como Cópia. Isso instruirá a MTC a copiar os dados do cluster de origem (ARO) para o bucket S3 e do bucket para o cluster de destino (ROSA).	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Execute o plano de migração.	Execute o plano de migração usando a opção Stage ou Cutover: • Escolha Stage para copiar dados para o cluster de destino sem interromper seu aplicativo. Você pode executar migrações em vários estágios para copiar a maioria dos seus dados antes da migração por transição. Isso reduz a duração da migração por transição. • Escolha Cutover para interromper seu aplicativo no cluster de origem enquanto move os recursos para o cluster de destino. Para evitar a interrupção do aplicativo, você pode desmarcar a caixa de seleção Interromper transações no cluster de origem durante a migração.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS

Solução de problemas

Problema	Solução
Problemas de conectividade	Ao migrar suas cargas de trabalho de contêiner do ARO para o ROSA, você pode encontrar

Problema	Solução
	problemas de conectividade que devem ser resolvidos para garantir uma migração bem-sucedida. Para resolver esses problemas de conectividade (listados nesta tabela) durante a migração, um planejamento meticuloso, a coordenação com suas equipes de rede e segurança e testes completos são essenciais. A implementação de uma estratégia de migração gradual e a verificação da conectividade em cada etapa ajudarão a minimizar possíveis interrupções e garantir uma transição suave do ARO para o ROSA.
Diferenças de configuração de rede	ARO e ROSA podem ter variações em suas configurações de rede, como configurações de rede virtual (VNet), sub-redes e políticas de rede. Para uma comunicação adequada entre os serviços, certifique-se de que as configurações de rede estejam alinhadas entre as duas plataformas.
Grupo de segurança e regras de firewall	O ROSA e o ARO podem ter configurações de firewall e grupo de segurança padrão diferentes. Certifique-se de ajustar e atualizar essas regras para permitir que o tráfego necessário mantenha a conectividade entre contêineres e serviços durante a migração.
Alterações no endereço IP e no DNS	Quando você migra cargas de trabalho, os endereços IP e os nomes DNS podem mudar. Reconfigure aplicativos que dependem de nomes DNS estáticos IPs ou específicos.

Problema	Solução
Acesso ao serviço externo	Se seu aplicativo depender de serviços externos, como bancos de dados ou APIs, talvez seja necessário atualizar suas configurações de conexão para garantir que eles possam se comunicar com os novos serviços do ROSA.
Configuração do Azure Private Link	Se você usa o Azure Private Link ou serviços de endpoint privados no ARO, precisará configurar a funcionalidade equivalente no ROSA para garantir a conectividade privada entre os recursos.
AWS VPN ou AWS Direct Connect configuração	Se houver AWS Direct Connect conexões existentes AWS VPN ou entre sua rede local e o ARO, você precisará estabelecer conexões semelhantes com o ROSA para comunicação ininterrupta com seus recursos locais.
Configurações do balanceador de entrada e carga	As configurações para controladores de entrada e balanceadores de carga podem ser diferentes entre ARO e ROSA. Redefina essas configurações para manter o acesso externo aos seus serviços.
Tratamento de certificados e TLS	Se seus aplicativos usarem certificados SSL ou TLS, verifique se os certificados são válidos e configurados corretamente no ROSA.
Acesso ao registro de contêineres	Se seus contêineres estiverem hospedados em um registro de contêiner externo, configure a autenticação adequada e as permissões de acesso para o ROSA.

Problema	Solução
Monitorar e registrar em log	Atualize as configurações de monitoramento e registro para refletir a nova infraestrutura no ROSA para que você possa continuar monitorando a integridade e o desempenho de seus contêineres de forma eficaz.

Recursos relacionados

AWSreferências

- O que Serviço Red Hat OpenShift na AWSé (documentação ROSA)
- Comece com o ROSA (documentação do ROSA)
- Serviço Red Hat OpenShift na AWS estratégias de implementação (AWS orientação prescritiva)
- Serviço Red Hat OpenShift na AWS Agora GA (postagem AWS no blog)
- Workshop ROSA
- PERGUNTAS FREQUENTES SOBRE ROSA
- Perguntas frequentes sobre o workshop ROSA
- Preços do ROSA

OpenShift Documentação da Red Hat

- Instalando um cluster rapidamente em AWS
- Instalando um cluster AWS em uma rede restrita
- Instalando um cluster AWS em uma VPC existente
- Instalando um cluster na infraestrutura provisionada pelo usuário usando modelos AWS CloudFormation
- Instalando um cluster AWS em uma rede restrita com infraestrutura provisionada pelo usuário
- Instalando um cluster AWS com personalizações
- Começando com a OpenShift CLI

Mais informações

Escolha entre as opções de reimplantação do pipeline MTC e CI/CD

A migração de aplicativos de um OpenShift cluster para outro exige uma análise cuidadosa. Idealmente, você desejaria uma transição suave usando um pipeline de CI/CD para reimplantar o aplicativo e lidar com a migração de dados de volume persistente. No entanto, na prática, um aplicativo em execução em um cluster é suscetível a mudanças imprevistas ao longo do tempo. Essas alterações podem fazer com que o aplicativo se desvie gradualmente de seu estado original de implantação. A MTC oferece uma solução para cenários em que o conteúdo exato de um namespace é incerto e uma migração perfeita de todos os componentes do aplicativo para um novo cluster é importante.

Fazer a escolha certa exige avaliar seu cenário específico e pesar os benefícios de cada abordagem. Ao fazer isso, você pode garantir uma migração bem-sucedida e perfeita, alinhada às suas necessidades e prioridades. Aqui estão as diretrizes adicionais para escolher entre as duas opções.

Reimplantação do pipeline de CI/CD

O método de pipeline de CI/CD é a abordagem recomendada se seu aplicativo puder ser reimplantado com confiança usando um pipeline. Isso garante que a migração seja controlada, previsível e alinhada às suas práticas de implantação existentes. Ao escolher esse método, você pode usar estratégias de implantação azul/verde ou de implantação canária para transferir gradualmente a carga para implantações no ROSA. Para esse cenário, esse padrão pressupõe que o Jenkins esteja orquestrando implantações de aplicativos a partir do ambiente local.

Vantagens:

- Você não precisa de acesso administrativo ao cluster ARO de origem nem precisa implantar nenhum operador no cluster de origem ou de destino.
- Essa abordagem ajuda você a mudar o tráfego gradualmente usando uma DevOps estratégia.

Desvantagens:

- É preciso mais esforço para testar a funcionalidade do seu aplicativo.
- Se seu aplicativo contiver dados persistentes, ele precisará de etapas adicionais para copiar os dados usando AWS DataSync ou outras ferramentas.

Migração MTC

No mundo real, os aplicativos em execução podem passar por mudanças imprevistas que fazem com que eles se afastem da implantação inicial. Escolha a opção MTC quando não tiver certeza sobre o estado atual do seu aplicativo no cluster de origem. Por exemplo, se seu ecossistema de aplicativos abrange vários componentes, configurações e volumes de armazenamento de dados, recomendamos que você escolha o MTC para garantir uma migração completa que abranja o aplicativo e todo o seu ambiente.

Vantagens:

- O MTC fornece backup e restauração completos da carga de trabalho.
- Ele copiará os dados persistentes da origem para o destino durante a migração da carga de trabalho.
- Ele não requer acesso ao repositório do código-fonte.

Desvantagens:

- Você precisa de privilégios administrativos para instalar o operador MTC nos clusters de origem e destino.
- A DevOps equipe precisa de treinamento para usar a ferramenta MTC e realizar migrações.

Otimizar imagens do Docker geradas pelo AWS App2Container

Criado por Varun Sharma (AWS)

Resumo

O AWS App2Container é uma ferramenta de linha de comando que ajuda a transformar aplicativos existentes executados on-premises ou em máquinas virtuais em contêineres, sem a necessidade de alterações no código.

Com base no tipo de aplicativo, o App2Container adota uma abordagem conservadora para identificar dependências. No modo de processo, todos os arquivos que não são do sistema no servidor de aplicativos são incluídos na imagem do contêiner. Nesses casos, uma imagem bastante grande pode ser gerada.

Esse padrão fornece uma abordagem para otimizar as imagens de contêiner geradas pelo App2Container. É aplicável a todos os aplicativos Java descobertos pelo App2Container no modo de processo. O fluxo de trabalho definido no padrão foi projetado para ser executado no servidor do aplicativo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo Java em execução em um servidor de aplicativos em um servidor Linux
- App2Container instalado e configurado, com todos os pré-requisitos atendidos, no servidor Linux

Arquitetura

Pilha de tecnologia de origem

- Um aplicativo Java em execução em um servidor Linux

Pilha de tecnologias de destino

- Uma imagem do Docker gerada pelo App2Container

Fluxo da arquitetura de destino

1. Descubra os aplicativos em execução no servidor de aplicativos e analisar os aplicativos.
2. Colocar os aplicativos no contêiner.
3. Avalie o tamanho da imagem do Docker. Se a imagem estiver muito grande, prossiga para a etapa 4.
4. Use o script de shell (anexado) para identificar arquivos grandes.
5. Atualize as listas `appExcludedFiles` e `appSpecificFiles` no arquivo `analysis.jsone`.

Ferramentas

Ferramentas

- AWS App2Container: o AWS App2Container (A2C)é uma ferramenta da linha de comando que ajuda você a mover sem alterações (lift-and-shift) os aplicativos executados em seus datacenters on-premises ou em máquinas virtuais, para que eles sejam executados em contêineres gerenciados pelo Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS). .

Código

O script de shell `optimizeImage.sh` e um arquivo `analysis.json` de exemplo estão anexados.

O arquivo `optimizeImage.sh` é um script utilitário para revisar o conteúdo do arquivo gerado pelo App2Container,. `ContainerFiles.tar`. A análise identifica arquivos ou subdiretórios que são grandes e podem ser excluídos. O script é um invólucro para o seguinte comando tar.

```
tar -Ptvf <path>|tr -s ' '|cut -d ' ' -f3,6| awk '$2 ~/<filetype>$/'| awk '$2 ~/
^<toplevel>/'| cut -f1-<depth> -d'/'|awk '{ if ($1>= <size>) arr[$2]+=$1 } END { for
 (key in arr) { if(<verbose>) printf("%-50s\t%-50s\n", key, arr[key]) else printf("%s,
\n", key) } } '|sort -k2 -nr
```

No comando tar, o script usa os seguintes valores:

`path`	O caminho para `ContainerFiles.tar`
`filetype`	Tipo de arquivo a ser usado

`toplevel`	O diretório de nível superior a ser correspon dente
`depth`	A profundidade do caminho absoluto
`size`	O tamanho de cada arquivo

O script faz o seguinte:

1. Ele usa `tar -Ptvf` para listar os arquivos sem extraí-los.
2. Ele filtra os arquivos por tipo de arquivo, começando pelo diretório de nível superior.
3. Com base na profundidade, ele gera o caminho absoluto como um índice.
4. Com base no índice e nos armazenamentos, ele fornece o tamanho total do subdiretório.
5. Ele imprime o tamanho do subdiretório.

Você também pode substituir os valores manualmente no comando tar.

Épicos

Descubra, analise e coloque aplicativos em contêineres

Tarefa	Descrição	Habilidades necessárias
Descubra os aplicativos Java locais on-premises.	Para descobrir todos os aplicativos em execução no servidor de aplicativos, execute o comando a seguir. `sudo app2container inventory`	AWS DevOps
Analise os aplicativos descobertos.	Para analisar cada aplicativo usando o `application-id` que foi obtido no estágio de inventário, execute o comando a seguir.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`sudo app2container analyze --application-id <java-app-id>`	
Coloque os aplicativos analisados em contêineres.	Para armazenar um aplicativo em contêineres, execute o comando a seguir. `sudo app2container containerize --application-id <application-id>` O comando gera a imagem do Docker junto com um pacote tar no local do espaço de trabalho. Se a imagem do Docker for muito grande, vá para a próxima etapa.	AWS DevOps

Identifique appExcludedFiles e appSpecificFiles do arquivo tar extraído do App2Container

Tarefa	Descrição	Habilidades necessárias
Identifique o tamanho do arquivo tar dos artefatos.	Identifique o arquivo `ContainerFiles.tar` em `{workspace}/{java-app-id}/Artifacts`, onde `workspace` é o espaço de trabalho do App2Container e `java-app-id` é o ID do aplicativo.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Esse é o tamanho total do arquivo tar após a otimização.	

Liste os subdiretórios no diretório/e seus tamanhos.	Para identificar os tamanhos dos subdiretórios principais sob o diretório de nível superior `/`, execute o comando a seguir.
	
	`./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 1 -t / -s 1000000 -v`
	`/var`
	`554144711`
	`/usr`
	`2097300819`
	`/tmp`
	`18579660`
	`/root`
	`43645397`
	`/opt`
	`222320534`
	`/home`
	`65212518`
	`/etc`
	`11357677`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Identifique subdiretórios grandes no diretório /.	Para cada subdiretório principal listado no comando anterior, identifique os tamanhos de seus subdiretórios. Use `-d` para aumentar a profundidade e `-t` para indicar o diretório de nível superior. Por exemplo, use `/var` como diretório de nível superior. Sob `/var`, identifique todos os subdiretórios grandes e seus tamanhos. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 2 -t /var -s 1000000 -v` Repita esse processo para cada subdiretório listado na etapa anterior (por exemplo, `/usr`, `/tmp`, `/opt`, e/home).	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Analise a pasta grande em cada subdiretório sob o diretório /.	Para cada subdiretório listado na etapa anterior, identifique as pastas necessárias para executar o aplicativo.
	
	Por exemplo, usando os subdiretórios da etapa anterior, liste todos os subdiretórios no diretório `/var` e seus tamanhos. Identifiq ue todos os subdiretórios necessários ao aplicativo.
	
	`/var/tmp 237285851`
	`/var/lib 24489984`
	`/var/cache 237285851`
	
	Para excluir subdiretórios que não são necessários para o aplicativo, no arquivo `analysis.json` , adicione esses subdiretórios à seção `appExcludedFiles` sob `containerParameters` .
	
	Um arquivo `analysis. json` de exemplo está anexado.
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Identifique os arquivos necessários na lista AppExcludes.	Para cada subdiretório adicionado à lista AppExclud es, identifique todos os arquivos desse subdiretó rio que sejam exigidos pelo aplicativo. No arquivo analysis.json, adicione os arquivos ou subdiretó rios específicos na seção `appSpecificFiles` sob `containerParameters` . Por exemplo, se o diretório `/usr/lib` for adicionado à lista de exclusão, mas `/ usr/lib/jvm` for necessári o para o aplicativo, adicione `/usr/lib/jvm` à seção `appSpecificFiles` .	AWS DevOps

Extraia e coloque o aplicativo em contêineres novamente

Tarefa	Descrição	Habilidades necessárias
Coloque em contêineres o aplicativo analisado.	Para conteinerizar o aplicativo, execute o seguinte comando. `sudo app2container containerize --applica tion-id <application-id>` O comando gera a imagem do Docker junto com um pacote	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	tar no local do espaço de trabalho.	
Identifique o tamanho do arquivo tar dos artefatos.	Identifique o arquivo `ContainerFiles.tar` em `{workspace}/{java-app-id}/Artifacts` , onde `workspace` é o espaço de trabalho do App2Container e `java-app-id` é o ID do aplicativo. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Esse é o tamanho total do arquivo tar após a otimização.	AWS DevOps
Executar a imagem do Docker.	Para verificar se a imagem começa sem erros, execute a imagem do Docker localmente usando os comandos a seguir. Para identificar o `imageId` do contêiner, use `docker images |grep java-app-id` . Para executar o contêiner, use `docker run -d <image id>`.	AWS DevOps

Recursos relacionados

- O que é o App2Container?
- AWS App2Container – uma nova ferramenta de conteinerização para aplicativos Java e .NET (postagem no blog)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Coloque pods do Kubernetes no Amazon EKS usando afinidade de nó, taints e tolerâncias

Criado por Hitesh Parikh (AWS) e Raghu Bhamidimarri (AWS)

Resumo

Esse padrão demonstra o uso da afinidade de nós do Kubernetes, das taints dos nós e das tolerâncias de pods para programar intencionalmente pods de aplicativos em nós de processamento específicos em um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) na nuvem da Amazon Web Services (AWS).

Uma taint é uma propriedade do nó que permite que os nós rejeitem um conjunto de pods. Uma tolerância é uma propriedade do Pod que permite que o programador do Kubernetes agende pods em nós com taints correspondentes.

No entanto, as tolerâncias por si só não podem impedir que um programador coloque um pod em um nó de processamento que não tenha nenhum taint. Por exemplo, um pod de computação intensiva com uma tolerância pode ser programado involuntariamente em um nó sem taints de uso geral. Nesse cenário, a propriedade de afinidade do nó de um pod instrui o agendador a colocar o pod em um nó que atenda aos critérios de seleção do nó especificados na afinidade do nó.

Taints, tolerâncias e afinidade de nós juntos instruem o programador a programar pods de forma consistente nos nós com taints correspondentes e os rótulos de nós que correspondam aos critérios de seleção de nós de afinidade de nós especificados no pod.

Esse padrão fornece um exemplo de arquivo de manifesto de implantação do Kubernetes e as etapas para criar um cluster do EKS, implantar um aplicativo e validar o posicionamento do pod.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da AWS com credenciais configuradas para criar recursos em sua conta da AWS
- AWS Command Line Interface (AWS CLI)
- eksctl
- kubectl
- Docker foi instalado (para o sistema operacional que está sendo usado) e o mecanismo foi iniciado (para obter informações sobre os requisitos de licenciamento do Docker, consulte o site do Docker)

- Java versão 11 ou superior
- Um microsserviço Java executado em seu ambiente de desenvolvimento integrado (IDE) favorito; por exemplo, IntelliJ IDEA Community Edition ou Eclipse (se você não tiver um microsserviço Java, consulte o padrão Implantar um microsserviço Java de amostra no Amazon EKS e Microservices with Spring para obter ajuda na criação do microsserviço)

Limitações

- Esse padrão não fornece o código Java e pressupõe que você já esteja familiarizado com Java. Para criar um microsserviço Java básico, consulte Implantar um exemplo de microsserviço Java no Amazon EKS.
- As etapas deste artigo criam recursos da AWS que podem gerar custos. Certifique-se de limpar os recursos da AWS depois de concluir as etapas para implementar e validar o padrão.

Arquitetura

Pilha de tecnologias de destino

- Amazon EKS
- Java
- Docker
- Amazon Elastic Container Registry (Amazon ECR)

Arquitetura de destino

O diagrama da arquitetura da solução mostra o Amazon EKS com dois pods (implantação 1 e implantação 2) e dois grupos de nós (ng1 e ng2) com dois nós cada. Os Pods e os nós têm as seguintes propriedades.

	Implantação 1 pod	Implantação 2 Pod	Grupo de nós 1 (ng1)	Grupo de nós 2 (ng2)
Tolerância	chave: classified_workload, valor: true, efeito: NoSchedule	Nenhum		

	chave: machine_learning_workload, valor: verdadeiro, efeito: NoSchedule			
Afinidade de nós	chave: alpha.eksctl.io/nodegroup-name = ng1;	Nenhum	nodeGroups.name = ng1	
Taint			chave: classified_workload, valor: true, efeito: NoSchedule chave: machine_learning_workload, valor: verdadeiro, efeito: NoSchedule	Nenhum

1. O pod de implantação 1 tem tolerâncias e afinidade de nós definidas, o que instrui o programador do Kubernetes a colocar os pods de implantação nos nós do grupo de nós 1 (ng1).
2. O grupo de nós 2 (ng2) não tem um rótulo de nó que corresponda à expressão do seletor de nós de afinidade de nós para a implantação 1, portanto, os pods não serão programados nos nós ng2.
3. O pod de implantação 2 não tem nenhuma tolerância ou afinidade de nós definida no manifesto de implantação. O agendador rejeitará o agendamento de 2 pods de implantação no grupo de nós 1 devido às taints nos nós.
4. Em vez disso, os pods de implantação 2 serão colocados no grupo de nós 2, porque os nós não têm nenhum taint.

Esse padrão demonstra que, usando taints e tolerâncias, combinadas com a afinidade de nós, você pode controlar o posicionamento dos pods em conjuntos específicos de nós de trabalho.

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- eksctl é equivalente ao kubectl na AWS e ajuda na criação do EKS.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- kubectl é uma interface de linha de comando que ajuda você na execução de comandos em clusters do Kubernetes.

Épicos

Crie o cluster do EKS

Tarefa	Descrição	Habilidades necessárias

Crie o arquivo cluster.yaml.	Crie um arquivo denominado `cluster.yaml` com o seguinte código.
	`apiVersion: eksctl.io/v1alpha5`
	`kind: ClusterConfig`
		Proprietário do aplicativo, AWS DevOps, administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	``
	metadata:
	  name: eks-taint-demo
	  region: us-west-1
	
	# Unmanaged nodegroup
	s with and without
	 taints.
	nodeGroups:
	  - name: ng1
	  instanceType:
	 m5.xlarge
	  minSize: 2
	  maxSize: 3
	  taints:
	  - key: classifie
	d_workload
	  value: "true"
	  effect:
	 NoSchedule
	  - key: machine_l
	earning_workload
	  value: "true"
	  effect:
	 NoSchedule
	
	  - name: ng2
	  instanceType:
	 m5.xlarge
	  minSize: 2
	  maxSize: 3
	``	

Crie o cluster usando eksctl.	Execute o arquivo `cluster.yaml` para criar o cluster do EKS. A criação do cluster pode levar alguns minutos. ``` eksctl create cluster -f cluster.yaml ```	AWS DevOps, administrador de sistemas da AWS, desenvolvedor de aplicativos

Crie uma imagem e faça o upload para o Amazon ECR

Tarefa	Descrição	Habilidades necessárias
Crie um repositório privado do Amazon ECR.	Para criar um repositório do Amazon ECR, consulte Criação de um repositório privado. Observe o URI do repositório.	AWS DevOps, DevOps engenheiro, desenvolvedor de aplicativos

Crie o Dockerfile.	Se você já tiver um imagem de contêiner do Docker que deseja usar para testar o padrão, você pode ignorar esta etapa.
	
	Para criar um Dockerfile, use o seguinte trecho como referência. Se encontrar erros, consulte a seção Solução de problemas.
	
	`FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`
	
	`RUN apk add maven`
	`WORKDIR /code`
	
	`# Prepare by downloading dependencies`
	`ADD pom.xml /code/pom.xml`
	`RUN ["mvn", "dependency:resolve"]`
	`RUN ["mvn", "verify"]`
	
	`# Adding source, compile and package into a fat jar`
		AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`ADD src /code/src`
	`RUN ["mvn", "package"]`
	
	`EXPOSE 4567`
	`CMD ["java", "-jar",`
	` "target/eksExample`
	`-jar-with-dependen`
	`cies.jar"]`	

Crie o pom.xml e os arquivos de origem, crie e envie a imagem do Docker.	Para criar o arquivo `pom.xml` e o arquivo de origem Java, consulte Implantar um exemplo de microsserviço Java no Amazon EKS padrão. Use as instruções desse padrão para criar e enviar a imagem do Docker.	AWS DevOps, DevOps engenheiro, desenvolvedor de aplicativos

Implante no Amazon EKS

Tarefa	Descrição	Habilidades necessárias
Crie o arquivo deploymen t.yaml.	Para criar o arquivo `deployment.yaml` , use o código na seção Informações adicionais. No código, a chave para a afinidade de nós é qualquer rótulo que você cria ao criar grupos de nós. Esse padrão usa o rótulo padrão criado pelo eksctl. Para obter informações sobre a personali zação de rótulos, consulte	AWS DevOps, DevOps engenheiro, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Atribuição de pods a nós na documentação do Kubernetes. O valor da chave de afinidade do nó é o nome do grupo de nós que foi criado pelo `cluster.yaml` . Para obter a chave e o valor do taint, execute o seguinte comando. `kubectl get nodes -o json | jq '.items[] .spec.taints'` A imagem é o URI do repositório do Amazon ECR que você criou em uma etapa anterior.	
Implante o arquivo.	Para implantar no Amazon EKS, execute o seguinte comando. `kubectl apply -f deployment.yaml`	Desenvolvedor de aplicativos, DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Verifique a implantação.	1. Para verificar se os pods estão PRONTOS, execute o seguinte comando.
	`kubectl get pods -o wide`
	Se o POD estiver pronto, a saída será semelhante à saída a seguir, com o STATUS como Running.
	`NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES`
	`<pod_name> 1/1 Running 0 12d 192.168.18.50 ip-192-168-20-110.us-west-1.compute.internal <none> <none>`
	Anote o nome do pod e o nome do nó. Você pode ignorar a próxima etapa.
	2. (Opcional) Para obter mais detalhes sobre o pod e verificar as tolerâncias do pod, execute o seguinte comando.
		Desenvolvedor de aplicativos, DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`kubectl describe pod <pod_name>`
	
	Um exemplo da saída está na seção Informações adicionais.
	3. Para validar se o posicionamento do pod no nó está correto, execute o seguinte comando.
	
	`kubectl describe node <node name> | grep -A 1 "Taints"`
	
	Confirme se o taint no nó corresponde à tolerância e se o rótulo no nó corresponde à afinidade do nó definida em `deployment.yaml` .
	
	O pod com tolerâncias e afinidade de nós deve ser colocado em um nó com os taints correspondentes e os rótulos de afinidade do nó. O comando anterior fornece os taints no nó. Veja a seguir um exemplo de saída.
	
	`kubectl describe node ip-192-168-29-181.us-west-1.compute.`	

Tarefa	Descrição	Habilidades necessárias

	`internal | grep -A 1 "Taints"`
	`Taints:`
	` classifled_workloa`
	`d=true:NoSchedule`
	
	` machine_learning_w`
	`orkload=true:NoSch`
	`edule`
	
	Além disso, execute o seguinte comando para verificar se o nó no qual o pod está colocado tem um rótulo correspondente ao rótulo do nó de afinidade do nó.
	
	`kubectl get node <node name> --show-labels`
	
	4. Para verificar se o aplicativo está fazendo o que deveria fazer, verifique os registros do pod executando o seguinte comando.
	
	`kubectl logs -f <name-of-the-pod>`	

Tarefa	Descrição	Habilidades necessárias

Crie um segundo arquivo de implantação .yaml sem tolerância e afinidade do nós.	Essa etapa adicional é para validar que, quando nenhuma afinidade ou tolerância de nó for especificada no arquivo de manifesto de implantação, o pod resultante não será programado em um nó com taints. (Ele deve ser programado em um nó que não tenha nenhum taint). Use o código a seguir para criar um novo arquivo de implantação chamado `deploy_no_taint.yaml` .
	
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: microservice-deployment-non-tainted`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app.kubernetes.io/name: java-microservice-no-taint`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app.kubernetes.io/name: java-microservice-no-taint`
	`  spec:`
	`  containers:`
	`  - name: java-microservice-container-2`
		Desenvolvedor de aplicativos, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre>image:
	 <account_number>.d
	kr.ecr<region>.ama
	zonaws.com/<reposi
	tory_name>:latest
	ports:
	- container
	Port: 4567</pre>	

Implante a segunda implantação do arquivo deploy.yaml e valide o posicionamento do pod	1. Execute o comando a seguir.
	<pre>kubectl apply -f
	 deploy_no_taint.ya
	ml</pre>
	2. Depois que a implantação for bem-sucedida, execute os mesmos comandos que você executou anteriorm ente para verificar p posicionamento do pod em um grupo de nós sem taint.
	<pre>kubectl describe node
	 <node_name> | grep
	 "Taints"</pre>
	A saída deve ser a seguinte.
	<pre>Taints: <none></pre>
	Isso conclui o teste.
		Desenvolvedor de aplicativos, AWS DevOps, DevOps engenheiro

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Limpe os recursos.	Para evitar incorrer em cobranças da AWS por recursos que permanecem em execução, use o seguinte comando. `eksctl delete cluster --name <Name of the cluster> --region <region-code>`	AWS DevOps, desenvolvedor de aplicativos

Solução de problemas

Problema	Solução
Alguns desses comandos poderão não ser executados se o sistema usar a arquitetura arm64 (especialmente se você estiver executando isso em um Mac M1). A linha a seguir pode falhar. `FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`	Se você tiver erros ao executar o Dockerfile, substitua a linha `FROM` pela linha a seguir. `FROM bellsoft/liberica-openjdk-alpine-musl:17`

Recursos relacionados

- Implante um exemplo de microsserviço Java no Amazon EKS
- Crie um repositório privado do Amazon ECR
- Atribuição de pods a nós (documentação do Kubernetes)
- Taints e tolerâncias (documentação do Kubernetes)
- Amazon EKS

- Amazon ECR
- CLI da AWS
- Docker
- IntelliJ IDEA CE
- Eclipse

Mais informações

deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 1
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
              - matchExpressions:
                  - key: alpha.eksctl.io/nodegroup-name
                    operator: In
                    values:
                      - <node-group-name-from-cluster.yaml>
      tolerations: #only this pod has toleration and is viable to go to ng with taint
        - key: "<Taint key>" #classified_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
        - key: "<Taint key>" #machine_learning_workload in our case
          operator: Equal
          value: "<Taint value>" #true
```

```
          effect: "NoSchedule"
      containers:
        - name: java-microservice-container
          image: <account_number>.dkr.ecr<region>.amazonaws.com/
<repository_name>:latest
          ports:
            - containerPort: 4567
```

descreva o exemplo de saída do pod

```
Name:         microservice-deployment-in-tainted-nodes-5684cc495b-vpcfx
Namespace:    default
Priority:     0
Node:         ip-192-168-29-181.us-west-1.compute.internal/192.168.29.181
Start Time:   Wed, 14 Sep 2022 11:06:47 -0400
Labels:       app.kubernetes.io/name=java-microservice-taint
              pod-template-hash=5684cc495b
Annotations:  kubernetes.io/psp: eks.privileged
Status:       Running
IP:           192.168.13.44
IPs:
  IP:           192.168.13.44
Controlled By:  ReplicaSet/microservice-deployment-in-tainted-nodes-5684cc495b
Containers:
  java-microservice-container-1:
    Container ID:
 docker://5c158df8cc160de8f57f62f3ee16b12725a87510a809d90a1fb9e5d873c320a4
    Image:          934188034500.dkr.ecr.us-east-1.amazonaws.com/java-eks-apg
    Image ID:       docker-pullable://934188034500.dkr.ecr.us-east-1.amazonaws.com/
java-eks-apg@sha256:d223924aca8315aab20d54eddf3443929eba511b6433017474d01b63a4114835
    Port:           4567/TCP
    Host Port:      0/TCP
    State:          Running
      Started:      Wed, 14 Sep 2022 11:07:02 -0400
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-ddvvw (ro)
Conditions:
  Type              Status
  Initialized       True
  Ready             True
```

```
  ContainersReady   True
  PodScheduled      True
Volumes:
  kube-api-access-ddvvw:
    Type:                     Projected (a volume that contains injected data from
 multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 classifled_workload=true:NoSchedule
                             machine_learning_workload=true:NoSchedule
                             node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for
 300s
Events:                      <none>
```

Replique imagens filtradas de contêineres do Amazon ECR entre contas ou regiões

Criado por Abdal Garuba (AWS)

Resumo

O Amazon Elastic Container Registry (Amazon ECR) pode replicar todas as imagens de contêineres em um repositório de imagens nas regiões da Amazon Web Services (AWS) e nas contas da AWS de forma nativa, usando os atributos de replicação entre regiões e entre contas. (Para obter mais informações, consulte a postagem no blog da AWS: A replicação entre regiões no Amazon ECR chegou.) No entanto, não há como filtrar as imagens que são copiadas nas contas ou regiões da AWS com base em nenhum critério.

Esse padrão descreve como replicar imagens de contêineres que são armazenadas no Amazon ECR em todas as contas e regiões da AWS, com base em padrões de tag de imagem. O padrão usa o Amazon CloudWatch Events para ouvir eventos push para imagens que têm uma tag personalizada predefinida. Um evento push inicia um CodeBuild projeto da AWS e passa os detalhes da imagem para ele. O CodeBuild projeto copia as imagens do registro de origem do Amazon ECR para o registro de destino com base nos detalhes fornecidos.

Esse padrão copia imagens que têm tags específicas em todas as contas. Por exemplo, você pode usar esse padrão para copiar somente imagens seguras e prontas para produção na conta de produção da AWS. Na conta de desenvolvimento, depois que as imagens forem completamente testadas, você poderá adicionar uma tag predefinida às imagens seguras e usar as etapas desse padrão para copiar as imagens marcadas para a conta de produção.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa AWS para registros de origem e destino do Amazon ECR
- Permissões administrativas para as ferramentas usadas nesse padrão
- Docker instalado em sua máquina local para teste
- AWS Command Line Interface (AWS CLI)), para autenticação no Amazon ECR

Limitações

- Esse padrão observa os eventos push do registro de origem em apenas uma região da AWS. Você pode implantar esse padrão em outras regiões para observar os registros nessas regiões.
- Nesse padrão, uma regra da Amazon CloudWatch Events escuta um único padrão de tag de imagem. Se quiser verificar vários padrões, você pode adicionar eventos para ouvir padrões adicionais de tags de imagem.

Arquitetura

Arquitetura de destino

Automação e escala

Esse padrão pode ser automatizado com um script de infraestrutura como código (IaC) e implantado em grande escala. Para usar os CloudFormation modelos da AWS para implantar esse padrão, baixe o anexo e siga as instruções na seção Informações adicionais.

Você pode direcionar vários CloudWatch eventos da Amazon Events (com diferentes padrões de eventos personalizados) para o mesmo CodeBuild projeto da AWS para replicar vários padrões de tag de imagem, mas precisará atualizar a validação secundária no `buildspec.yaml` arquivo (que está incluído no anexo e na seção Ferramentas) da seguinte forma para suportar vários padrões.

```
...
if [[ ${IMAGE_TAG} != release-* ]]; then
...
```

Ferramentas

Serviço da Amazon

- IAM: o AWS Identity and Access Management (IAM) permite que você gerencie o acesso aos serviços e recursos da AWS com segurança. Nesse padrão, você precisaria criar a função do IAM entre contas que a AWS CodeBuild assumirá ao enviar imagens de contêiner para o registro de destino.
- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um registro de contêiner do Docker totalmente gerenciado que facilita o armazenamento, o gerenciamento e a implantação de imagens de contêiner do Docker. As ações de envio de imagens para o registro de origem

enviam detalhes do evento do sistema para o barramento de eventos que é coletado pela Amazon CloudWatch Events.

- AWS CodeBuild — CodeBuild A AWS é um serviço de integração contínua totalmente gerenciado que fornece poder computacional para realizar trabalhos como compilar código-fonte, executar testes e produzir artefatos prontos para serem implantados. Esse padrão usa CodeBuild a AWS para realizar a ação de cópia do registro de origem do Amazon ECR para o registro de destino.
- CloudWatch Eventos — A Amazon CloudWatch Events fornece um fluxo de eventos do sistema que descrevem as mudanças nos recursos da AWS. Esse padrão usa regras para combinar as ações push do Amazon ECR com um padrão de tag de imagem específico.

Ferramentas

- Docker CLI: o Docker é uma ferramenta que facilita a criação e o gerenciamento de contêineres. Os contêineres empacotam um aplicativo e todas as suas dependências em uma unidade ou pacote que pode ser facilmente implantado em qualquer plataforma que ofereça suporte ao runtime do contêiner.

Código

É possível implementar esse padrão de duas maneiras:

- Configuração automatizada: implante os dois CloudFormation modelos da AWS fornecidos no anexo. Para obter instruções, consulte a seção Informações adicionais.
- Configuração manual: siga as etapas na seção Épicos.

Exemplo: buildspec.yaml

Se você estiver usando os CloudFormation modelos fornecidos com esse padrão, o `buildspec.yaml` arquivo será incluído nos CodeBuild recursos.

```
version: 0.2
env:
  shell: bash
phases:
  install:
    commands:
      - export CURRENT_ACCOUNT=$(echo ${CODEBUILD_BUILD_ARN} | cut -d':' -f5)
```

```
        - export CURRENT_ECR_REGISTRY=${CURRENT_ACCOUNT}.dkr.ecr.
${AWS_REGION}.amazonaws.com
        - export DESTINATION_ECR_REGISTRY=${DESTINATION_ACCOUNT}.dkr.ecr.
${DESTINATION_REGION}.amazonaws.com
    pre_build:
      on-failure: ABORT
      commands:
        - echo "Validating Image Tag ${IMAGE_TAG}"
        - |
          if [[ ${IMAGE_TAG} != release-* ]]; then
            aws codebuild stop-build --id ${CODEBUILD_BUILD_ID}
            sleep 60
            exit 1
          fi
        - aws ecr get-login-password --region ${AWS_REGION} | docker login -u AWS --
password-stdin ${CURRENT_ECR_REGISTRY}
        - docker pull ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
    build:
      commands:
        - echo "Assume cross-account role"
        - CREDENTIALS=$(aws sts assume-role --role-arn ${CROSS_ACCOUNT_ROLE_ARN} --
role-session-name Rolesession)
        - export AWS_DEFAULT_REGION=${DESTINATON_REGION}
        - export AWS_ACCESS_KEY_ID=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.AccessKeyId')
        - export AWS_SECRET_ACCESS_KEY=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.SecretAccessKey')
        - export AWS_SESSION_TOKEN=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.SessionToken')
        - echo "Logging into cross-account registry"
        - aws ecr get-login-password --region ${DESTINATION_REGION} | docker login -u
 AWS --password-stdin ${DESTINATION_ECR_REGISTRY}
        - echo "Check if Destination Repository exists, else create"
        - |
          aws ecr describe-repositories --repository-names ${REPO_NAME} --region
 ${DESTINATION_REGION} \
          || aws ecr create-repository --repository-name ${REPO_NAME} --region
 ${DESTINATION_REGION}
        - echo "retag image and push to destination"
        - docker tag ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
 ${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
        - docker push ${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
```

Épicos

Criar perfis do IAM.

Tarefa	Descrição	Habilidades necessárias

Crie uma função de CloudWatch eventos.	Na conta de origem da AWS, crie uma função do IAM para a Amazon CloudWatch Events assumir. A função deve ter permissões para iniciar um CodeBuild projeto da AWS.
	
	Para criar a função usando a AWS CLI, siga as instruções na documentação do IAM.
	
	Exemplo de política de confiança do `trustpolicy.json` .
	
	`{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Principal": {"Service": "events.amazonaws.com"}, "Action": "sts:AssumeRole" } }`
	
	Exemplo de política de permissões (`permissionpolicy.json`)
	
	`{`
		Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administrador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	  "Version": "2012-10-17",
	  "Statement": {
	  "Effect": "Allow",
	  "Action": "codebuild:StartBuild",
	  "Resource": "<CodeBuild Project ARN>"
	  }
	}</pre>	

Tarefa	Descrição	Habilidades necessárias
Crie uma CodeBuild função.	Crie uma função do IAM para CodeBuild a AWS assumir, seguindo as instruções na documentação do IAM. O perfil também deve ter as seguintes permissões: • Permissão para assumir a função de destino entre contas • Permissão para criar grupos e fluxos de log e colocar eventos de log • Permissões somente de leitura para todos os repositórios do Amazon ECR, adicionando a política EC2 ContainerRegistryR eadOnly gerenciada da Amazon à função • Permissão para parar CodeBuild Exemplo de política de confiança do `trustpoli cy.json` . `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administr ador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	<pre>"Service": "codebuild.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre> Exemplo de política de permissões (`permissionpolicy.json`) <pre>{ "Version": "2012-10-17", "Statement": [{ "Action": ["codebuild:StartBuild", "codebuild:StopBuild", "codebuild:Get*", "codebuild:List*", "codebuild:BatchGet*"], "Resource": "*", "Effect": "Allow" }, { "Action": [</pre>	

Tarefa	Descrição	Habilidades necessárias
	"logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"], "Resource": "*", "Effect": "Allow" }, { "Action": "sts:AssumeRole", "Resource": "<ARN of destination role>", "Effect": "Allow", "Sid": "AssumeCrossAccountArn" }] } Anexe a política gerenciada `AmazonEC2ContainerRegistryReadOnly` ao comando da CLI da seguinte forma: `~$ aws iam attach-role-policy \ --policy-arn arn:aws:iam::aws:policy/Ama`	

Tarefa	Descrição	Habilidades necessárias
	zonEC2ContainerReg istryReadOnly \ --role-name <name of CodeBuild Role>	

Tarefa	Descrição	Habilidades necessárias
Criar uma função de conta cruzada.	Na conta da AWS de destino, crie uma função do IAM para a CodeBuild função da AWS para a conta de origem assumir. A função entre contas deve permitir que imagens de contêiner criem um novo repositório e façam upload de imagens de contêiner para o Amazon ECR. Para criar o perfil do IAM usando a AWS CLI, siga as instruções na documentação do IAM. Para permitir o CodeBuild projeto da AWS da etapa anterior, use a seguinte política de confiança: `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Principal": { "AWS": "<ARN of source codebuild role>" }, "Action": "sts:AssumeRole" } }`	Administrador da AWS, AWS DevOps, administrador de nuvem, arquiteto de nuvem, DevOps engenheiro, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	Para permitir que o CodeBuild projeto da AWS da etapa anterior salve imagens no registro de destino, use a seguinte política de permissão : `{ "Version": "2012-10-17", "Statement": [ { "Action": [ "ecr:GetDownloadUrlForLayer", "ecr:BatchCheckLayerAvailability", "ecr:PutImage", "ecr:InitiateLayerUpload", "ecr:UploadLayerPart", "ecr:CompleteLayerUpload", "ecr:GetRepositoryPolicy", "ecr:DescribeRepositories", "ecr:GetAuthorizationToken",`	

Tarefa	Descrição	Habilidades necessárias
	"ecr:CreateRepository"], "Resource": "*", "Effect": "Allow" }] }	

Crie o CodeBuild projeto

Tarefa	Descrição	Habilidades necessárias
Crie um CodeBuild projeto.	Crie um CodeBuild projeto da AWS na conta de origem seguindo as instruções na CodeBuild documentação da AWS. O projeto deve estar na mesma região que o registro de origem. Configure o projeto da seguinte forma: • Tipo de ambiente: `LINUX CONTAINER` • Perfil de `CodeBuild Role` serviço • Modo privilegiado: `true` • Imagem do ambiente: `aws/codebuild/standard:x.x` (use a imagem mais recente disponível)	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administrador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	• Variáveis de ambiente:
	  • `CROSS_ACCOUNT_ROLE_ARN` : o nome do recurso da Amazon (ARN) da conta do usuário.
	  • `DESTINATION_REGION` : o nome da região de várias contas
	  • `DESTINATION_ACCOUNT` : o número da conta de destino
	• Especificações de compilação: use o `buildspec.yaml` arquivo listado na seção Ferramentas.	

Criar evento

Tarefa	Descrição	Habilidades necessárias
Criar uma regra de evento.	Como o padrão usa o recurso de filtragem de conteúdo, você precisa criar o evento usando a Amazon EventBridge. Crie o evento e o alvo seguindo as instruções na EventBridge documentação, com algumas modificações: • Em Definir padrão, escolha Padrão de evento e escolha Padrão personalizado.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administrador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	• Copie o seguinte código de amostra de padrão de eventos personalizados na caixa de texto fornecida:
	
	`{ "source": ["aws.ecr "], "detail-type": ["ECR Image Action"], "detail": { "action-type": ["PUSH"], "result": ["SUCCESS"], "image-ta g": [{ "prefix": "release-"}] } }`
	
	• Em Selecionar destinos, escolha o CodeBuild projeto da AWS e cole o ARN do CodeBuild projeto da AWS que você criou no épico anterior.
	• Em CConfigurar entrada, selecione Transformador de entrada.
	• Na caixa de texto Caminho de entrada, cole:
	
	`{"IMAGE_TAG":"$.de tail.image-tag","R EPO_NAME":"$.detai`	

Tarefa	Descrição	Habilidades necessárias

	<pre>l.repository-name"
	}</pre>
	• Na caixa de texto Modelo de entrada, cole:
	<pre>{"environmentVariablesOverride":
	[{"name":
	"IMAGE_TAG",
	"value":<IMAGE_TAG>},{"name":"REPO_NAME","value":<REPO_NAME>}]}</pre>
	• Escolha Usar papel existente e escolha o nome do papel de CloudWatch Eventos que você criou anteriormente no épico Create IAM roles.	

Validar

Tarefa	Descrição	Habilidades necessárias
Autenticar com o Amazon ECR	Autentique-se nos registros de origem e destino seguindo as etapas na documentação do Amazon ECR.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administrador de nuvem, DevOps engenheiro, arquiteto de nuvem
Replicação de imagem de teste.	Em sua conta de origem, envie uma imagem de contêiner para um repositório de origem novo ou existente	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administr

Tarefa	Descrição	Habilidades necessárias
	do Amazon ECR com uma tag de imagem prefixada com `release-`. Para enviar a imagem, siga as etapas na documentação do Amazon ECR. Você pode monitorar o progresso do CodeBuild projeto no CodeBuild console. Depois que o CodeBuild projeto for concluído com sucesso, faça login na conta da AWS de destino, abra o console do Amazon ECR e confirme que a imagem existe no registro do Amazon ECR de destino.	ador de nuvem, arquiteto de nuvem, DevOps engenheiro
Exclusão de imagem de teste.	Em sua conta de origem, envie uma imagem de contêiner para um repositório de origem novo ou existente do Amazon ECR com uma tag de imagem que não tenha o prefixo personalizado. Confirme se o CodeBuild projeto não foi iniciado e se nenhuma imagem de contêiner aparece no registro de destino.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administr ador de nuvem, arquiteto de nuvem, DevOps engenheiro

Recursos relacionados

- Começando com CodeBuild
- Começando com a Amazon EventBridge
- Filtragem baseada em conteúdo nos padrões de eventos da Amazon EventBridge
- Delegar acesso entre contas da AWS usando perfis do IAM
- Replicação de imagem privada

Mais informações

Para implantar automaticamente os recursos desse padrão, siga estas etapas:

1. Baixe o anexo e extraia os dois CloudFormation modelos: `part-1-copy-tagged-images.yaml` `part-2-destination-account-role.yaml` e.
2. Faça login no CloudFormation console da AWS e implante `part-1-copy-tagged-images.yaml` na mesma conta e região da AWS dos registros de origem do Amazon ECR. Atualizar parâmetros conforme necessário: O modelo define os seguintes recursos:
   - Função do Amazon CloudWatch Events IAM
   - Função CodeBuild do IAM do projeto AWS
   - CodeBuild Projeto AWS
   - Regra de CloudWatch eventos da AWS
3. Anote o valor de `SourceRoleName` na guia Saídas. Você precisará desse valor na próxima etapa.
4. Implante o segundo CloudFormation modelo,`part-2-destination-account-role.yaml`, na conta da AWS para a qual você deseja copiar as imagens do contêiner Amazon ECR. Atualizar parâmetros conforme necessário: Para o parâmetro `SourceRoleName`, especifique o valor da etapa 3. Esse modelo implanta o perfil do IAM entre contas.
5. Valide a replicação e exclusão de imagens, conforme descrito na última etapa da seção Épicos.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Alternar as credenciais do banco de dados sem reiniciar os contêineres

Criado por Josh Joy (AWS)

Resumo

Na Nuvem da Amazon Web Services (AWS), você pode usar o AWS Secrets Manager para alternar, gerenciar e recuperar credenciais de banco de dados durante o ciclo de vida deles. Usuários e aplicativos recuperam segredos com uma chamada para a API do Secrets Manager, removendo a necessidade de codificar informações confidenciais.

Se você estiver usando contêineres para workload de microsserviços, poderá armazenar credenciais com segurança no AWS Secrets Manager. Para separar a configuração do código, essas credenciais geralmente são injetadas no contêiner. No entanto, é importante alternar suas credenciais periodicamente e automaticamente. Também é importante oferecer suporte à capacidade de atualizar as credenciais após a revogação. Ao mesmo tempo, os aplicativos exigem a capacidade de alternar as credenciais e, ao mesmo tempo, reduzir qualquer impacto potencial na disponibilidade posterior.

Esse padrão descreve como alternar seus segredos protegidos com o AWS Secrets Manager em seus contêineres sem exigir que eles reiniciem. Além disso, esse padrão reduz o número de pesquisas de credenciais no Secrets Manager usando o componente de cache do lado do cliente do Secrets Manager. Ao usar o componente de cache do lado do cliente para atualizar as credenciais no aplicativo, o contêiner não precisa ser reiniciado para obter uma credencial alternada.

Esta abordagem funciona para Amazon Elastic Kubernetes Service (Amazon EKS) e Amazon Elastic Container Service (Amazon ECS).

Dois cenários são abordados. No cenário de usuário único, a credencial do banco de dados é atualizada na rotação secreta, detectando a credencial expirada. O cache de credenciais é instruído a atualizar o segredo e, em seguida, o aplicativo restabelece a conexão com o banco de dados. O componente de cache do lado do cliente armazena em cache a credencial dentro do aplicativo e ajuda a evitar o contato com o Secrets Manager para cada consulta de credencial. A credencial é alternada dentro do aplicativo sem a necessidade de forçar a atualização da credencial ao reiniciar o contêiner.

O segundo cenário alterna o segredo ao alternar entre dois usuários. Ter dois usuários ativos reduz a possibilidade de tempo de inatividade, pois as credenciais de um usuário estão sempre ativas. A rotação de credenciais de dois usuários é útil quando você tem uma grande implantação com clusters nos quais pode haver um pequeno atraso na propagação das atualizações de credenciais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo executado em um contêiner no Amazon EKS ou no Amazon ECS.
- Credenciais armazenadas no Secrets Manager, com a alternância ativada.
- Um segundo conjunto de credenciais armazenado no Secrets Manager, se estiver implantando a solução para dois usuários. Exemplos de código podem ser encontrados no GitHub repo aws-secrets-manager-rotation-lambdas.
- Um banco de dados Amazon Aurora.

Limitações

- Este exemplo é voltado para aplicativos em Python. Para aplicativos Java, você pode usar o Java client-side caching component ou o JDBC client-side caching library para o Secrets Manager.

Arquitetura

Arquitetura de destino

Cenário 1: alternância de uma credencial para um único usuário

No primeiro cenário, uma única credencial de banco de dados é alternada periodicamente pelo Secrets Manager. O contêiner do aplicativo é executado no Fargate. Quando a primeira conexão com o banco de dados é estabelecida, o contêiner do aplicativo busca a credencial do banco de dados para o Aurora. O componente de cache do Secrets Manager então armazena em cache a credencial para o estabelecimento futuro da conexão. Quando o período de rotação termina, a credencial expira e o banco de dados retorna um erro de autenticação. O aplicativo então busca a credencial alternada, invalida o cache e atualiza o cache de credenciais por meio do componente de cache do lado do cliente do Secrets Manager.

Nesse cenário, pode haver uma interrupção mínima enquanto a credencial está sendo alternada e as conexões obsoletas estão usando a credencial desatualizada. Essa preocupação pode ser resolvida usando o cenário de dois usuários.

Cenário 2: alternância de credenciais para dois usuários

No segundo cenário, duas credenciais de usuário do banco de dados (Alice e Bob) são alternadas periodicamente pelo Secrets Manager. O contêiner do aplicativo é executado em um cluster Fargate. Quando a primeira conexão com o banco de dados é estabelecida, o contêiner do aplicativo busca a credencial do banco de dados Aurora para o primeiro usuário (Alice). O componente de cache do Secrets Manager então armazena em cache a credencial para o estabelecimento futuro da conexão.

Embora existam dois usuários e credenciais, uma única credencial ativa é gerenciada pelo Secrets Manager. Nesse caso, o componente de cache expira periodicamente e busca a credencial mais recente. Se o período de alternância do Secrets Manager for maior que o tempo limite do cache, o componente de cache pega a credencial alternada para o segundo usuário (Bob). Por exemplo, se a expiração do cache for medida em minutos e o período de alternância for medido em dias, o componente de cache buscará a nova credencial como parte da atualização periódica do cache. Dessa forma, o tempo de inatividade é minimizado porque a credencial de cada usuário está ativa para uma alternância do Secrets Manager.

Automação e escala

Você pode usar CloudFormation a AWS para implantar esse padrão usando a infraestrutura como código. Isso compila e cria o contêiner do aplicativo, cria a tarefa do Fargate, implanta o contêiner no Fargate e configura o Secrets Manager com o Aurora. Para obter instruções de step-by-step implantação, consulte o arquivo readme.

Ferramentas

Ferramentas

- O AWS Secrets Manager permite a substituição de credenciais codificadas no seu código, incluindo senhas, por uma chamada de API para o Secrets Manager para recuperar o segredo. Como o Secrets Manager pode alternar automaticamente o segredo de acordo com uma agenda, você pode substituir segredos de longo prazo por segredos de curto prazo, reduzindo o risco de comprometimento.
- O Docker ajuda os desenvolvedores a empacotar, enviar e executar qualquer aplicativo como um contêiner leve, portátil e autossuficiente.

Código

Código em Python de exemplo

Esse padrão usa o componente de cache do lado do cliente Python para o Secrets Manager para recuperar as credenciais de autenticação ao estabelecer a conexão com o banco de dados. O componente de cache do lado do cliente ajuda a evitar o contato com o Secrets Manager todas as vezes.

Agora, quando o período de rotação terminar, a credencial em cache expirará e a conexão com o banco de dados resultará em um erro de autenticação. Para o MySQL, o código de erro de autenticação é 1045. Este exemplo usa o Amazon Aurora para MySQL, embora você possa usar outro mecanismo, como o PostgreSQL. Após o erro de autenticação, o código de tratamento da exceção de conexão do banco de dados detecta o erro. Em seguida, informa-se o componente de cache do lado do cliente do Secrets Manager para atualizar o segredo e, em seguida, reautenticar e restabelecer a conexão com o banco de dados. Se você estiver usando o PostgreSQL ou outro mecanismo, deverá procurar o código de erro de autenticação correspondente.

O aplicativo de contêiner agora pode atualizar a senha do banco de dados com a senha alternada sem reiniciar o contêiner.

Coloque o código a seguir no código do seu aplicativo que manipula as conexões do banco de dados. Este exemplo usa o Django e subclassifica o backend do banco de dados com um invólucro de banco de dados para conexões. Se você estiver usando uma linguagem de programação ou biblioteca de conexão de banco de dados diferente, consulte sua biblioteca de conexão de banco de dados para analisar como subclassificar a recuperação de conexão de banco de dados.

```
    def get_new_connection(self, conn_params):
        try:
            logger.info("get connection")
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn =super(DatabaseWrapper,self).get_new_connection(conn_params)
            return conn
        except MySQLdb.OperationalError as e:
            error_code=e.args[0]
            if error_code!=1045:
                raise e

            logger.info("Authentication error. Going to refresh secret and try again.")
            databasecredentials.refresh_now()
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn=super(DatabaseWrapper,self).get_new_connection(conn_params)
            logger.info("Successfully refreshed secret and established new database
connection.")
            return conn
```

Código AWS CloudFormation e Python

- https://github.com/aws-samples/aws-secrets-manager-credential-rotation-without-container-restart

Épicos

Manter a disponibilidade do aplicativo durante a alternância de credenciais

Tarefa	Descrição	Habilidades necessárias
Instale o componente de cache.	Baixe e instale o componente de cache do lado do cliente do Secrets Manager para Python. Para obter o link para download, consulte a seção Recursos relacionados.	Desenvolvedor
Armazene em cache a credencial de trabalho.	Use o componente de cache do lado do cliente do Secrets Manager para armazenar em cache a credencial de trabalho localmente.	Desenvolvedor
Atualize o código do aplicativo para atualizar a credencial após o erro não autorizado da conexão com o banco de dados.	Atualize o código do aplicativo para usar o Secrets Manager para buscar e atualizar as credenciais do banco de dados. Adicione a lógica para lidar com códigos de erro não autorizados e, em seguida, busque a credencial recém-alternada. Consulte a seção Código em Python de exemplo.	Desenvolvedor

Recursos relacionados

Crie um segredo do Secrets Manager

- Crie chaves no AWS KMS
- Crie e gerencie segredos com o AWS Secrets Manager

Crie um cluster do Amazon Aurora

- Criação de uma instância de banco de dados do Amazon RDS

Criar os componentes do Amazon ECS

- Criação de um cluster usando o console clássico
- Criar uma imagem do Docker
- Criar um repositório privado
- Registro privado do Amazon ECR
- Envio de uma imagem do Docker
- Definições de tarefa do Amazon ECS
- Criar um serviço do Amazon ECS usando o console clássico

Baixe e instale o componente de cache do lado do cliente do Secrets Manager

- Cliente armazenado em cache para Python

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Execute tarefas do Amazon ECS na Amazon WorkSpaces com o Amazon ECS Anywhere

Criado por Akash Kumar (AWS)

Resumo

O Amazon Elastic Container Service (Amazon ECS) Anywhere é compatível com a implantação de tarefas do Amazon ECS em qualquer ambiente, incluindo a infraestrutura gerenciada pelo Amazon Web Services (AWS) e a infraestrutura gerenciada pelo cliente. Você pode fazer isso usando um ambiente de gerenciamento totalmente gerenciado pela AWS, executado na nuvem e sempre atualizado.

As empresas costumam usar a Amazon WorkSpaces para desenvolver aplicativos baseados em contêineres. Isso exigiu o Amazon Elastic Compute Cloud (Amazon EC2) ou o AWS Fargate com um cluster Amazon ECS para testar e executar tarefas do ECS. Agora, usando o Amazon ECS Anywhere, você pode adicionar a WorkSpaces Amazon como instâncias externas diretamente a um cluster do ECS e executar suas tarefas diretamente. Isso reduz seu tempo de desenvolvimento, porque você pode testar seu contêiner com um cluster ECS localmente na Amazon WorkSpaces. Você também pode economizar o custo de usar EC2 nossas instâncias Fargate para testar seus aplicativos de contêiner.

Esse padrão mostra como implantar tarefas do ECS na Amazon WorkSpaces com o Amazon ECS Anywhere. Ele configura o cluster do ECS e usa o AWS Directory Service Simple AD para iniciar o. WorkSpaces Em seguida, o exemplo de tarefa do ECS inicia o NGINX no. WorkSpaces

Pré-requisitos e limitações

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI)
- Credenciais da AWS configuradas em sua máquina

Arquitetura

Pilha de tecnologias de destino

- Uma nuvem privada virtual (VPC).

- Um cluster do Amazon ECS
- Amazon WorkSpaces
- AWS Directory Service com Simple AD

Arquitetura de destino

A arquitetura inclui os seguintes serviços e recursos:

- Um cluster do ECS com sub-redes públicas e privadas em uma VPC personalizada
- Simple AD na VPC para fornecer acesso ao usuário à Amazon WorkSpaces
- Amazon WorkSpaces provisionada na VPC usando Simple AD
- AWS Systems Manager ativado para adicionar a Amazon WorkSpaces como instâncias gerenciadas
- Usando o Amazon ECS e o AWS Systems Manager Agent (SSM Agent), a Amazon WorkSpaces adicionou ao Systems Manager e ao cluster ECS
- Um exemplo de tarefa do ECS a ser executada WorkSpaces no cluster do ECS

Ferramentas

- O Simple Active Directory (Simple AD) do AWS Directory Service é um diretório gerenciado autônomo alimentado por um servidor compatível com o Samba 4 Active Directory. O Simple AD fornece um subconjunto dos recursos oferecidos pelo AWS Managed Microsoft AD, incluindo a capacidade de gerenciar usuários e se conectar com segurança às instâncias da Amazon. EC2
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Systems Manager ajuda você a gerenciar seus aplicativos e infraestrutura em execução na nuvem AWS. Isso simplifica o gerenciamento de aplicações e recursos, diminui o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus recursos da AWS de modo seguro e em grande escala.

- WorkSpacesA Amazon ajuda você a provisionar desktops Microsoft Windows ou Amazon Linux virtuais baseados em nuvem para seus usuários, conhecidos como. WorkSpaces WorkSpaces elimina a necessidade de adquirir e implantar hardware ou instalar software complexo.

Épicos

Configurar o cluster ECS

Tarefa	Descrição	Habilidades necessárias
Criar e configurar o cluster ECS.	Para criar o cluster ECS, siga as instruções na documentação da AWS, incluindo as seguintes etapas: • Em Selecionar compatibilidade de cluster, escolha Somente rede, que suportará uma Amazon WorkSpace como uma instância externa para o cluster ECS. • Selecione Criar uma nova VPC.	Arquiteto de nuvem

Lance a Amazon WorkSpaces

Tarefa	Descrição	Habilidades necessárias
Configure o Simple AD e inicie a Amazon WorkSpaces.	Para provisionar um diretório Simple AD para sua VPC recém-criada e iniciar a Amazon WorkSpaces, siga as instruções na documentação da AWS.	Arquiteto de nuvem

Configuração do AWS Systems Manager para um ambiente híbrido

Tarefa	Descrição	Habilidades necessárias
Baixe os scripts anexados.	Em sua máquina local, baixe os arquivos `ssm-trust-policy.json` e `ssm-activation.json` que estão na seção Anexos.	Arquiteto de nuvem

Adicionar o perfil do IAM.	Adicionar variáveis de ambiente com base nos requisitos da sua empresa.
	`export AWS_DEFAULT_REGION=${AWS_REGION_ID}`
	`export ROLE_NAME=${ECS_TASK_ROLE}`
	`export CLUSTER_NAME=${ECS_CLUSTER_NAME}`
	`export SERVICE_NAME=${ECS_CLUSTER_SERVICE_NAME}`
	Execute o seguinte comando:
	`aws iam create-role --role-name $ROLE_NAME --assume-role-policy-document file://ssm-trust-policy.json`
		Arquiteto de nuvem

Adicione a SSMManaged InstanceCore política da Amazon à função do IAM.	Execute o seguinte comando: `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:p`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`olicy/AmazonSSMMan agedInstanceCore`	
Adicione a política do Amazon EC2 ContainerServicefor EC2 Role à função do IAM.	Execute o seguinte comando: `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`	Arquiteto de nuvem
Verificar o perfil do IAM.	Para verificar o perfil do IAM, excute o comando a seguir. `aws iam list-attached-role-policies --role-name $ROLE_NAME`	Arquiteto de nuvem
Ativar o Systems Manager.	Execute o seguinte comando: `aws ssm create-activation --iam-role $ROLE_NAME | tee ssm-activation.json`	Arquiteto de nuvem

Adicionar WorkSpaces ao cluster ECS

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao seu WorkSpaces.	Para se conectar e configurar seus espaços de trabalho, siga as instruções na documentação da AWS.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Baixar o script de instalação do ecs-anywhere.	No prompt de comando, execute o seguinte comando da . `curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh" && sudo chmod +x ecs-anywhere-install.sh`	Desenvolvedor de aplicativos
Verificar a integridade do script de shell.	(Opcional) Execute o seguinte comando. `curl -o "ecs-anywhere-install.sh.sha256" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh.sha256" && sha256sum -c ecs-anywhere-install.sh.sha256`	Desenvolvedor de aplicativos
Adicionar um repositório EPEL no Linux do Amazon.	Para adicionar um repositório de Extra Packages for Enterprise Linux (EPEL), execute o comando `sudo amazon-linux-extras install epel -y`.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Instalar o Amazon ECS Anywhere.	Para executar o script de instalação, use o seguinte comando. `sudo ./ecs-anywhere-install.sh --cluster $CLUSTER_NAME --activation-id $ACTIVATION_ID --activation-code $ACTIVATION_CODE --region $AWS_REGION`	
Verificar as informações da instância do cluster ECS.	Para verificar as informações da instância de cluster do Systems Manager e do ECS e validar as que WorkSpaces foram adicionadas ao cluster, execute o comando a seguir em sua máquina local. `aws ssm describe-instance-information" && "aws ecs list-container-instances --cluster $CLUSTER_NAME`	Desenvolvedor de aplicativos

Adicione uma tarefa do ECS para o WorkSpaces

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM de execução de tarefas	Baixar `task-execution-assume-role.json` e `external-task-defi`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`nition.json` na seção Anexos. Execute o seguinte comando na máquina local. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	
Adicione a política à função de execução.	Execute o seguinte comando: `aws iam --region $AWS_DEFAULT_REGION attach-role-policy --role-name $ECS_TASK_EXECUTION_ROLE --policy-arn arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um perfil de tarefas.	Execute o seguinte comando: `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	Arquiteto de nuvem
Registre a definição de tarefa para o cluster.	Execute o seguinte comando na máquina local. `aws ecs register-task-definition --cli-input-json file://external-task-definition.json`	Arquiteto de nuvem
Execute a tarefa.	Execute o seguinte comando na máquina local. `aws ecs run-task --cluster $CLUSTER_NAME --launch-type EXTERNAL --task-definition nginx`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

Validar o estado de execução da tarefa.	Para obter o ID da tarefa, execute o comando a seguir.
	`export TEST_TASKID= $(aws ecs list-tasks -- cluster $CLUSTER_NAME | jq -r '.taskArns[0]')`
	Com o ID da tarefa, execute o seguinte comando.
	`aws ecs describe-tasks --cluster $CLUSTER_ NAME --tasks ${TEST_TA SKID}`
		Arquiteto de nuvem

Verifique a tarefa no WorkSpace.	Para verificar se o NGINX está sendo executado no WorkSpace, execute o comando. `curl http://lo calhost:8080`	Desenvolvedor de aplicativos

Recursos relacionados

- Clusters do ECS
- Configurar ambientes híbridos
- Amazon WorkSpaces
- Simple AD

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Execute um contêiner Docker da API web ASP.NET Core em uma instância Amazon Linux EC2

Criado por Vijai Anand Ramalingam (AWS) e Sreelaxmi Pai (AWS)

Resumo

Esse padrão é para pessoas que estão começando a conteinerizar seus aplicativos na Nuvem da Amazon Web Services (AWS). Quando você começa a conteinerizar aplicativos na nuvem, geralmente não há plataformas de orquestração de contêineres configuradas. Esse padrão ajuda você a configurar rapidamente a infraestrutura na AWS para testar suas aplicações em contêineres sem precisar de uma infraestrutura elaborada de orquestração de contêineres.

A primeira etapa na jornada de modernização é transformar o aplicativo. Se for uma aplicação herdada do .NET Framework, você deve primeiro alterar o runtime para o ASP.NET Core. Faça o seguinte:

- Crie a imagem de contêiner do Docker
- Execute o contêiner do Docker usando a imagem criada
- Valide a aplicação antes de implantá-la em qualquer plataforma de orquestração de contêiner, como Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS).

Esse padrão abrange os aspectos de construção, execução e validação do desenvolvimento de aplicativos modernos em uma instância Linux do Amazon Elastic Compute Cloud EC2 (Amazon).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da Amazon Web Services (AWS)
- Um perfil do AWS Identity and Access Management (IAM) com acesso suficiente ao IAM para criar recursos da AWS para esse padrão.
- Visual Studio Community 2022 ou versão mais recente baixado e instalado
- Um projeto do .NET Framework modernizado para o ASP.NET Core
- Um GitHub repositório

Versões do produto

- Visual Studio Community 2022 ou versão mais recente

Arquitetura

Arquitetura de destino

Esse padrão usa um CloudFormation modelo da AWS para criar a arquitetura altamente disponível mostrada no diagrama a seguir. Uma instância Amazon EC2 Linux é executada em uma sub-rede privada. O AWS Systems Manager Session Manager é usado para acessar a instância privada Amazon EC2 Linux e testar a API em execução no contêiner Docker.

1. Acessar a instância Linux por meio do Session Manager

Ferramentas

Serviços da AWS

- AWS Command Line Interface (AWS CLI): a AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto para interagir com serviços da AWS por meio de comandos no seu shell de linha de comando. Com configuração mínima, você pode executar comandos da AWS CLI que implementam funcionalidade equivalente àquela fornecida pelo Console de Gerenciamento da AWS baseado em navegador.
- Console de Gerenciamento da AWS: o Console de Gerenciamento da AWS é um aplicativo web que compreende e se refere a uma ampla coleção de consoles de serviço para gerenciar recursos da AWS. Quando você faz login pela primeira vez, vê a página inicial do console. A página inicial fornece acesso a todos os consoles de serviço e oferece um único local para acessar as informações necessárias para executar as tarefas da AWS relacionadas.
- Session Manager do AWS Systems Manager: o Session Manager é um recurso totalmente gerenciado do AWS Systems Manager. Com o Session Manager, você pode gerenciar suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2). O Session Manager fornece gerenciamento de nós seguro e auditável sem a necessidade de abrir portas de entrada, manter bastion hosts ou gerenciar chaves SSH.

Outras ferramentas

- Visual Studio 2022: o Visual Studio 2022 é um ambiente de desenvolvimento integrado (IDE).
- Docker: o Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.

Código

```
FROM mcr.microsoft.com/dotnet/aspnet:5.0 AS base
 WORKDIR /app
EXPOSE 80
EXPOSE 443

FROM mcr.microsoft.com/dotnet/sdk:5.0 AS build
WORKDIR /src
COPY ["DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj", "DemoNetCoreWebAPI/"]
RUN dotnet restore "DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj"
COPY . .
WORKDIR "/src/DemoNetCoreWebAPI"
RUN dotnet build "DemoNetCoreWebAPI.csproj" -c Release -o /app/build

FROM build AS publish
RUN dotnet publish "DemoNetCoreWebAPI.csproj" -c Release -o /app/publish

FROM base AS final
WORKDIR /app
COPY --from=publish /app/publish .
ENTRYPOINT ["dotnet", "DemoNetCoreWebAPI.dll"]
```

Épicos

Desenvolver a API Web ASP.NET Core

Tarefa	Descrição	Habilidades necessárias
Criar uma API Web ASP.NET Core usando o Visual Studio.	Para criar um exemplo da ASP.NET Core Web API, faça o seguinte: 1. Abra o Visual Studio 2022. 2. Selecione Criar um novo projeto.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	3. Selecione o modelo de projeto ASP.NET Core Web API e escolha Avançar.
	4. Para o nome do projeto, insira DemoNetCoreWebAPI e escolha Avançar.
	5. Escolha Criar.
	6. Para executar o projeto localmente, pressione F5.
	7. Verifique se o endpoint padrão WeatherForecastda API está retornando os resultados usando o Swagger.
	8. Abra o prompt de comando, navegue até a pasta do projeto .csproj e execute os comandos a seguir para enviar a nova API da web para o seu repositório. GitHub
	`git add --all`
	`git commit -m “Initial Version”`
	`git push`	

Tarefa	Descrição	Habilidades necessárias

Crie um Dockerfile.	Para criar um novo Dockerfile, faça o seguinte:
	• Crie o Dockerfile manualmente usando o Dockerfile de exemplo na seção Código. Com base nos requisitos, selecione a imagem base .NET apropriada. Para obter informações sobre imagens relacionadas a .NET e ASP.NET Core, consulte o Docker hub.
	• Crie o Dockerfile usando o Visual Studio e o Docker Desktop. No explorador de soluções, clique com o botão direito do mouse no projeto e escolha Adicionar -> Suporte a Docker. Em SO de destino, selecione Linux. Certifique-se de que o novo Dockerfile esteja no mesmo caminho do arquivo de solução (.sln).
	
	Para enviar as alterações ao seu GitHub repositório, execute o comando a seguir.
	`git add --all`
	`git commit -m “Dockerfile added”`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`git push`	

Configurar a instância Amazon EC2 Linux

Tarefa	Descrição	Habilidades necessárias
Configure a infraestrutura.	Inicie o CloudFormation modelo da AWS para criar a infraestrutura, que inclui o seguinte: • Uma nuvem privada virtual (VPC), usando o AWS VPC Quick Start, com duas sub-redes públicas e duas privadas abrangendo duas zonas de disponibilidade. • O perfil do IAM necessári o para habilitar o AWS Systems Manager. • Em uma das sub-redes privadas, uma instância de demonstração do Amazon Linux 2 com o SSM Agent mais recente. Embora essa instância não tenha nenhuma conectividade direta com a Internet, ela pode ser acessada com segurança usando o Session Manager do AWS Systems Manager sem a necessidade de um bastion host.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Note O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs. Para saber mais sobre como acessar uma EC2 instância privada da Amazon usando o Session Manager sem precisar de um host bastion, consulte a postagem do blog Toward a bastion-less world.	

Tarefa	Descrição	Habilidades necessárias
Faça login na instância Amazon EC2 Linux.	Para se conectar à instância Amazon EC2 Linux na sub-rede privada, faça o seguinte: 1. Abra o EC2 console da Amazon. 2. No painel de navegação, escolha Instâncias. 3. Selecione a instância de demonstração do Amazon Linux 2 e escolha Conectar. **Note** O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs. 4. Escolha Session Manager. 5. Escolha Conectar para abrir uma nova janela de terminal. 6. Execute o seguinte comando: `sudo su`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Instala e inicializa o Docker.	Para instalar e iniciar o Docker na instância Amazon EC2 Linux, faça o seguinte:
	1. Para instalar o Docker, execute o comando a seguir:
	`yum install -y docker`
	2. Para reiniciar o serviço Docker, execute o seguinte comando.
	`service docker start`
	3. Para verificar a instalação Docker, execute o comando a seguir.
	`docker info`
		Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Acesse o Git e clone o repositório.	Para instalar o Git na instância Amazon EC2 Linux e clonar o repositório GitHub, faça o seguinte.
	1. Para instalar o Git, execute o comando a seguir.
	`yum install git -y`
	2. Para clonar o repositór io, execute o comando a seguir.
	`git clone https://g ithub.com/<usernam e>/<repo-name>.git`
	3. Para navegar até o Dockerfile, execute o comando a seguir.
	`cd <repo-name>/DemoNe tCoreWebAPI/`
		Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Compile e execute o contêiner do Docker.	Para criar a imagem do Docker e executar o contêiner dentro da instância Amazon EC2 Linux, faça o seguinte:
	1. Para criar a imagem do Docker, excute o comando a seguir.
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	2. Para visualizar todas as imagens do Docker, excute o comando a seguir.
	`docker images`
	3. Para criar e executar um contêiner, excute o comando a seguir.
	`docker run -d -p 80:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
		Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Testar a API da web

Tarefa	Descrição	Habilidades necessárias
Testar a API da web usando o comando curl.	Para testar a API, Execute o comando a seguir.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`curl -X GET "http://localhost/WeatherForecast" -H "accept: text/plain"` Verifique a resposta da API. **Note** Você pode obter os comandos curl para cada endpoint do Swagger ao executá-lo localmente.	

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Exclua todos os recursos	Exclua a pilha para remover todos os recursos. Isso garante que você não seja cobrado por nenhum serviço que não esteja usando.	Administrador da AWS, AWS DevOps

Recursos relacionados

- Conectar-se à instância do Linux no Windows usando PuTTY
- Criar uma API Web com o ASP.NET Core
- Toward a bastion-less world

Executar workloads orientadas por mensagens em grande escala usando o AWS Fargate

Criado por Stan Zubarev (AWS)

Resumo

Este padrão mostra como executar workloads orientadas por mensagens em grande escala na Nuvem AWS usando contêineres e o AWS Fargate.

O uso de contêineres para processar dados pode ser útil quando a quantidade de dados que um aplicativo processa excede as limitações dos serviços de computação de tecnologia sem servidor baseados em perfis. Por exemplo, se um aplicativo exigir mais capacidade computacional ou tempo de processamento do que o AWS Lambda oferece, o uso do Fargate pode melhorar o desempenho.

O exemplo de configuração a seguir usa o AWS Cloud Development Kit (AWS CDK) TypeScript para configurar e implantar os seguintes recursos na Nuvem AWS:

- Um serviço Fargate
- Uma fila do Amazon Simple Queue Service (Amazon SQS)
- Uma tabela do Amazon DynamoDB.
- Um CloudWatch painel da Amazon

O serviço Fargate recebe e processa mensagens da fila do Amazon SQS e as armazena na tabela do Amazon DynamoDB. Você pode monitorar quantas mensagens do Amazon SQS são processadas e quantos itens do DynamoDB são criados pelo Fargate usando o painel. CloudWatch

> **Note**
>
> Você também pode usar o código de exemplo desse padrão para criar cargas de trabalho de processamento de dados mais complexas em arquiteturas sem servidor orientadas por eventos. Para obter mais informações, consulte Execute workloads agendadas e orientadas por eventos em grande escala com o AWS Fargate.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- A versão mais recente da AWS Command Line Interface (AWS CLI), instalada e configurada em seu computador local
- O Git, instalado e configurado em sua máquina local
- O AWS CDK, instalado e configurado em sua máquina local
- Go, instalado e configurado em sua máquina local
- Docker, instalado e configurado em sua máquina local.

Arquitetura

Pilha de tecnologias de destino

- Amazon SQS
- AWS Fargate
- Amazon DynamoDB

Arquitetura de destino

O diagrama a seguir mostra um exemplo de fluxo de trabalho para executar workloads orientadas por mensagens em grande escala na Nuvem AWS usando o Fargate:

O diagrama mostra o seguinte fluxo de trabalho:

1. O serviço Fargate usa sondagem longa do Amazon SQS para receber mensagens de uma fila do Amazon SQS.
2. Em seguida, o serviço Fargate processa as mensagens do Amazon SQS e as armazena em uma tabela do DynamoDB.

Automação e escala

Para automatizar o ajuste de escala da contagem de tarefas do Fargate, é possível configurar o Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling. É uma prática recomendada configurar a política de ajuste de escala com base no número de mensagens visíveis na fila do Amazon SQS do seu aplicativo.

Para obter mais informações, consulte Escalabilidade com base no Amazon SQS no Guia do usuário do Amazon Auto EC2 Scaling.

Ferramentas

Serviços da AWS

- O AWS Fargate ajuda você a executar contêineres sem precisar gerenciar servidores ou instâncias do Amazon Elastic Compute Cloud (Amazon). EC2 É usado em conjunto com o Amazon Elastic Container Service (Amazon ECS).
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.

Código

O código desse padrão está disponível no repositório GitHub sqs-fargate-ddb-cdk-go.

Épicos

Crie e implante os recursos usando o AWS CDK

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Clone o repositório GitHub sqs-fargate-ddb-cdk-go em sua máquina local executando o seguinte comando: `git clone https://github.com/aws-samples/sqs-fargate-ddb-cdk-go.git`	Desenvolvedor de aplicativos
Verifique se a AWS CLI está configurado para a conta	Para verificar se as configurações da AWS CLI estão	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
correta da AWS e se a CDK da AWS tem as permissões necessárias.	corretas, é possível executar o seguinte comando ls do Amazon Simple Storage Service (Amazon S3): `aws s3 ls` Esse procedimento também exige que o AWS CDK tenha permissões para provision ar a infraestrutura em sua conta da AWS. Para conceder as permissões necessári as, você deve criar um perfil nomeado da AWS na AWS CLI e exportá-lo como uma variável de AWS_PROFI LEambiente. **Note** Se você nunca usou o AWS CDK em sua conta da AWS, primeiro você deve provisionar os recursos necessários do AWS CDK. Para obter mais informaçõ es, consulte Inicializar no Guia do desenvolv edor do AWS CDK v2.	

Tarefa	Descrição	Habilidades necessárias

Implante a pilha da AWS CDK em sua conta da AWS.	1. Compile uma imagem de contêiner executando o seguinte comando da AWS CLI:
	`docker build -t go-fargate .`
	2. Abra o diretório da AWS CDK executando o seguinte comando:
	`cd cdk`
	3. Instale os módulos npm necessários executando o seguinte comando:
	`npm i`
	4. Implante o padrão da AWS CDK em sua conta da AWS executando o seguinte comando:
	`cdk deploy --profile ${AWS_PROFILE}`
		Desenvolvedor de aplicativos

Testar a configuração

Tarefa	Descrição	Habilidades necessárias
Envie uma mensagem de teste para a fila do Amazon SQS.	Para obter instruções, consulte Enviar mensagens para uma fila (console) no Guia do desenvolvedor do Amazon SQS.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Exemplo de mensagem de teste do Amazon SQS `{ "message": "hello, Fargate" }`	
Verifique se a mensagem de teste aparece nos registros do serviço Fargate. CloudWatch	Siga as instruções em Visualização de CloudWatch registros no Amazon ECS Developer Guide. Certifique-se de revisar os registros do grupo de go-fargate-service registros no cluster do go-service-clusterECS.	Desenvolvedor de aplicativos
Verifique se a mensagem de teste aparece na tabela do DynamoDB.	1. Abra o console do DynamoDB. 2. No painel de navegação à esquerda, selecione Tables (Tabelas). Em seguida, selecione a tabela a seguir na lista: sqs-fargate-ddb-table. 3. Escolha Explore table items (Explorar itens da tabela). 4. Verifique se a mensagem de teste aparece na lista Itens devolvidos.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Verifique se o serviço Fargate está enviando mensagens para CloudWatch o Logs.	1. Abra o console de CloudWatch . 2. No painel de navegação à esquerda, escolha Painéis. 3. Na lista Painéis personalizados, selecione o painel chamado go-service-dashboard. 4. Verifique se a mensagem de teste aparece nos logs. **Note** O AWS CDK cria automaticamente o CloudWatch painel na sua conta da AWS.	Desenvolvedor de aplicativos

Limpeza

Tarefa	Descrição	Habilidades necessárias
Exclua a pilha do AWS CDK.	1. Abra o diretório do AWS CDK na AWS CLI executando o seguinte comando: `cd cdk` 2. Exclua a pilha do AWS CDK executando o seguinte comando:	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`cdk destroy --profile ${AWS_PROFILE}`	
Verifique se a pilha do AWS CDK foi excluída.	Para garantir que a pilha foi excluída, execute o seguinte comando: `aws cloudformation list-stacks --query \ "StackSummaries[?contains(StackName,'SqsFargate')].StackStatus" \ --profile ${AWS_PROFILE}` O valor `StackStatus` retornado na saída do comando é `DELETE_COMPLETE` se a pilha foi excluída. Para obter mais informações, consulte exemplos de comandos de operação de CloudFormation pilha para AWS CLI e PowerShell no Guia do CloudFormation usuário da AWS.	Desenvolvedor de aplicativos

Recursos relacionados

- Como configurar a AWS CLI (Guia do usuário da AWS CLI para versão 2)
- Referência de API (referência de API do AWS CDK)

- Documentação do AWS SDK para Go v2 (documentação do Go)

Executar workloads monitoradas com armazenamento de dados persistente usando o Amazon EFS no Amazon EKS com o AWS Fargate

Criado por Ricardo Morais (AWS), Rodrigo Bersa (AWS) e Lucio Pereira (AWS)

Resumo

Esse padrão fornece orientação para habilitar o Amazon Elastic File System (Amazon EFS) como um dispositivo de armazenamento para contêineres que estão sendo executados no Amazon Elastic Kubernetes Service (Amazon EKS) usando o AWS Fargate para provisionar seus recursos computacionais.

A configuração descrita nesse padrão segue as práticas recomendadas de segurança e fornece segurança em repouso e segurança em trânsito por padrão. Para criptografar seu sistema de arquivos Amazon EFS, ele usa uma chave do AWS Key Management Service (AWS KMS), mas você também pode especificar um alias de chave que despacha o processo de criação de uma chave KMS.

Você pode seguir as etapas desse padrão para criar um namespace e um perfil Fargate para um aplicativo proof-of-concept (PoC), instalar o driver Amazon EFS Container Storage Interface (CSI) usado para integrar o cluster Kubernetes ao Amazon EFS, configurar a classe de armazenamento e implantar o aplicativo PoC. Essas etapas resultam em um sistema de arquivos Amazon EFS que é compartilhado entre várias workloads do Kubernetes, executado no Fargate. O padrão é acompanhado por scripts que automatizam essas etapas.

Você pode usar esse padrão se quiser a persistência de dados em seus aplicativos em contêineres e evitar a perda de dados durante as operações de escalabilidade. Por exemplo:

- DevOps ferramentas — Um cenário comum é desenvolver uma ferramenta de integração e entrega contínuas (CI/CD) strategy. In this case, you can use Amazon EFS as a shared file system to store configurations among different instances of the CI/CD tool or to store a cache (for example, an Apache Maven repository) for pipeline stages among different instances of the CI/CDferramenta).
- Servidores Web — Um cenário comum é usar o Apache como um servidor Web HTTP. Você pode usar o Amazon EFS como um sistema de arquivos compartilhado para armazenar arquivos estáticos que são compartilhados entre diferentes instâncias do servidor web. Neste cenário de exemplo, as modificações são aplicadas diretamente ao sistema de arquivos em vez de arquivos estáticos serem incorporados a uma imagem do Docker.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um cluster Amazon EKS existente com Kubernetes versão 1.17 ou posterior (testado até a versão 1.27)
- Um sistema de arquivos Amazon EFS existente para vincular um Kubernetes StorageClass e provisionar sistemas de arquivos dinamicamente
- Permissões de administração do cluster
- Contexto configurado para apontar para o cluster Amazon EKS desejado

Limitações

- Há algumas limitações a serem consideradas ao usar o Amazon EKS com o Fargate. Por exemplo, o uso de algumas construções do Kubernetes, como DaemonSets contêineres privilegiados, não é suportado. Para obter mais informações sobre as limitações do Fargate, consulte as considerações sobre o AWS Fargate na documentação do Amazon EKS.
- O código fornecido com esse padrão é compatível com estações de trabalho que executam Linux ou macOS.

Versões do produto

- AWS Command Line Interface (AWS CLI) versão 2 ou superior
- Driver Amazon EFS CSI versão 1.0 ou posterior (testado até a versão 2.4.8)
- eksctl versão 0.24.0 ou posterior (testado até a versão 0.158.0)
- jq versão 1.6 ou posterior
- kubectl versão 1.17 ou posterior (testado até a versão 1.27)
- Kubernetes versão 1.17 ou posterior (testado até a versão 1.27)

Arquitetura

A arquitetura de destino é composta pela seguinte infraestrutura:

- Uma nuvem privada virtual (VPC).
- Duas zonas de disponibilidade
- Uma sub-rede pública com um gateway NAT que fornece acesso à Internet
- Uma sub-rede privada com um cluster Amazon EKS e destinos de montagem do Amazon EFS (também conhecidos como pontos de montagem)
- Amazon EFS no nível da VPC

A seguir está a infraestrutura do ambiente para o cluster Amazon EKS:

- Perfis do AWS Fargate que acomodam as construções do Kubernetes no nível do namespace
- Um namespace Kubernetes com:
  - Dois pods de aplicativos distribuídos em zonas de disponibilidade
  - Uma declaração de volume persistente (PVC) vinculada a um volume persistente (PV) no nível do cluster
- Um PV em todo o cluster que está vinculado ao PVC no namespace e que aponta para os destinos de montagem do Amazon EFS na sub-rede privada, fora do cluster

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que você pode usar para interagir com os serviços da AWS a partir da linha de comando.
- Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS. Nesse padrão, ele fornece um sistema de arquivos simples, escalável, totalmente gerenciado e compartilhado para uso com o Amazon EKS.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar ou operar seus próprios clusters.
- O AWS Fargate é um mecanismo de computação sem servidor para o Amazon EKS. Ele cria e gerencia recursos computacionais para seus aplicativos Kubernetes.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- O eksctl é utilitário de linha de comando para criar e gerenciar clusters do Kubernetes no Amazon EKS.
- kubectl é uma interface de linha de comando que ajuda você na execução de comandos em clusters do Kubernetes.
- jq é uma ferramenta de linha de comando para analisar JSON.

Código

O código desse padrão é fornecido na Configuração de GitHub persistência com o Amazon EFS no Amazon EKS usando o repositório AWS Fargate. Os scripts são organizados por épicos, nas pastas a `epic01` meio`epic06`, correspondendo à ordem na seção Epics nesse padrão.

Práticas recomendadas

A arquitetura de destino inclui os seguintes serviços e componentes e segue as melhores práticas do AWS Well-Architected Framework:

- Amazon EFS, que fornece um sistema de arquivos NFS elástico simples, escalável e totalmente gerenciado. Isso é usado como um sistema de arquivos compartilhado entre todas as replicações do aplicativo PoC que estão sendo executadas em pods, que são distribuídos nas sub-redes privadas do cluster Amazon EKS escolhido.
- Um destino de montagem do Amazon EFS para cada sub-rede privada. Isso fornece redundância por zona de disponibilidade na nuvem privada virtual (VPC) do cluster.
- Amazon EKS, que executa as workloads do Kubernetes. Você deve provisionar um cluster do Amazon EKS antes de usar esse padrão, conforme descrito na seção Pré-requisitos.
- AWS KMS, que fornece criptografia em repouso para o conteúdo armazenado no sistema de arquivos Amazon EFS.
- Fargate, que gerencia os recursos computacionais dos contêineres para que você possa se concentrar nos requisitos de negócios em vez da carga de infraestrutura. O perfil Fargate é criado para todas as sub-redes privadas. Ele fornece redundância por zona de disponibilidade na nuvem privada virtual (VPC) do cluster.
- Kubernetes Pods, para validar se o conteúdo pode ser compartilhado, consumido e gravado por diferentes instâncias de um aplicativo.

Épicos

Provisionar um cluster Amazon EKS (opcional)

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do Amazon EKS.	**Note** Se você já tem um cluster implantado, pule para o próximo épico. Crie um cluster Amazon EKS em sua conta existente da AWS. No GitHub diretório, use um dos padrões para implantar um cluster Amazon EKS usando o Terraform ou o eksctl. Para obter mais informações, consulte Criação de um cluster do Amazon EKS na documenta ção do Amazon EKS. No padrão Terraform, também há exemplos que mostram como: vincular perfis do Fargate ao seu cluster do Amazon EKS, criar um sistema de arquivos do Amazon EFS e implantar o driver CSI do Amazon	Administrador da AWS, administrador do Terraform ou eksctl, administrador do Kubernetes

Tarefa	Descrição	Habilidades necessárias
	EFS no seu cluster do Amazon EKS.	

Tarefa	Descrição	Habilidades necessárias

Exporte variáveis de ambiente.	Execute o script env.sh. Isso fornece as informações necessárias nas próximas etapas.
	`source ./scripts/env.sh`
	`Inform the AWS Account ID: <13-digit-account-id>`
	`Inform your AWS Region: <aws-Region-code>`
	`Inform your Amazon EKS Cluster Name: <amazon-eks-cluster-name>`
	`Inform the Amazon EFS Creation Token: <self-genereated-uuid>`
	Se ainda não foi mencionado, você pode obter todas as informações solicitadas acima com os seguintes comandos da CLI.
	`# ACCOUNT ID`
	`aws sts get-caller-identity --query "Account" --output text`
	`# REGION CODE`
	`aws configure get region`
	`# CLUSTER EKS NAME`
		Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	`aws eks list-clusters --query "clusters" --output text`
	
	`# GENERATE EFS TOKEN uuidgen`	

Crie um namespace Kubernetes e um perfil Fargate vinculado

Tarefa	Descrição	Habilidades necessárias
Crie um namespace Kubernetes e um perfil Fargate para cargas de trabalho de aplicativos.	Crie um namespace para receber as workloads do aplicativo que interagem com o Amazon EFS. Execute o script `create-k8s-ns-and-linked-fargate-profile.sh` . Você pode optar por usar um nome de namespace personalizado ou o namespace padrão fornecido. `poc-efs-eks-fargate` Com um nome de namespace de aplicativo personalizado: `export $APP_NAME SPACE=<CUSTOM_NAME> ./scripts/epic01/ create-k8s-ns-and -linked-fargate-pr ofile.sh \ -c "$CLUSTER_NAME" -n "$APP_NAMESPACE"`	Usuário do Kubernetes com permissões concedidas

Tarefa	Descrição	Habilidades necessárias

	Sem um nome de namespace de aplicativo personalizado:
	
	`./scripts/epic01/create-k8s-ns-and-linked-fargate-profile.sh \`
	`  -c "$CLUSTER_NAME"`
	
	onde `$CLUSTER_NAME` é o nome do cluster do Amazon EKS. O `-n <NAMESPACE>` parâmetro é opcional; se não for informado, um nome de namespace padrão gerado será fornecido.	

Criar um sistema de arquivos do Amazon EFS

Tarefa	Descrição	Habilidades necessárias
Gere um token exclusivo.	O Amazon EFS requer um token de criação para garantir uma operação idempotente (chamar a operação com o mesmo token de criação não tem efeito). Para atender a esse requisito, você deve gerar um token exclusivo por meio de uma técnica disponível. Por exemplo, você pode gerar um identificador universal exclusivo (UUID) para usar como um token de criação.	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

Criar um sistema de arquivos do Amazon EFS.	Crie o sistema de arquivos para receber os arquivos de dados que são lidos e gravados pelas workloads do aplicativo. Você pode criar um sistema de arquivos criptografado ou não criptografado. (Como prática recomendada, o código deste padrão cria um sistema criptografado para habilitar a criptografia em repouso por padrão.) Você pode usar uma chave exclusiva e simétrica do AWS KMS para criptografar seu sistema de arquivos. Se uma chave personalizada não for especificada, uma chave gerenciada pela AWS será usada.
	
	Use o script create-efs.sh para criar um sistema de arquivos Amazon EFS criptografado ou não criptografado, depois de gerar um token exclusivo para o Amazon EFS.
	
	Com a criptografia em repouso, sem uma chave KMS:
	
	`./scripts/epic02/create-efs.sh \`
	`-c "$CLUSTER_NAME" \`
		Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	`-t "$EFS_CREATION_TOKEN"`
	
	onde `$CLUSTER_NAME` é o nome do seu cluster Amazon EKS e `$EFS_CREATION_TOKEN` é um token de criação exclusivo para o sistema de arquivos.
	
	Com a criptografia em repouso, com uma chave KMS:
	
	`./scripts/epic02/create-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \ -k "$KMS_KEY_ALIAS"`
	
	onde `$CLUSTER_NAME` é o nome do seu cluster Amazon EKS e `$EFS_CREATION_TOKEN` é um token de criação exclusivo para o sistema de arquivos, e `$KMS_KEY_ALIAS` é o alias para a chave do KMS.
	
	Sem criptografia:
	
	`./scripts/epic02/create-efs.sh -d \ -c "$CLUSTER_NAME" \`	

Tarefa	Descrição	Habilidades necessárias
	`-t "$EFS_CRE ATION_TOKEN"` onde `$CLUSTER_NAME` é o nome do seu cluster Amazon EKS, `$EFS_CREA TION_TOKEN` é um token de criação exclusivo para o sistema de arquivos e `-d` desabilita a criptografia em repouso.	
Crie um grupo de segurança.	Crie um grupo de segurança para permitir que o cluster do Amazon EKS acesse o sistema de arquivos do Amazon EFS.	Administrador de sistemas AWS
Atualize a regra de entrada para o grupo de segurança.	Atualize as regras de entrada do grupo de segurança para permitir o tráfego de entrada nas seguintes configurações: • Protocolo TCP — porta 2049 • Fonte — intervalos de blocos CIDR para as sub-redes privadas na VPC que contém o cluster Kubernetes	Administrador de sistemas AWS
Adicione um destino de montagem para cada sub-rede privada.	Para cada sub-rede privada do cluster Kubernetes, crie um destino de montagem para o sistema de arquivos e o grupo de segurança.	Administrador de sistemas AWS

Instale componentes do Amazon EFS no cluster Kubernetes

Tarefa	Descrição	Habilidades necessárias
Implemente o driver da CSI do Amazon EFS.	Implemente o driver da CSI do Amazon EFS no cluster. O driver provisiona o armazenamento de acordo com as declarações de volume persistentes criadas pelos aplicativos. Execute o `create-k8s-efs-csi-sc.sh` script para implantar o driver CSI do Amazon EFS e a classe de armazenamento no cluster. `./scripts/epic03/create-k8s-efs-csi-sc.sh` Esse script usa o `kubectl` utilitário, portanto, certifique-se de que o contexto tenha sido configurado e aponte para o cluster Amazon EKS desejado.	Usuário do Kubernetes com permissões concedidas
Implante a classe de armazenamento.	Implante a classe de armazenamento no cluster do provisionador Amazon EFS (efs.csi.aws.com).	Usuário do Kubernetes com permissões concedidas

Instale o aplicativo PoC no cluster Kubernetes

Tarefa	Descrição	Habilidades necessárias
Implante o volume persistente.	Implante o volume persisten te e vincule-o à classe de armazenamento criada e ao ID do sistema de arquivos Amazon EFS. O aplicativo usa o volume persistente para ler e gravar conteúdo. Você pode especificar qualquer tamanho para o volume persistente no campo de armazenam ento. O Kubernetes requer esse campo, mas como o Amazon EFS é um sistema de arquivos elástico, ele não impõe nenhuma capacidad e de sistema de arquivos. Você pode implantar o volume persistente com ou sem criptografia. (O driver CSI do Amazon EFS habilita a criptografia por padrão, como uma prática recomenda da.) Execute o `deploy-poc-app.sh` script para implantar o volume persisten te, a declaração de volume persistente e as duas cargas de trabalho. Com criptografia em trânsito: `./scripts/epic04/deploy-poc-app.sh \`	Usuário do Kubernetes com permissões concedidas

Tarefa	Descrição	Habilidades necessárias

	`-t "$EFS_CREATION_TOKEN"`
	
	onde `$EFS_CREATION_TOKEN` é o token de criação exclusivo para o sistema de arquivos.
	
	Sem criptografia em trânsito:
	
	`./scripts/epic04/deploy-poc-app.sh -d \ -t "$EFS_CREATION_TOKEN"`
	
	onde `$EFS_CREATION_TOKEN` é o token de criação exclusivo para o sistema de arquivos e `-d` desativa a criptografia em trânsito.	

Tarefa	Descrição	Habilidades necessárias
Implante a declaração de volume persistente solicitada pelo aplicativo.	Implante a declaração de volume persistente solicitad a pelo aplicativo e vincule-a à classe de armazenam ento. Use o mesmo modo de acesso do volume persisten te que você criou anteriorm ente. Você pode especific ar qualquer tamanho para a reivindicação de volume persistente no campo de armazenamento. O Kubernete s requer esse campo, mas como o Amazon EFS é um sistema de arquivos elástico, ele não impõe nenhuma capacidade de sistema de arquivos.	Usuário do Kubernetes com permissões concedidas
Implante a workload 1.	Implante o pod que represent a a workload 1 do aplicativo. Essa carga de trabalho grava conteúdo no arquivo `/data/out1.txt` .	Usuário do Kubernetes com permissões concedidas
Implante a workload 2.	Implante o pod que represent a a workload 2 do aplicativo. Essa carga de trabalho grava conteúdo no arquivo `/data/out2.txt` .	Usuário do Kubernetes com permissões concedidas

Valide a persistência, a durabilidade e a capacidade de compartilhamento do sistema de arquivos

Tarefa	Descrição	Habilidades necessárias
Verifique o status do`PersistentVolume` .	Digite o comando a seguir para verificar o status do`PersistentVolume` . `kubectl get pv` Para obter um exemplo de saída, consulte a seção Informações adicionais.	Usuário do Kubernetes com permissões concedidas
Verifique o status do`PersistentVolumeClaim` .	Digite o comando a seguir para verificar o status do`PersistentVolumeClaim` . `kubectl -n poc-efs-eks-fargate get pvc` Para obter um exemplo de saída, consulte a seção Informações adicionais.	Usuário do Kubernetes com permissões concedidas
Validar se a workload 1 pode gravar no sistema de arquivos.	Digite o comando a seguir para validar se a carga de trabalho 1 está sendo gravada. `/data/out1.txt` `kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -f /data/out1.txt` Os resultados são semelhantes aos seguintes:	Usuário do Kubernetes com permissões concedidas

Tarefa	Descrição	Habilidades necessárias
	``` ... Thu Sep 3 15:25:07 UTC 2023 - PoC APP 1 Thu Sep 3 15:25:12 UTC 2023 - PoC APP 1 Thu Sep 3 15:25:17 UTC 2023 - PoC APP 1 ... ```	
Validar se a workload 2 pode gravar no sistema de arquivos.	Digite o comando a seguir para validar se a carga de trabalho 2 está sendo gravada. `/data/out2.txt` ``` kubectl -n $APP_NAME SPACE exec -ti poc-app2 -- tail -f /data/out 2.txt ``` Os resultados são semelhant es aos seguintes: ``` ... Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2 ... ```	Usuário do Kubernetes com permissões concedidas

Tarefa	Descrição	Habilidades necessárias

Validar se a workload 1 pode ler o arquivo gravado pela workload 2.	Insira o comando a seguir para validar se a carga de trabalho 1 pode ler o `/data/out2.txt` arquivo gravado pela carga de trabalho 2.
	`kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -n 3 /data/out2.txt`
	Os resultados são semelhantes aos seguintes:
	`... Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2 ...`
		Usuário do Kubernetes com permissões concedidas

Tarefa	Descrição	Habilidades necessárias

Validar se a workload 2 pode ler o arquivo gravado pela workload 1.	Insira o comando a seguir para validar se a carga de trabalho 2 pode ler o `/data/out1.txt` arquivo gravado pela carga de trabalho 1.
	`kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -n 3 /data/out1.txt`
	Os resultados são semelhantes aos seguintes:
	`... Thu Sep 3 15:29:22 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:27 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:32 UTC 2023 - PoC APP 1 ...`
		Usuário do Kubernetes com permissões concedidas

Tarefa	Descrição	Habilidades necessárias

Valide se os arquivos são retidos após a remoção dos componentes do aplicativo.	Em seguida, você usa um script para remover os componentes do aplicativo (volume persistente, declaração de volume persistente e pods) e validar se os arquivos `/data/out1.txt` `/data/out2.txt` estão retidos no sistema de arquivos. Execute o script `validate-efs-content.sh` usando o comando a seguir.
	`./scripts/epic05/validate-efs-content.sh \`
	`-t "$EFS_CREATION_TOKEN"`
	onde `$EFS_CREATION_TOKEN` é o token de criação exclusivo para o sistema de arquivos.
	Os resultados são semelhantes aos seguintes:
	`pod/poc-app-validation created`
	`Waiting for pod get Running state...`
	`Waiting for pod get Running state...`
	`Waiting for pod get Running state...`
	`Results from execution of 'find /data' on`
		Usuário do Kubernetes com permissões concedidas, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
	validation process pod: /data /data/out2.txt /data/out1.txt	

Monitore as operações

Tarefa	Descrição	Habilidades necessárias
Monitore os registros do aplicativo.	Como parte de uma operação do segundo dia, envie os registros do aplicativo para a Amazon CloudWatch para monitoramento.	Administrador de sistemas da AWS, usuário do Kubernetes com permissões concedidas
Monitore os contêineres do Amazon EKS e do Kubernetes com o Container Insights.	Como parte de uma operação do segundo dia, monitore os sistemas Amazon EKS e Kubernetes usando o Amazon Container Insights. CloudWatch Essa ferramenta coleta, agrega e resume métricas de aplicações em contêineres em diferentes níveis e dimensões. Para obter mais informações, consulte a seção Recursos relacionados.	Administrador de sistemas da AWS, usuário do Kubernetes com permissões concedidas
Monitore o Amazon EFS com CloudWatch.	Como parte de uma operação do segundo dia, monitore os sistemas de arquivos usando a Amazon CloudWatch, que coleta e processa dados brutos do Amazon EFS em	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	métricas legíveis e quase em tempo real. Para obter mais informações, consulte a seção Recursos relacionados.	

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Limpe todos os recursos criados para o padrão.	Depois de concluir esse padrão, limpe todos os recursos para evitar incorrer em cobranças da AWS. Execute o `clean-up-resources.sh` script para remover todos os recursos depois de terminar de usar o aplicativo PoC. Conclua uma das opções a seguir. Com a criptografia em repouso, com uma chave KMS: `./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \ -k "$KMS_KEY_ALIAS"` onde `$CLUSTER_NAME` é o nome do seu cluster Amazon EKS, `$EFS_CREA`	Usuário do Kubernetes com permissões concedidas, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
	`TION_TOKEN` é o token de criação exclusivo para o sistema de arquivos e `$KMS_KEY_ALIAS` é o alias da chave KMS. Sem criptografia em repouso: `./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"` onde `$CLUSTER_NAME` é o nome do seu cluster Amazon EKS e `$EFS_CREATION_TOKEN` é um token de criação para o sistema de arquivos.	

Recursos relacionados

Referências

- O AWS Fargate para Amazon EKS agora oferece suporte ao Amazon EFS (anúncio)
- How to capture application logs when using Amazon EKS on AWS Fargate (Como capturar registros de aplicativos ao usar o Amazon EKS no AWS Fargate) (publicação do blog)
- Usando o Container Insights (CloudWatch documentação da Amazon)
- Configuração do Container Insights no Amazon EKS e no Kubernetes (documentação da Amazon) CloudWatch
- Métricas do Amazon EKS e do Kubernetes Container Insights (documentação da Amazon) CloudWatch

- Monitoramento do Amazon EFS com a Amazon CloudWatch (documentação do Amazon EFS)

GitHub tutoriais e exemplos

- Static provisioning (Provisionamento estático)
- Criptografia em trânsito
- Accessing the file system from multiple pods (Accessing the file system from multiple pods)
- Consumindo o Amazon EFS em StatefulSets
- Mounting subpaths (Montagem de subcaminhos)
- Using Amazon EFS access points (Uso de pontos de acesso do Amazon EFS)
- Amazon EKS Blueprints para Terraform

Ferramentas necessárias

- Instalação da AWS CLI versão 2
- Instalação do eksctl
- Instalação do kubectl
- Instalação do jq

Mais informações

Veja a seguir um exemplo de saída do `kubectl get pv` comando.

```
NAME         CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM
            STORAGECLASS   REASON   AGE
poc-app-pv   1Mi        RWX            Retain           Bound    poc-efs-eks-fargate/
poc-app-pvc   efs-sc                  3m56s
```

Veja a seguir um exemplo de saída do `kubectl -n poc-efs-eks-fargate get pvc` comando.

```
NAME          STATUS   VOLUME       CAPACITY   ACCESS MODES   STORAGECLASS   AGE
poc-app-pvc   Bound    poc-app-pv   1Mi        RWX            efs-sc         4m34s
```

Configure o escalonamento automático orientado por eventos no Amazon EKS usando o Amazon EKS Pod Identity e o KEDA

Criado por Dipen Desai (AWS), Abhay Diwan (AWS), Kamal Joshi (AWS) e Mahendra Revanasiddappa (AWS)

Resumo

Plataformas de orquestração, como o Amazon Elastic Kubernetes Service (Amazon EKS), simplificaram o gerenciamento do ciclo de vida de aplicativos baseados em contêineres. Isso ajuda as organizações a se concentrarem na criação, proteção, operação e manutenção de aplicativos baseados em contêineres. À medida que as implantações orientadas por eventos se tornam mais comuns, as organizações estão escalando com mais frequência as implantações do Kubernetes com base em várias fontes de eventos. Esse método, combinado com o escalonamento automático, pode resultar em economias de custo significativas ao fornecer recursos computacionais sob demanda e escalabilidade eficiente, adaptada à lógica do aplicativo.

O KEDA é um autoescalador baseado em eventos baseado em Kubernetes. O KEDA ajuda você a escalar qualquer contêiner no Kubernetes com base no número de eventos que precisam ser processados. É leve e se integra a qualquer cluster Kubernetes. Ele também funciona com componentes padrão do Kubernetes, como o escalonamento automático de pods horizontais (HPA). A KEDA também oferece TriggerAuthenticationum recurso que ajuda você a delegar a autenticação. Ele permite que você descreva os parâmetros de autenticação separados dos contêineres ScaledObject e de implantação.

AWS fornece funções AWS Identity and Access Management (IAM) que oferecem suporte a diversas opções de implantação do Kubernetes, incluindo Amazon EKS, Amazon EKS Anywhere Serviço Red Hat OpenShift na AWS (ROSA) e clusters de Kubernetes autogerenciados no Amazon Elastic Compute Cloud (Amazon). EC2 Essas funções usam construções do IAM, como provedores de identidade OpenID Connect (OIDC) e políticas de confiança do IAM, para operar em diferentes ambientes sem depender diretamente dos serviços do Amazon EKS ou. APIs Para obter mais informações, consulte Funções do IAM para contas de serviço na documentação do Amazon EKS.

O Amazon EKS Pod Identity simplifica o processo para que as contas de serviço do Kubernetes assumam funções do IAM sem exigir provedores de OIDC. Ele fornece a capacidade de gerenciar credenciais para seus aplicativos. Em vez de criar e distribuir suas AWS credenciais para os contêineres ou usar a função da EC2 instância da Amazon, você associa uma função do IAM a uma conta de serviço do Kubernetes e configura seus pods para usar a conta de serviço. Isso ajuda você

a usar uma função do IAM em vários clusters e simplifica o gerenciamento de políticas ao permitir a reutilização de políticas de permissão em todas as funções do IAM.

Ao implementar o KEDA com o Amazon EKS Pod Identity, as empresas podem obter escalabilidade automática eficiente orientada por eventos e gerenciamento simplificado de credenciais. Os aplicativos são dimensionados com base na demanda, o que otimiza a utilização dos recursos e reduz os custos.

Esse padrão ajuda você a integrar o Amazon EKS Pod Identity com o KEDA. Ele mostra como você pode usar a conta de `keda-operator` serviço e delegar a autenticação com. `TriggerAuthentication` Também descreve como configurar uma relação de confiança entre uma função do IAM para o operador KEDA e uma função do IAM para o aplicativo. Essa relação de confiança permite que a KEDA monitore mensagens nas filas de eventos e ajuste a escala para os objetos Kubernetes de destino.

Pré-requisitos e limitações

Pré-requisitos

- AWS Command Line Interface (AWS CLI) versão 2.13.17 ou posterior, instalada
- Python versão 3.11.5 ou posterior, instalado
- AWS SDK para Python (Boto3) versão 1.34.135 ou posterior, instalada
- Helm versão 3.12.3 ou posterior, instalado
- kubectl versão 1.25.1 ou posterior, instalado
- Docker Engine versão 26.1.1 ou posterior, instalado
- Um cluster Amazon EKS versão 1.24 ou posterior, criado
- Pré-requisitos para criar o agente Amazon EKS Pod Identity, atendidos

Limitações

- É necessário que você estabeleça uma relação de confiança entre a `keda-operator` função e a `keda-identity` função. As instruções são fornecidas na seção Epics desse padrão.

Arquitetura

Nesse padrão, você cria os seguintes AWS recursos:

- Repositório Amazon Elastic Container Registry (Amazon ECR) — Nesse padrão, esse repositório é nomeado. `keda-pod-identity-registry` Esse repositório privado é usado para armazenar imagens Docker do aplicativo de amostra.
- Fila do Amazon Simple Queue Service (Amazon SQS) — Nesse padrão, essa fila é nomeada. `event-messages-queue` A fila funciona como um buffer de mensagens que coleta e armazena as mensagens recebidas. O KEDA monitora as métricas da fila, como contagem de mensagens ou comprimento da fila, e escala automaticamente o aplicativo com base nessas métricas.
- Função do IAM para o aplicativo — Nesse padrão, essa função é nomeada`keda-identity`. O `keda-operator` papel assume esse papel. Essa função permite acesso à fila do Amazon SQS.
- Função do IAM para o operador KEDA — Nesse padrão, essa função é nomeada`keda-operator`. O operador KEDA usa essa função para fazer as chamadas de AWS API necessárias. Essa função tem permissões para assumir a `keda-identity` função. Devido à relação de confiança entre as funções `keda-operator` e as `keda-identity` funções, a `keda-operator` função tem permissões do Amazon SQS.

Por meio dos recursos personalizados `TriggerAuthentication` e do `ScaledObject` Kubernetes, o operador usa a `keda-identity` função para se conectar a uma fila do Amazon SQS. Com base no tamanho da fila, o KEDA escala automaticamente a implantação do aplicativo. Ele adiciona 1 pod para cada 5 mensagens não lidas na fila. Na configuração padrão, se não houver mensagens não lidas na fila do Amazon SQS, o aplicativo é reduzido para 0 pods. O operador KEDA monitora a fila em um intervalo especificado por você.

A imagem a seguir mostra como você usa o Amazon EKS Pod Identity para fornecer à `keda-operator` função acesso seguro à fila do Amazon SQS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Você instala o agente Amazon EKS Pod Identity no cluster Amazon EKS.
2. Você implanta o operador KEDA no namespace KEDA no cluster Amazon EKS.
3. Você cria os papéis `keda-operator` e `keda-identity` IAM no alvo Conta da AWS.
4. Você estabelece uma relação de confiança entre as funções do IAM.
5. Você implanta o aplicativo no `security` namespace.
6. O operador KEDA pesquisa mensagens em uma fila do Amazon SQS.

7. O KEDA inicia o HPA, que escala automaticamente o aplicativo com base no tamanho da fila.

Ferramentas

Serviços da AWS

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.

Outras ferramentas

- O KEDA é um autoescalador baseado em eventos baseado em Kubernetes.

Repositório de código

O código desse padrão está disponível no escalonamento GitHub automático orientado por eventos usando o EKS Pod Identity e o repositório KEDA.

Práticas recomendadas

Convém seguir estas práticas recomendadas:

- Melhores práticas do Amazon EKS
- Práticas recomendadas de segurança no IAM
- Melhores práticas do Amazon SQS

Épicos

Crie AWS recursos

Tarefa	Descrição	Habilidades necessárias
Crie a função do IAM para o operador KEDA.	1. Faça login no e AWS Management Console, em seguida, abra o console do IAM. 2. No painel de navegação, selecione Perfis. 3. Escolha Criar Perfil. 4. Selecione o tipo de função Custom trust policy (Política de confiança personali zada). 5. Na seção Política de confiança personalizada, insira a seguinte política de confiança personalizada para essa função: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principa l": { "Service": "pods.eks .amazonaws.com" }, "Action": [`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>"sts:AssumeRole",
	
	"sts:TagSession"
	]
	}
	]
	}</pre>
	6. Na página Adicionar permissões, escolha Próximo. Você não adiciona nenhuma política a essa função.
	7. Em Nome do perfil, insira `keda-operator` .
	8. Escolha Create role (Criar função).	

Tarefa	Descrição	Habilidades necessárias
Crie a função do IAM para o aplicativo de amostra.	1. No console do IAM, selecione Perfis no painel de navegação. 2. Selecione Criar perfil. 3. Selecione o tipo de função Custom trust policy (Política de confiança personali zada). 4. Na seção Política de confiança personali zada, insira a seguinte política de confiança personalizada para essa função. `<account number>` Substitua pelo número da sua conta de destino: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principa l": { "Service": "pods.eks .amazonaws.com", "AWS": "arn:aws:iam::<acc ount number>:role/ keda-operator" }, "Action": [`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>"sts:AssumeRole",
	
	"sts:TagSession"
	]
	}
	]
	}</pre>
	5. Na página Adicionar permissões, adicione as seguintes políticas AWS gerenciadas à função:
	• `AmazonSQSReadOnlyAccess`
	• `AWSLambdaSQSQueueExecutionRole`
	6. Escolha Próximo.
	7. Em Nome do perfil, insira `keda-identity` .
	8. Escolha Create role (Criar função).	

Como criar uma fila do Amazon SQS.	1. Abra o console do Amazon SQS. 2. Selecione Criar fila. 3. Em Tipo, escolha Padrão. 4. Na página Criar fila, em Nome, insira `event-messages-queue` . 5. Selecione Criar fila. Você não altera nenhuma das configurações padrão dessa fila.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie um repositório do Amazon ECR.	1. Abra o console do Amazon ECR. 2. Escolha Criar repositório. 3. Em Nome do repositório, insira `keda-pod-identity-registry` . 4. Escolha Criar repositório. Você não altera nenhuma das configurações padrão desse repositório.	AWS geral

Configurar o cluster Amazon EKS

Tarefa	Descrição	Habilidades necessárias
Implante o agente Amazon EKS Pod Identity.	Para o cluster de destino do Amazon EKS, configure o agente Amazon EKS Pod Identity. Siga as instruções em Configurar o Amazon EKS Pod Identity Agent na documentação do Amazon EKS.	AWS DevOps

Implante o KEDA.	1. Insira os seguintes comandos para implantar o KEDA no cluster de destino do Amazon EKS:
	`# Add Helm Repo for Keda`
	`helm repo add kedacore https://kedacore.github.io/charts`
	`# Update Helm repo`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`helm repo update`
	`# Install Keda`
	`helm install keda kedacore/keda --namespace keda --create-namespace`
	
	Para obter mais informações, consulte Implantando com o Helm na documentação do KEDA.
	2. Após a implantação bem-sucedida, na saída, valide se três implantações foram criadas para o operador KEDA. Veja a seguir um exemplo de saída:
	
	`NAME READY UP-TO-DATE AVAILABLE AGE`
	`keda-admission-webhooks 1/1 1 1 89s`
	`keda-operator 1/1 1 1 89s`
	`keda-operator-metrics-apiserver 1/1 1 1 89s`	

Tarefa	Descrição	Habilidades necessárias
Atribua a função do IAM à conta de serviço do Kubernetes.	Siga as instruções em Atribuir uma função do IAM a uma conta de serviço do Kubernetes na documentação do Amazon EKS. Use os seguintes valores: • Para a função do IAM, insira `keda-operator` . • Para o namespace Kubernetes, insira. `keda` • Para a conta de serviço do Kubernetes, insira. `keda-operator`	AWS DevOps
Crie um namespace .	Insira o comando a seguir para criar um `security` namespace no cluster de destino do Amazon EKS: `kubectl create ns security`	DevOps engenheiro

Implantar o aplicativo de exemplo

Tarefa	Descrição	Habilidades necessárias
Clone os arquivos do aplicativo.	Insira o comando a seguir para clonar o escalonamento automático controlado por eventos usando o EKS Pod Identity e o repositório KEDA em: GitHub	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/aws-samples/event-driven-autoscaling-using-podidentity-and-keda.git`	

Crie a imagem do Docker.	1. Digite o comando a seguir para navegar até o repositório clonado:
	`cd event-driven-autoscaling-using-podidentity-and-keda`
	2. Insira o comando a seguir para criar a imagem do Docker para o aplicativo de amostra:
	`docker build -t keda-pod-identity-registry .`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Envie a imagem do Docker para o Amazon ECR.	1. No terminal em que você criou a imagem do Docker, digite o seguinte comando para fazer login no Amazon ECR. `<AWS_ACCOUNT_ID>` Substitua `<AWS_REGION>` e por valores de seu AWS ambiente:
	`aws ecr get-login-password \ --region <AWS_REGION> | docker login \ --username AWS \ --password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com`
	2. Digite o comando a seguir para marcar a imagem. `<AWS_ACCOUNT_ID>` Substitua `<AWS_REGION>` e por valores de seu AWS ambiente:
	`docker tag keda-pod-identity-registry:latest <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/keda-pod-identity-registry:latest`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	3. Digite o comando a seguir para enviar a imagem para o Amazon ECR. `<AWS_ACCOUNT_ID>` Substitua `<AWS_REGION>` e por valores de seu AWS ambiente: `docker push <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/keda-pod-identity-registry:latest` **Note** Você pode encontrar comandos push navegando até a página do repositório do Amazon ECR e, em seguida, escolhendo Exibir comandos push.	

Tarefa	Descrição	Habilidades necessárias
Implante a aplicação de exemplo.	1. No repositório clonado, abra o arquivo deploy.yaml. 2. <AWS_REGION> Substitua <AWS_ACCOUNT_ID> e por valores de seu ambiente. 3. Salve e feche o arquivo deploy.yaml. 4. Insira o comando a seguir para implantar o aplicativ o de amostra no cluster de destino do Amazon EKS: `kubectl apply -f deploy.yaml` Esse comando cria uma conta de implantação e serviço no cluster.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Atribua a função do IAM à conta de serviço do aplicativo.	Faça o seguinte para associar a função `keda-identity` do IAM à conta de serviço do aplicativo de amostra:
	• Siga as instruções em Atribuir uma função do IAM a uma conta de serviço do Kubernetes na documentação do Amazon EKS. Use os seguintes valores:
	  • Para a função do IAM, insira`keda-identity` .
	  • Para o namespace Kubernetes, insira. `security`
	  • Para a conta de serviço do Kubernetes, insira. `my-sqs-read-msgs`
	• Digite o AWS CLI comando a seguir. `<cluster-name>` Substitua pelo nome do cluster Amazon EKS de destino e `<role-ARN>` substitua pelo Amazon Resource Name (ARN) da `keda-identity` função:
	`aws eks create-pod-identity-association \`
	`  --cluster-name <cluster-name> \`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`--role-arn <role-ARN> \`
	`--namespace security \`
	`--service-account my-sqs-read-msgs`	

Tarefa	Descrição	Habilidades necessárias
Implante `ScaledObject` `TriggerAuthentication` e.	1. No repositório clonado, abra o arquivo keda.yaml. 2. `{{AWS_ACCOUNT_ID}}` Substitua pelo ID do seu alvo Conta da AWS. 3. `{{AWS_REGION}}` Substitua pelo seu alvo Região da AWS. 4. (Opcional) Nas linhas 21 a 24, atualize os parâmetros da política de `ScaledObject` escalabilidade. Consulte o seguinte para obter mais informações sobre esses parâmetros: • Intervalo de pesquisa • Período de resfriamento • idleReplicaCount • minReplicaCount 5. Salve e feche o arquivo keda.yaml. 6. Insira o comando a seguir para implantar os `TriggerAuthentication` recursos `ScaledObject` e: `kubectl -n security apply -f keda.yaml`	DevOps engenheiro

Teste o escalonamento automático

Tarefa	Descrição	Habilidades necessárias

Envie mensagens para a fila do Amazon SQS.	1. Digite o comando a seguir para navegar até o repositório clonado:
	`cd event-driven-autoscaling-using-podidentity-and-keda`
	2. Digite o seguinte comando para enviar mensagens de teste para a fila do Amazon SQS:
	`python sqs_send_msg.py`
	O script sqs_send_msg.py atua como um aplicativo que gera mensagens para testar o escalonamento automático.
	Note
	Se você estiver executando o Python 3, insira. `python3 sqs_send_msg.py`
		DevOps engenheiro

Monitore os pods de aplicativos.	1. Em um terminal diferente, insira o seguinte comando para monitorar os pods:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`kubectl -n security get po`
	2. Para cada 5 mensagens não lidas na fila do Amazon SQS, o KEDA adiciona um pod. Na saída do comando anterior, confirme se novos pods estão sendo adicionados. Veja a seguir um exemplo de saída:
	`kubectl -n security get po`
	`NAME READY STATUS RESTARTS AGE`
	`q-read-797f4c7589-2bj76 1/1 Running 0 2s`
	`q-read-797f4c7589-4zxph 1/1 Running 0 49s`
	`q-read-797f4c7589-cg9dt 1/1 Running 0 18s`
	`q-read-797f4c7589-slc69 1/1 Running 0 33s`
	3. Ao terminar o teste, no terminal original, digite CTRL + C (Windows) ou CMD + C (macOS). Isso	

Tarefa	Descrição	Habilidades necessárias
	interrompe o script python sqs_send_msg.py.	

Solução de problemas

Problema	Solução

O operador KEDA não pode escalar o aplicativo.	Insira o comando a seguir para verificar os registros da função `keda-operator` do IAM:
	`kubectl logs -n keda -l app=keda-operator -c keda-operator`
	
	Se houver um código de `HTTP 403` resposta, o aplicativo e o escalador KEDA não terão permissões suficientes para acessar a fila do Amazon SQS. Execute as etapas a seguir:
	1. Verifique as políticas e declarações do IAM da `keda-identity` função para confirmar se o acesso de leitura da fila foi concedido.
	2. Valide a relação de confiança entre as funções do IAM. Veja um exemplo a seguir:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "pods.eks.amazonaws.com" }, "Action": [ "sts:AssumeRole",`

Problema	Solução

	<pre>"sts:TagSession"
	]
	}
	]
	}</pre>
	Se houver um `Assume-Role` erro, uma função IAM do nó do Amazon EKS não poderá assumir a função do IAM definida para`TriggerAuthentication` . Execute as etapas a seguir:
	1. Digite o comando a seguir para excluir o `keda-operator` pod e criar um novo:
	<pre>kubectl delete pod keda-operator-
	<alphenumeric-value> --namespace
	keda</pre>
	2. Digite o comando a seguir para verificar a identidade que o pod assume:
	<pre>kubectl describe pod <keda-operator-
	pod-name> --namespace keda</pre>
	3. Quando o pod for reiniciado com sucesso, confirme se as duas variáveis a seguir foram adicionadas à descrição do pod:
	• `AWS_CONTAINER_CREDENTIALS_FULL_URI`
	• `AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE`

Recursos relacionados

- Configurar o Amazon EKS Pod Identity Agent (documentação do Amazon EKS)

- Implantando o KEDA (documentação do KEDA)
- ScaledObject especificação (documentação KEDA)
- Autenticação com TriggerAuthentication (documentação KEDA)

Simplifique as implantações do PostgreSQL no Amazon EKS usando o PGO

Criado por Shalaka Dengale (AWS)

Resumo

Esse padrão integra o Postgres Operator da Crunchy Data (PGO) com o Amazon Elastic Kubernetes Service (Amazon EKS) para simplificar as implantações do PostgreSQL em ambientes nativos da nuvem. O PGO fornece automação e escalabilidade para gerenciar bancos de dados PostgreSQL no Kubernetes. Quando você combina o PGO com o Amazon EKS, ele forma uma plataforma robusta para implantar, gerenciar e escalar bancos de dados PostgreSQL de forma eficiente.

Essa integração oferece os seguintes benefícios principais:

- Implantação automatizada: simplifica a implantação e o gerenciamento do cluster PostgreSQL.
- Definições de recursos personalizadas (CRDs): usa primitivas do Kubernetes para gerenciamento do PostgreSQL.
- Alta disponibilidade: suporta failover automático e replicação síncrona.
- Backups e restaurações automatizados: simplifica os processos de backup e restauração.
- Escalonamento horizontal: permite o escalonamento dinâmico dos clusters do PostgreSQL.
- Atualizações de versão: facilita as atualizações contínuas com o mínimo de tempo de inatividade.
- Segurança: aplica criptografia, controles de acesso e mecanismos de autenticação.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Command Line Interface (AWS CLI) versão 2, instalado e configurado no Linux, macOS ou Windows.
- AWS CLI Config, para conectar AWS recursos a partir da linha de comando.
- eksctl, instalado e configurado no Linux, macOS ou Windows.
- `kubectl`, instalado e configurado para acessar recursos em seu cluster Amazon EKS. Para obter mais informações, consulte Configurar kubectl e eksctl na documentação do Amazon EKS.

- Seu terminal de computador configurado para acessar o cluster Amazon EKS. Para obter mais informações, consulte Configurar seu computador para se comunicar com seu cluster na documentação do Amazon EKS.

Versões do produto

- Versões 1.21—1.24 ou posteriores do Kubernetes (consulte a documentação do PGO).
- PostgreSQL versão 10 ou posterior. Esse padrão usa o PostgreSQL versão 16.

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Pilha de tecnologias de destino

- Amazon EKS
- Amazon Virtual Private Cloud (Amazon VPC)
- Nuvem de computação elástica da Amazon (Amazon EC2)

Arquitetura de destino

Esse padrão cria uma arquitetura que contém um cluster Amazon EKS com três nós. Cada nó é executado em um conjunto de EC2 instâncias no back-end. Essa configuração do PostgreSQL segue uma arquitetura de réplica primária, que é particularmente eficaz para casos de uso com muita leitura. A arquitetura inclui os seguintes componentes:

- O contêiner primário do banco de dados (pg-primary) hospeda a instância principal do PostgreSQL para a qual todas as operações de gravação são direcionadas.
- Os contêineres de réplica secundários (pg-replica) hospedam as instâncias do PostgreSQL que replicam os dados do banco de dados primário e manipulam as operações de leitura.

- PgBounceré um agrupador de conexões leve para bancos de dados PostgreSQL incluído no PGO. Ele fica entre o cliente e o servidor PostgreSQL e atua como intermediário para conexões de banco de dados.
- O PGO automatiza a implantação e o gerenciamento de clusters PostgreSQL nesse ambiente Kubernetes.
- O Patroni é uma ferramenta de código aberto que gerencia e automatiza configurações de alta disponibilidade para o PostgreSQL. Está incluído no PGO. Quando você usa o Patroni com o PGO no Kubernetes, ele desempenha um papel crucial para garantir a resiliência e a tolerância a falhas de um cluster PostgreSQL. Para obter mais informações, consulte a documentação do Patroni.

O fluxo de trabalho inclui as seguintes etapas:

- Implante o operador PGO. Você implanta o operador PGO em seu cluster Kubernetes que é executado no Amazon EKS. Isso pode ser feito usando manifestos do Kubernetes ou gráficos do Helm. Esse padrão usa manifestos do Kubernetes.
- Defina instâncias do PostgreSQL. Quando o operador está em execução, você cria recursos personalizados (CRs) para especificar o estado desejado das instâncias do PostgreSQL. Isso inclui configurações como armazenamento, replicação e configurações de alta disponibilidade.
- Gerenciamento de operadores. Você interage com o operador por meio de objetos da Kubernetes API, como CRs criar, atualizar ou excluir instâncias do PostgreSQL.
- Monitoramento e manutenção. Você pode monitorar a integridade e o desempenho das instâncias do PostgreSQL em execução no Amazon EKS. Os operadores geralmente fornecem métricas e registros para fins de monitoramento. Você pode realizar tarefas de manutenção de rotina, como atualizações e correções, conforme necessário. Para obter mais informações, consulte Monitore o desempenho do seu cluster e visualize os registros na documentação do Amazon EKS.
- Dimensionamento e backup: você pode usar os recursos fornecidos pelo operador para escalar instâncias do PostgreSQL e gerenciar backups.

Esse padrão não abrange operações de monitoramento, manutenção e backup.

Automação e escala

- Você pode usar AWS CloudFormation para automatizar a criação da infraestrutura. Para obter mais informações, consulte Criar recursos do Amazon EKS AWS CloudFormation na documentação do Amazon EKS.

- Você pode usar os números GitVersion de compilação do Jenkins para automatizar a implantação de instâncias de banco de dados.

Ferramentas

Serviços da AWS

- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.

Outras ferramentas

- eksctl é uma ferramenta de linha de comando simples para criar clusters no Amazon EKS.
- O Kubectl: é um utilitário de linha de comando para executar comandos em clusters do Kubernetes.
- O PGO automatiza e dimensiona o gerenciamento de bancos de dados PostgreSQL no Kubernetes.

Práticas recomendadas

Siga estas melhores práticas para garantir uma implantação tranquila e eficiente:

- Proteja seu cluster EKS. Implemente as melhores práticas de segurança para seu cluster EKS, como usar funções AWS Identity and Access Management (IAM) para contas de serviço (IRSA), políticas de rede e grupos de segurança de VPC. Limite o acesso ao servidor da API do cluster EKS e criptografe as comunicações entre os nós e o servidor da API usando o TLS.
- Garanta a compatibilidade de versões entre o PGO e o Kubernetes em execução no Amazon EKS. Alguns recursos do PGO podem exigir versões específicas do Kubernetes ou introduzir limitações de compatibilidade. Para obter mais informações, consulte Componentes e compatibilidade na documentação do PGO.
- Planeje a alocação de recursos para sua implantação de PGO, incluindo CPU, memória e armazenamento. Considere os requisitos de recursos do PGO e das instâncias do PostgreSQL que ele gerencia. Monitore o uso de recursos e escale os recursos conforme necessário.

- Design para alta disponibilidade. Projete sua implantação de PGO para alta disponibilidade para minimizar o tempo de inatividade e garantir a confiabilidade. Implante várias réplicas do PGO em várias zonas de disponibilidade para tolerância a falhas.
- Implemente procedimentos de backup e restauração para seus bancos de dados PostgreSQL gerenciados pelo PGO. Use recursos fornecidos pelo PGO ou soluções de backup de terceiros que sejam compatíveis com o Kubernetes e o Amazon EKS.
- Configure o monitoramento e o registro para sua implantação de PGO para monitorar o desempenho, a integridade e os eventos. Use ferramentas como o Prometheus para monitorar métricas e o Grafana para visualização. Configure o registro para capturar registros do PGO para solução de problemas e auditoria.
- Configure a rede adequadamente para permitir a comunicação entre PGO, instâncias do PostgreSQL e outros serviços em seu cluster Kubernetes. Use os recursos de rede Amazon VPC e plug-ins de rede Kubernetes, como Calico ou Amazon VPC CNI, para aplicação de políticas de rede e isolamento de tráfego.
- Escolha as opções de armazenamento apropriadas para seus bancos de dados PostgreSQL, considerando fatores como desempenho, durabilidade e escalabilidade. Use volumes do Amazon Elastic Block Store (Amazon EBS) AWS ou serviços de armazenamento gerenciado para armazenamento persistente. Para obter mais informações, consulte Armazenar volumes do Kubernetes com o Amazon EBS na documentação do Amazon EKS.
- Use ferramentas de infraestrutura como código (IaC), como AWS CloudFormation para automatizar a implantação e a configuração do PGO no Amazon EKS. Defina os componentes da infraestrutura, incluindo o cluster EKS, a rede e os recursos do PGO, como código para consistência, repetibilidade e controle de versão.

Épicos

Criar um perfil do IAM

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM.	1. Crie uma função do IAM usando o seguinte comando no AWS CLI: `aws iam create-role \`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`--role-name {YourRoleName} \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "eks.amazonaws.com" }, "Action": "sts:AssumeRole" }] }' && \ aws iam attach-role-policy \ --role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy && \ aws iam attach-role-policy \ --role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/AmazonEKSServicePolicy && \ aws iam attach-role-policy \`	

Tarefa	Descrição	Habilidades necessárias

	`--role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/CloudWatchFullAccess`
	2. Analise a função em AWS Management Console:
	a. Abra o console do IAM.
	b. Escolha Funções e pesquise o nome da função que você criou.
	c. Valide se as seguintes políticas estão anexadas:
	`AmazonEKSClusterPolicy`
	`AmazonEKSServicePolicy`
	`CloudWatchFullAccess`	

Criar um cluster do Amazon EKS.

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do Amazon EKS.	Se você já implantou um cluster, pule esta etapa. Caso contrário, implante um cluster Amazon EKS em seu cluster atual Conta da AWS usando `eksctl` Terraform ou AWS CloudFormation. Esse	Administrador da AWS, administrador do Terraform ou eksctl, administrador do Kubernetes

Tarefa	Descrição	Habilidades necessárias

	padrão é usado `eksctl` para implantação de clusters.
	
	Note
	Esse padrão usa a Amazon EC2 como um grupo de nós para o Amazon EKS. Se você quiser usar AWS Fargate, consulte a `managedNodeGroups` configuração na documentação do eksctl.
	
	1. Use o arquivo `eksctl` de entrada a seguir para gerar o cluster.
	
	`sample-cluster.yaml`:
	
	`apiVersion: eksctl.io/v1alpha5`
	`kind: ClusterConfig`
	`metadata:`
	`  name: postgresql`
	`  region: us-east-1`
	`  version: "1.29"`
	`accessConfig:`
	`  authenticationMode: API_AND_CONFIG_MAP`
	`availabilityZones:`
	`- us-east-1a`
	`- us-east-1b`	

Tarefa	Descrição	Habilidades necessárias

	<pre>- us-east-1c
	nodeGroups:
	  - name: ng-1
	    instanceType:
	 m5.16xlarge
	    desiredCapacity:
	 2
	  - name: ng-2
	    instanceType:
	 m5.16xlarge
	    desiredCapacity:
	 2
	  - name: ng-3
	    instanceType:
	 m5.16xlarge
	    desiredCapacity:
	 2
	vpc:
	  cidr: 192.168.0
	.0/16
	  clusterEndpoints:
	    publicAccess:
	 true
	  nat:
	    gateway: HighlyAva
	ilable
	iamIdentity
	Mappings:
	  - arn: arn:aws:i
	am::<account-id>:r
	ole/<role-name> #
	 update the IAM role
	 ARN created in step 1
	    username: <user-
	name> # Enter the
	 user name per your
	 choice
	    noDuplicateARNs:
	 false</pre>
	2. Execute o comando a seguir para criar o cluster	

Tarefa	Descrição	Habilidades necessárias
	(forneça o caminho `sample-cluster.yaml` do arquivo): `eksctl create cluster -f sample-cluster.yaml`	
Valide o status do cluster.	Execute o comando a seguir para ver o status atual dos nós no cluster: `kubectl get nodes` Se você encontrar erros, consulte a seção de solução de problemas da documentação do Amazon EKS.	Administrador da AWS, administrador do Terraform ou eksctl, administrador do Kubernetes

Crie um provedor de identidade OIDC

Tarefa	Descrição	Habilidades necessárias
Ative o provedor IAM OIDC.	Como pré-requisito para o driver Amazon EBS Container Storage Interface (CSI), você deve ter um provedor do IAM OpenID Connect (OIDC) existente para seu cluster. Ative o provedor IAM OIDC usando o seguinte comando: `eksctl utils associate -iam-oidc-provider`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`--region={region} --cluster={YourClusterNameHere} --approve` Para obter mais informações sobre essa etapa, consulte a documentação do Amazon EKS.	

Tarefa	Descrição	Habilidades necessárias
Crie uma função do IAM para o driver CSI do Amazon EBS.	Use o `eksctl` comando a seguir para criar a função do IAM para o driver CSI: `eksctl create iamservic eaccount \ --region {RegionName} \ --name ebs-csi-c ontroller-sa \ --namespace kube-syst em \ --cluster {YourClus terNameHere} \ --attach-policy-ar n arn:aws:iam::aws:p olicy/service-role /AmazonEBSCSIDrive rPolicy \ --approve \ --role-only \ --role-name AmazonEKS _EBS_CSI_DriverRole` Se você usa unidades criptografadas do Amazon EBS, precisa configurar ainda mais a política. Para obter instruções, consulte a documentação do driver SCI do Amazon EBS.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Adicione o driver CSI do Amazon EBS.	Use o `eksctl` comando a seguir para adicionar o driver CSI do Amazon EBS: `eksctl create addon \ --name aws-ebs-csi-driver \ --cluster <YourClusterName> service-account-role-arn arn:aws:iam::$(aws sts get-caller-identity \ --query Account \ --output text):role/AmazonEKS_EBS_CSI_DriverRole \ --force`	Administrador da AWS

Instale o PGO

Tarefa	Descrição	Habilidades necessárias
Clone o repositório PGO.	Clone o GitHub repositório para PGO: `git clone https://github.com/CrunchyData/postgres-operator-examples.git`	AWS DevOps
Forneça os detalhes da função para a criação da conta de serviço.	Para conceder ao cluster do Amazon EKS acesso aos AWS recursos necessários, especifique o Amazon Resource Name (ARN) da função do OIDC que	Administrador da AWS, administrador do Kubernetes

Tarefa	Descrição	Habilidades necessárias

	você criou anteriormente no arquivo. `service_account.yaml` Esse arquivo está localizado na pasta de namespace do repositório.
	
	`cd postgres-operator-examples`
	
	`--- metadata: annotations: eks.amazonaws.com/role-arn: arn:aws:iam::<accountId>:role/<role_name> # Update the OIDC role ARN created earlier`	

Tarefa	Descrição	Habilidades necessárias

Crie o namespace e os pré-requisitos do PGO.	1. Execute o comando a seguir para criar o namespace :
	`kubectl apply -k kustomize/install/namespace`
	Isso estabelece um namespace dedicado para o PGO. Se necessário, você pode modificar o `namespace.yml` arquivo e atribuir um nome diferente ao namespace.
	2. Execute o comando a seguir para aplicar a configuração padrão ao cluster:
	`kubectl apply --server-side -k kustomize/install/default`
	`kustomize/install/default` fornece a configuração padrão para os arquivos de controle de acesso baseado em função (RBAC), definição de recursos personalizados (CRD) e Kubernetes Manager.
		Administrador do Kunernetes

Tarefa	Descrição	Habilidades necessárias
Verifique a criação dos pods.	Verifique se o namespace e a configuração padrão foram criados: `kubectl get pods -n postgres-operator`	Administrador da AWS, administrador do Kubernetes
Verificar PVCs.	Use o comando a seguir para verificar as declarações de volume persistentes (PVCs): `kubectl describe pvc -n postgres-operator`	Administrador da AWS, administrador do Kubernetes

Crie e implante um operador

Tarefa	Descrição	Habilidades necessárias

Crie um operador.	Revise o conteúdo do arquivo localizado em `/kustomize/postgres/postgres.yaml` para que corresponda ao seguinte:
	`spec:`
	`  instances:`
	`  - name: pg-1`
	`  replicas: 3`
	`  patroni:`
	`  dynamicConfiguration:`
	`  postgresql:`
	`  pg_hba:`
	`  - "host all all 0.0.0.0/0 trust"`
	`  # this line enabled`
		Administrador da AWS, DBA, administrador do Kubernetes

Tarefa	Descrição	Habilidades necessárias

	<pre>logical replication
	with programmatic
	access
	- "host all
	postgres 127.0.0.1/32
	md5"
	synchronous_mode:
	true
	users:
	- name: replicator
	databases:
	- testdb
	options: "REPLICAT
	ION"</pre>
	Essas atualizações fazem o seguinte:
	• Ajuste as configurações do PostgreSQL para facilitar o acesso à instância do PostgreSQL.
	• Inclua configurações para usuário de replicação, usuário do banco de dados e superusuário para permitir a replicação de streaming , o acesso ao banco de dados e o gerenciamento de clusters.	

Tarefa	Descrição	Habilidades necessárias
Implante o operador.	Implante o operador PGO para permitir o gerenciam ento e a operação simplific ados dos bancos de dados PostgreSQL em ambientes Kubernetes: `kubectl apply -k kustomize/postgres`	Administrador da AWS, DBA, administrador do Kubernetes

Verificar a implantação.	1. Valide se o operador foi implantado:
	`kubectl get pods -n postgres-operator --selector=postgres-operator.crunchydata.com/instance-set \ -L postgres-operator.crunchydata.com/role`
	2. Verifique se o recurso de serviço associado ao pod do operador foi criado:
	`kubectl get svc -n postgres-operator`
	Na saída do comando, observe a réplica primária (`primary_pod_name`) e a réplica de leitura (`read_pod_name`). Você os usará nas próximas etapas.
		Administrador da AWS, DBA, administrador do Kubernetes

Verifique a replicação de streaming

Tarefa	Descrição	Habilidades necessárias

Grave dados na réplica primária.	Use os comandos a seguir para se conectar à réplica primária do PostgreSQL e gravar dados no banco de dados:
	`kubectl exec -it <primary_pod_name> bash -n postgres-operator`
	`psql`
	`CREATE TABLE customers (firstname text, customer_id serial, date_created timestamp );`
	`\dt`
		Administrador da AWS, administrador do Kubernetes

Confirme se a réplica de leitura tem os mesmos dados.	Conecte-se à réplica de leitura do PostgreSQL e verifique se a replicação de streaming está funcionando corretamente:
	`kubectl exec -it {read_pod_name} bash -n postgres-operator`
	`psql`
	`\dt`
		Administrador da AWS, administrador do Kubernetes

Tarefa	Descrição	Habilidades necessárias
	A réplica de leitura deve ter a tabela que você criou na réplica primária na etapa anterior.	

Solução de problemas

Problema	Solução

A cápsula não liga.	• Use o comando a seguir para inspecionar o status do pod:
	`kubectl get pods -n your-namespace`
	• Inspecione os registros em busca de erros:
	`kubectl logs your-pod-name -n your-namespace`
	• Verifique se há eventos anormais relacionados aos seus pods:
	`kubectl describe pod your-pod-name -n your-namespace`

As réplicas estão significativamente atrasadas em relação ao banco de dados principal.	• Verifique o atraso na replicação:
	`SELECT * FROM pg_stat_replication;`
	• Certifique-se de que as réplicas tenham recursos suficientes de CPU e memória. Verifique os limites de recursos:
	`kubectl describe pod your-replica-pod -n your-namespace`

Problema	Solução
	• Verifique se o back-end de armazenam ento está funcionando de maneira ideal. A E/S lenta do disco pode causar atraso na replicação.
Você não tem visibilidade do desempenho e da integridade do cluster PostgreSQL.	• Ative o Amazon CloudWatch Logs e certifiqu e-se de que os registros estejam sendo enviados para a Amazon CloudWatch para análise. Para obter mais informações, consulte a documentação do Amazon EKS. • Confira **`pg_stat_activity`** : `SELECT * FROM pg_stat_activity;`

Problema	Solução

A replicação não funciona.	• Verifique a configuração primária visualizando as configurações de replicação em: `postgresql.conf`
	`wal_level = replica`
	`max_wal_senders = 10`
	`wal_keep_size = 64  # or wal_keep_segments in older versions`
	• Verifique se isso `pg_hba.conf` inclui permissões de replicação:
	`host replication replica_user all md5`
	• Verifique a configuração da réplica. Verifique se as configurações `recovery.conf` ou configurações equivalentes (`standby.signal` e `primary_conninfo`) estão definidas corretamente nas réplicas.

Recursos relacionados

- Amazon Elastic Kubernetes Service (visão geral das opções de implantação no whitepaper da AWS)
- AWS CloudFormation(Visão geral das opções de implantação no whitepaper da AWS)
- Comece a usar o Amazon EKS — eksctl (Guia do usuário do Amazon EKS)
- Configurar kubectl e eksctl (Guia do usuário do Amazon EKS)
- Crie uma função para a federação do OpenID Connect (Guia do usuário do IAM)
- Definindo as configurações do AWS CLI (Guia AWS CLI do usuário)
- Documentação do Crunchy Postgres para Kubernetes

- Crunch & Learn: Crunchy Postgres para Kubernetes 5.0 (vídeo)

Simplifique a autenticação de aplicativos com TLS mútuo no Amazon ECS usando o Application Load Balancer

Criado por Olawale Olaleye (AWS) e Shamanth Devagari (AWS)

Resumo

Esse padrão ajuda você a simplificar a autenticação do seu aplicativo e aliviar os encargos de segurança com o TLS mútuo no Amazon Elastic Container Service (Amazon ECS) usando o Application Load Balancer (ALB). Com o ALB, você pode autenticar certificados de cliente X.509 do. AWS Private Certificate Authority Essa combinação poderosa ajuda a obter uma comunicação segura entre seus serviços, reduzindo a necessidade de mecanismos complexos de autenticação em seus aplicativos. Além disso, o padrão usa o Amazon Elastic Container Registry (Amazon ECR) para armazenar imagens de contêineres.

O exemplo desse padrão usa imagens do Docker de uma galeria pública para criar inicialmente as cargas de trabalho de amostra. Posteriormente, novas imagens do Docker são criadas para serem armazenadas no Amazon ECR. Para a fonte, considere um sistema baseado em Git GitHub, como, ou Bitbucket GitLab, ou use o Amazon Simple Storage Service Amazon S3 (Amazon S3). Para criar as imagens do Docker, considere usar AWS CodeBuild para as imagens subsequentes.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS com acesso para implantar AWS CloudFormation pilhas. Verifique se você tem permissões de usuário ou função AWS Identity and Access Management (IAM) para implantar CloudFormation.
- AWS Command Line Interface (AWS CLI) instalado. Configure suas AWS credenciais em sua máquina local ou em seu ambiente usando AWS CLI ou definindo as variáveis de ambiente no `~/.aws/credentials` arquivo.
- OpenSSL instalado.
- Docker instalado.
- Familiaridade com o Serviços da AWS descrito em Ferramentas.
- Conhecimento de Docker e NGINX.

Limitações

- O TLS mútuo para Application Load Balancer suporta somente certificados de cliente X.509v3. Não há suporte para certificados de cliente X.509v1.
- O CloudFormation modelo fornecido no repositório de código desse padrão não inclui o provisionamento de um CodeBuild projeto como parte da pilha.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- Docker versão 27.3.1 ou posterior
- AWS CLI versão 2.14.5 ou posterior

Arquitetura

O diagrama a seguir mostra os componentes da arquitetura desse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. Crie um repositório Git e confirme o código do aplicativo no repositório.
2. Crie uma autoridade de certificação (CA) privada em AWS Private CA.
3. Crie um CodeBuild projeto. O CodeBuildproject é acionado por alterações de confirmação e cria a imagem do Docker e publica a imagem criada no Amazon ECR.
4. Copie a cadeia de certificados e o corpo do certificado da CA e faça o upload do pacote de certificados para o Amazon S3.
5. Crie um armazenamento confiável com o pacote CA que você enviou para o Amazon S3. Associe o armazenamento confiável aos ouvintes TLS mútuos no Application Load Balancer (ALB).
6. Use a CA privada para emitir certificados de cliente para as cargas de trabalho do contêiner. Crie também um certificado TLS privado usando o. AWS Private CA
7. Importe o certificado TLS privado para AWS Certificate Manager (ACM) e use-o com o ALB.
8. A carga de trabalho do contêiner `ServiceTwo` usa o certificado de cliente emitido para se autenticar com o ALB quando ele se comunica com a carga de trabalho do contêiner em. `ServiceOne`

9. A carga de trabalho do contêiner `Service0ne` usa o certificado de cliente emitido para se autenticar com o ALB quando ele se comunica com a carga de trabalho do contêiner em. `ServiceTwo`

Automação e escala

Esse padrão pode ser totalmente automatizado usando CloudFormation AWS Cloud Development Kit (AWS CDK) , ou operações de API de um SDK para provisionar os AWS recursos.

Você pode usar AWS CodePipeline para implementar um pipeline de integração contínua e implantação contínua (CI/CD) usando CodeBuild para automatizar o processo de criação de imagens de contêineres e implantar novas versões nos serviços de cluster do Amazon ECS.

Ferramentas

Serviços da AWS

- AWS Certificate Manager (ACM) ajuda você a criar, armazenar e renovar certificados e chaves SSL/TLS X.509 públicos e privados que protegem seus sites e aplicativos. AWS
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido para executar, parar e gerenciar contêineres em um cluster. Você pode executar suas tarefas e serviços em uma infraestrutura sem servidor gerenciada pela. AWS Fargate Como alternativa, para ter mais controle sobre sua infraestrutura, você pode executar suas tarefas e serviços em um cluster de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que você gerencia.
- O Amazon ECS Exec permite que você interaja diretamente com os contêineres sem precisar primeiro interagir com o sistema operacional do contêiner hospedeiro, abrir portas de entrada ou gerenciar chaves SSH. Você pode usar o ECS Exec para executar comandos ou obter um shell para um contêiner em execução em uma EC2 instância da Amazon ou em. AWS Fargate
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre EC2 instâncias, contêineres

e endereços IP da Amazon em uma ou mais zonas de disponibilidade. O ELB monitora a integridade de seus alvos registrados e direciona o tráfego somente para os alvos saudáveis. O ELB dimensiona seu balanceador de carga à medida que o tráfego de entrada muda com o tempo. Ele pode ser escalado automaticamente para a maioria das cargas de trabalho.

- AWS Fargateajuda você a executar contêineres sem precisar gerenciar servidores ou EC2 instâncias da Amazon. O Fargate é compatível com o Amazon ECS e o Amazon Elastic Kubernetes Service (Amazon EKS). Você pode executar suas tarefas e serviços do Amazon ECS com o tipo de lançamento do Fargate ou com um provedor de capacidade do Fargate. Para fazer isso, empacote seu aplicativo em contêineres, especifique os requisitos de CPU e memória, defina políticas de rede e IAM e inicie o aplicativo. Cada tarefa do Fargate tem seu próprio limite de isolamento e não compartilha o kernel subjacente, os recursos de CPU, os recursos de memória nem a interface de rede elástica com outra tarefa.
- AWS Private Certificate Authoritypermite a criação de hierarquias de autoridade de certificação (CA) privada, incluindo raiz e subordinada CAs, sem os custos de investimento e manutenção da operação de uma CA local.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- GitHub, GitLab, e o Bitbucket são alguns dos sistemas de controle de código-fonte baseados em Git comumente usados para acompanhar as alterações no código-fonte.
- O NGINX Open Source é um balanceador de carga, cache de conteúdo e servidor web de código aberto. Esse padrão o usa como um servidor web.
- O OpenSSL é uma biblioteca de código aberto que fornece serviços usados pelas implementações do OpenSSL de TLS e CMS.

Repositório de código

O código desse padrão está disponível no repositório GitHub MTLS-with-Application-Load-Balancer-in-Amazon-ECS.

Práticas recomendadas

- Use o Amazon ECS Exec para executar comandos ou transferir um shell para um contêiner em execução no Fargate. Você também pode usar o ECS Exec para ajudar a coletar informações de diagnóstico para depuração.
- Use grupos de segurança e listas de controle de acesso à rede (ACLs) para controlar o tráfego de entrada e saída entre os serviços. As tarefas do Fargate recebem um endereço IP da sub-rede configurada em sua nuvem privada virtual (VPC).

Épicos

Crie o repositório

Tarefa	Descrição	Habilidades necessárias
Baixe o código-fonte.	Para baixar o código-fonte desse padrão, bifurque ou clone o repositório GitHub MTLS-with-application-load-Balancer-in-Amazon-ECS.	DevOps engenheiro
Crie um repositório Git.	Para criar um repositório Git para conter o Dockerfile e os `buildspec.yaml` arquivos, use as seguintes etapas: 1. Crie uma pasta em seu ambiente virtual. Nomeie com o nome do seu projeto. 2. Abra um terminal em sua máquina local e navegue até essa pasta. 3. Para clonar o repositório MTLS-with-application-load-balancer-in-Amazon-ECS no diretório do seu projeto, digite o seguinte comando:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/aws-samples/mTLS-with-Application-Load-Balancer-in-Amazon-ECS.git`	

Crie CA e gere certificados

Tarefa	Descrição	Habilidades necessárias
Crie uma CA privada em AWS Private CA.	Para criar uma autoridade de certificação (CA) privada, execute os seguintes comandos em seu terminal. Substitua os valores nas variáveis de exemplo pelos seus próprios valores. `export AWS_DEFAULT_REGION="us-west-2"` `export SERVICES_DOMAIN="www.example.com"` `export ROOT_CA_ARN=`aws acm-pca create-certificate-authority \` `--certificate-authority-type ROOT \` `--certificate-authority-configuration \` `"KeyAlgorithm=RSA_2048,` `SigningAlgorithm=SHA256WITHRSA,`	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	``
	    Subject={
	        Country=US,
	        State=WA,
	        Locality=
	Seattle,
	        Organizat
	ion=Build on AWS,
	        Organizat
	ionalUnit=mTLS Amazon
	 ECS and ALB Example,
	        CommonName=
	${SERVICES_DOMAIN}}" \
	        --query
	 CertificateAuthori
	tyArn --output text`
	``
	Para obter mais detalhes, consulte Criar uma CA privada AWS Private CA na AWS documentação.	

Tarefa	Descrição	Habilidades necessárias
Crie e instale seu certificado CA privado.	Para criar e instalar um certificado para sua CA raiz privada, execute os seguintes comandos em seu terminal: 1. Gere uma solicitação de assinatura de certificado (CSR). ``` ROOT_CA_CSR=`aws acm-pca get-certificate-authority-csr \     --certificate-authority-arn ${ROOT_CA_ARN} \     --query Csr --output text` ``` 2. Emita o certificado raiz. ``` AWS_CLI_VERSION=$(aws --version 2>&1 | cut -d/ -f2 | cut -d. -f1) [[${AWS_CLI_VERSION} -gt 1]] && ROOT_CA_CSR="$(echo ${ROOT_CA_CSR} | base64)" ROOT_CA_CERT_ARN=`aws acm-pca issue-certificate \ --certificate-authority-arn ${ROOT_CA_ARN} \ --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \ ```	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`--signing-algorithm SHA256WITHRSA \` `--validity Value=10,Type=YEARS \` `--csr "${ROOT_CA_CSR}" \` `--query CertificateArn --output text` 3. Recupere o certificado raiz. `ROOT_CA_CERT=`aws acm-pca get-certificate \` `--certificate-arn ${ROOT_CA_CERT_ARN} \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--query Certificate --output text`  `# store for later use` `aws acm-pca get-certificate \` `--certificate-arn ${ROOT_CA_CERT_ARN} \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--query Certificate --output text > ca-cert.pem` 4. Importe o certificado CA raiz para instalá-lo na CA.	

Tarefa	Descrição	Habilidades necessárias

	`[[ ${AWS_CLI_VERSION} -gt 1 ]] && ROOT_CA_CERT="$(echo ${ROOT_CA_CERT} | base64)"`
	
	`aws acm-pca import-certificate-authority-certificate \`
	`  --certificate-authority-arn ${ROOT_CA_ARN} \`
	`  --certificate "${ROOT_CA_CERT}"`
	
	Para obter mais detalhes, consulte Instalando o certificado CA na AWS documentação.	

Solicite um certificado gerenciado.	Para solicitar um certificado privado AWS Certificate Manager para uso com seu ALB privado, use o seguinte comando: `export TLS_CERTIFICATE_ARN=`aws acm request-certificate \` ` --domain-name "*.${DOMAIN_DOMAIN}" \` ` --certificate-authority-arn ${ROOT_CA_ARN} \` ` --query CertificateArn --output text``	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Use a CA privada para emitir um certificado de cliente.	• Para criar uma solicitação de assinatura de certificado (CSR) para os dois serviços, use o seguinte AWS CLI comando:
	
	`openssl req -out client_csr1.pem -new -newkey rsa:2048 -nodes -keyout client_private-key 1.pem`
	
	`openssl req -out client_csr2.pem -new -newkey rsa:2048 -nodes -keyout client_private-key 2.pem`
	
	Esse comando retorna a CSR e a chave privada dos dois serviços.
	
	• Para emitir um certificado para os serviços, execute os seguintes comandos para usar a CA privada que você criou:
	
	`SERVICE_ONE_CERT_ARN=`aws acm-pca issue-certificate \`
		DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`--certificate-authority-arn ${ROOT_CA_ARN} \` `--csr fileb://client_csr1.pem \` `--signing-algorithm "SHA256WITHRSA" \` `--validity Value=5,Type="YEARS" --query CertificateArn --output text` `echo "SERVICE_ONE_CERT_ARN: ${SERVICE_ONE_CERT_ARN}"` `aws acm-pca get-certificate \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--certificate-arn ${SERVICE_ONE_CERT_ARN} \` `| jq -r '.Certificate' > client_cert1.cert` `SERVICE_TWO_CERT_ARN=`aws acm-pca issue-certificate \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--csr fileb://client_csr2.pem \` `--signing-algorithm "SHA256WITHRSA" \` `--validity Value=5,Type="YEARS" --query CertificateArn --output text`	

Tarefa	Descrição	Habilidades necessárias

	``
	echo "SERVICE_TWO_CERT_
	ARN: ${SERVICE
	_TWO_CERT_ARN}"
	
	aws acm-pca get-certi
	ficate \
	    --certificate-auth
	ority-arn ${ROOT_CA
	_ARN} \
	    --certificate-arn
	 ${SERVICE_TWO_CERT
	_ARN} \
	     | jq -r '.Certifi
	cate' > client_ce
	rt2.cert
	``
	
	Para obter mais informações, consulte Emitir certificados privados de entidades finais na AWS documentação.	

Provisione serviços da AWS

Tarefa	Descrição	Habilidades necessárias
Provisão Serviços da AWS com o CloudFormation modelo.	Para provisionar a nuvem privada virtual (VPC), o cluster Amazon ECS, os serviços do Amazon ECS, o Application Load Balancer e o Amazon Elastic Container Registry (Amazon ECR), use o modelo. CloudFormation	DevOps engenheiro
Obtenha variáveis.	Verifique se você tem um cluster do Amazon ECS com	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	dois serviços em execução. Para recuperar os detalhes do recurso e armazená-los como variáveis, use os seguintes comandos:
	
	`export LoadBalancerDNS=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`LoadBalancerDNS`].OutputValue')`
	
	`export ECRRepositoryUri=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`ECRRepositoryUri`].OutputValue')`
	
	`export ECRRepositoryServiceOneUri=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`ECRRepositoryServiceOneUri`].OutputValue')`	

Tarefa	Descrição	Habilidades necessárias
	export ECRReposi toryServiceTwoUri= $(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputK ey==`ECRRepository ServiceTwoUri`].Ou tputValue') export ClusterName= $(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputK ey==`ClusterName`] .OutputValue') export BucketName= $(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputK ey==`BucketName`]. OutputValue') export Service1L istenerArn=$(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputK ey==`Service1Liste	

Tarefa	Descrição	Habilidades necessárias
	nerArn`].OutputVal ue')  export Service2L istenerArn=$(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`Service2Liste nerArn`].OutputVal ue')	

Tarefa	Descrição	Habilidades necessárias
Crie um CodeBuild projeto.	Para usar um CodeBuild projeto para criar as imagens do Docker para seus serviços do Amazon ECS, faça o seguinte: 1. Faça login no e abra AWS Management Console o CodeBuild console em https://console.aws.amazon.com/codesuite/codebuild/. 2. Criar um novo projeto da . Em Source, escolha o repositório Git que você criou. Para obter informações sobre os diferentes tipos de integração do repositório Git, consulte Trabalho com conexões na documentação. AWS 3. Confirme se o modo Privilegiado está ativado. Para criar imagens do Docker, esse modo é necessário. Caso contrário, a imagem não será criada com êxito. 4. Use o `buildspec.yaml` arquivo personalizado compartilhado para cada serviço.	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	5. Forneça valores para o nome e a descrição do projeto. Para obter mais detalhes, consulte Criar um projeto de compilação AWS CodeBuild na AWS documentação.	

Tarefa	Descrição	Habilidades necessárias

Crie as imagens do Docker.	Você pode usar CodeBuild para realizar o processo de criação da imagem. CodeBuild precisa de permissões para interagir com o Amazon ECR e trabalhar com o Amazon S3.
	
	Como parte do processo, a imagem do Docker é criada e enviada para o registro do Amazon ECR. Para obter detalhes sobre o modelo e o código, consulte Informações adicionais.
	
	(Opcional) Para criar localmente para fins de teste, use o seguinte comando:
	
	`# login to ECR`
	`aws ecr get-login`
	`-password | docker`
	`login --username`
	`AWS --password-stdin`
	`$ECRRepositoryUri`
	
	`# build image for`
	`service one`
	`cd /service1`
	`aws s3 cp s3://$Buc`
	`ketName/serviceone/`
	`service1/ --recursive`
	`docker build -t`
	`$ECRRepositoryServ`
	`iceOneUri .`
	`docker push $ECRRepos`
	`itoryServiceOneUri`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`# build image for service two`
	`cd ../service2`
	`aws s3 cp s3://$BucketName/servicetwo/service2/ --recursive`
	`docker build -t $ECRRepositoryServiceTwoUri .`
	`docker push $ECRRepositoryServiceTwoUri`	

Habilitar TLS mútuo

Tarefa	Descrição	Habilidades necessárias
Faça o upload do certificado CA para o Amazon S3.	Para fazer o upload do certificado CA para o bucket do Amazon S3, use o seguinte exemplo de comando: `aws s3 cp ca-cert.pem s3://$BucketName/acm-trust-store/`	AWS DevOps, DevOps engenheiro
Crie o repositório confiável.	Para criar o armazenamento confiável, use o comando de exemplo a seguir: `TrustStoreArn=`aws elbv2 create-trust-store --name acm-pca-trust-certs \` `--ca-certificates-bundle-s3-bucket $BucketName \` `--ca-certificates-bundle-s3-key acm-`	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`trust-store/ca-cert.pem --query 'TrustStores[].TrustStoreArn' --output text``	

Faça upload dos certificados do cliente.	Para fazer upload de certificados de cliente para o Amazon S3 para imagens do Docker, use o seguinte exemplo de comando:
	`# for service one`
	`aws s3 cp client_cert1.cert s3://$BucketName/serviceone/`
	`aws s3 cp client_private-key1.pem s3://$BucketName/serviceone/`
	
	`# for service two`
	`aws s3 cp client_cert2.cert s3://$BucketName/servicetwo/`
	`aws s3 cp client_private-key2.pem s3://$BucketName/servicetwo/`
		AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Modifique o ouvinte.	Para habilitar o TLS mútuo no ALB, modifique os ouvintes HTTPS usando os seguintes comandos:
	
	`aws elbv2 modify-listener \`
	`  --listener-arn $Service1ListenerArn \`
	`  --certificates CertificateArn=$TLS_CERTIFICATE_ARN_TWO \`
	`  --ssl-policy ELBSecurityPolicy-2016-08 \`
	`  --protocol HTTPS \`
	`  --port 8080 \`
	`  --mutual-authentication Mode=verify,TrustStoreArn=$TrustStoreArn,IgnoreClientCertificateExpiry=false`
	
	`aws elbv2 modify-listener \`
	`  --listener-arn $Service2ListenerArn \`
	`  --certificates CertificateArn=$TLS_CERTIFICATE_ARN_TWO \`
	`  --ssl-policy ELBSecurityPolicy-2016-08 \`
	`  --protocol HTTPS \`
	`  --port 8090 \`
		AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`--mutual-authentication Mode=verify,TrustStoreArn=$TrustStoreArn,IgnoreClientCertificateExpiry=false` Para obter mais informações, consulte Como configurar o TLS mútuo em um Application Load Balancer na documentação. AWS	

Atualize os serviços

Tarefa	Descrição	Habilidades necessárias
Atualize a definição da tarefa do Amazon ECS.	Para atualizar a definição da tarefa do Amazon ECS, modifique o `image` parâmetro na nova revisão. Para obter os valores dos respectivos serviços, atualize as definições de tarefas com o novo Uri de imagens do Docker que você criou nas etapas anteriores: `echo $ECRRepositoryServiceOneUri` ou `echo $ECRRepositoryServiceTwoUri` `"containerDefinitions": [`	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	"name":
	"nginx",
	"image":
	"public.ecr.aws/ng
	inx/nginx:latest",
	# <----- change to new
	Uri
	"cpu": 0,</pre>
	Para obter mais informações, consulte Atualização de uma definição de tarefa do Amazon ECS usando o console na AWS documentação.	

Tarefa	Descrição	Habilidades necessárias
Atualize o serviço Amazon ECS.	Atualize o serviço com a definição de tarefa mais recente. Essa definição de tarefa é o modelo para as imagens recém-criadas do Docker e contém o certificado do cliente necessário para a autenticação TLS mútua. Para atualizar o serviço, use o procedimento a seguir: 1. Abra o console do Amazon ECS na https://console.aws.amazon.com/ecs/v2. 2. Na página Clusters, escolha o cluster. 3. Na página de detalhes do cluster, na seção Serviços, marque a caixa de seleção ao lado do serviço e escolha Atualizar. 4. Para que seu serviço inicie uma nova implantação, selecione Force new deployment (Forçar nova implantação). 5. Em Definição da tarefa, escolha a família de definição da tarefa e a revisão mais recente. 6. Selecione Atualizar.	Administrador da AWS, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Repita as etapas para o outro serviço.	

Acessar a aplicação

Tarefa	Descrição	Habilidades necessárias
Copie o URL do aplicativo.	Use o console do Amazon ECS para visualizar a tarefa. Quando o status da tarefa for atualizado para Em execução, selecione a tarefa. Na seção Tarefa, copie o ID da tarefa.	Administrador da AWS, AWS DevOps

Testar seu aplicativo	Para testar seu aplicativo, use o ECS Exec para acessar as tarefas.
	1. Para o serviço 1, use o seguinte comando:
	`container="nginx"`
	`ECS_EXEC_TASK_ARN="<TASK ARN>"`
	`aws ecs execute-command --cluster $ClusterName \ --task $ECS_EXEC_TASK_ARN \ --container $container \ --interactive \ --command "/bin/bash"`
	2. No contêiner da tarefa do serviço um, use o comando
		Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	a seguir para inserir o balanceador de carga interno `url` e a porta do ouvinte que aponta para o serviço dois. Em seguida, especifique o caminho para o certificado do cliente para testar o aplicativo:
	
	`curl -kvs https://<internal-alb-url>:8090 --key /usr/local/share/ca-certificates/client.key --cert /usr/local/share/ca-certificates/client.crt`
	
	3. No contêiner da tarefa do serviço dois, use o comando a seguir para inserir o balanceador de carga interno `url` e a porta do ouvinte que aponta para o serviço um. Em seguida, especifique o caminho para o certificado do cliente para testar o aplicativo:
	
	`curl -kvs https://<internal-alb-url>:8080 --key /usr/local/share/ca-certificates/client.key --cert /usr/local/share/ca-certificates/client.crt`	

Tarefa	Descrição	Habilidades necessárias
	Note O `-k` sinalizador nos comandos curl (como parte de`-kvs`) desativa a validação do certificado SSL. Você pode remover esse sinalizador ao usar um certificado SSL que correspon da ao seu nome de domínio, permitind o a validação adequada do certificado.	

Recursos relacionados

Documentação do Amazon ECS

- Criação de uma definição de tarefa do Amazon ECS usando o console
- Criação de uma imagem de contêiner para uso no Amazon ECS
- Clusters do Amazon ECS
- Amazon ECS para AWS Fargate
- Melhores práticas de rede do Amazon ECS
- Parâmetros de definição de serviço do Amazon ECS

Outros AWS recursos

- Como uso a CA AWS privada para configurar o mTLS no Application Load Balancer? (AWS re:Post)

Mais informações

Editando o Dockerfile

O código a seguir mostra os comandos que você edita no Dockerfile para o serviço 1:

```
FROM public.ecr.aws/nginx/nginx:latest
WORKDIR /usr/share/nginx/html
RUN echo "Returning response from Service 1: Ok" > /usr/share/nginx/html/index.html
ADD client_cert1.cert client_private-key1.pem /usr/local/share/ca-certificates/
RUN chmod -R 400 /usr/local/share/ca-certificates/
```

O código a seguir mostra os comandos que você edita no Dockerfile para o serviço 2:

```
FROM public.ecr.aws/nginx/nginx:latest
WORKDIR /usr/share/nginx/html
RUN echo "Returning response from Service 2: Ok" > /usr/share/nginx/html/index.html
ADD client_cert2.cert client_private-key2.pem /usr/local/share/ca-certificates/
RUN chmod -R 400 /usr/local/share/ca-certificates/
```

Se você estiver criando as imagens do Docker com CodeBuild, o `buildspec` arquivo usa o número da CodeBuild compilação para identificar de forma exclusiva as versões da imagem como um valor de tag. Você pode alterar o `buildspec` arquivo para atender às suas necessidades, conforme mostrado no código `buildspec` personalizado a seguir:

```
version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws ecr get-login-password --region $AWS_DEFAULT_REGION | docker login --
username AWS --password-stdin $ECR_REPOSITORY_URI
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=${COMMIT_HASH:=latest}
  build:
    commands:
        # change the S3 path depending on the service
```

```
      - aws s3 cp s3://$YOUR_S3_BUCKET_NAME/serviceone/ $CodeBuild_SRC_DIR/ --
recursive
      - echo Build started on `date`
      - echo Building the Docker image...
      - docker build -t $ECR_REPOSITORY_URI:latest .
      - docker tag $ECR_REPOSITORY_URI:latest $ECR_REPOSITORY_URI:$IMAGE_TAG
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $ECR_REPOSITORY_URI:latest
      - docker push $ECR_REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      # for ECS deployment reference
      - printf '[{"name":"%s","imageUri":"%s"}]' $CONTAINER_NAME $ECR_REPOSITORY_URI:
$IMAGE_TAG > imagedefinitions.json

artifacts:
  files:
    - imagedefinitions.json
```

Mais padrões

- Avaliar a prontidão do aplicativo para migração para a Nuvem AWS usando o CAST Highlight
- Automatize a exclusão de AWS CloudFormation pilhas e recursos associados
- Automatize o gerenciamento dinâmico de pipelines para implantar soluções de hotfix em ambientes Gitflow usando e AWS Service CatalogAWS CodePipeline
- Compile automaticamente pipelines de CI/CD e clusters do Amazon ECS para microsserviços usando o AWS CDK
- Crie e envie imagens do Docker para o Amazon ECR usando GitHub Actions e Terraform
- Containerize workloads de mainframe que foram modernizadas pela Blu Age
- Crie um analisador de log personalizado para o Amazon ECS usando um roteador de log Firelens
- Implementar um pipeline de CI/CD para microsserviços Java no Amazon ECS
- Implante um cluster Amazon EKS a partir do AWS Cloud9 usando um perfil de instância EC2
- Implante um ambiente para aplicativos Blu Age conteinerizados usando o Terraform
- Implante a lógica de pré-processamento em um modelo de ML em um único endpoint usando um pipeline de inferência na Amazon SageMaker
- Gerencie implantações azul/verdes de microsserviços em várias contas e regiões usando os serviços de código da AWS e as chaves multirregionais do AWS KMS
- Gerencie aplicativos de contêineres on-premises configurando o Amazon ECS Anywhere com o AWS CDK
- Migre da Oracle GlassFish para o AWS Elastic Beanstalk
- Migre do Oracle WebLogic para o Apache Tomcat (TomEE) no Amazon ECS
- Configure um espaço de dados mínimo viável para compartilhar dados entre organizações
- Modernize aplicativos ASP.NET Web Forms na AWS
- Monitore os repositórios do Amazon ECR para obter permissões curinga usando o AWS e o AWS Config CloudFormation
- Monitore a atividade do aplicativo usando o CloudWatch Logs Insights
- Configure um pipeline de CI/CD para cargas de trabalho híbridas no Amazon ECS Anywhere usando o AWS CDK e GitLab
- Configurar um repositório de chart do Helm v3 no Amazon S3
- Configure a end-to-end criptografia para aplicativos no Amazon EKS usando cert-manager e Let's Encrypt

- Simplifique a implantação de aplicativos multilocatários do Amazon EKS usando o Flux
- Simplifique os fluxos de trabalho de aprendizado de máquina, do desenvolvimento local aos experimentos escaláveis, usando SageMaker IA e Hydra
- Estruture um projeto Python em arquitetura hexagonal usando o AWS Lambda
- Teste a AWS infraestrutura usando LocalStack e Terraform Tests
- Treine e implante um modelo de ML personalizado compatível com GPU na Amazon SageMaker
- Coordene a dependência de recursos e a execução de tarefas usando a AWS Fargate WaitCondition construção de gancho
- Use agentes do Amazon Bedrock para automatizar a criação de controles de entrada de acesso no Amazon EKS por meio de prompts baseados em texto

Sem servidor

Tópicos

- Crie um aplicativo móvel React Native de tecnologia sem servidor usando o AWS Amplify
- Gerenciar locatários em vários produtos de SaaS em um único ambiente de gerenciamento
- Crie uma EventBridge conexão entre contas da Amazon em uma organização
- Entregue registros do DynamoDB para o Amazon S3 usando o Kinesis Data Streams e o Firehose com AWS CDK
- Implemente o controle de versão de API baseado em caminhos usando domínios personalizados no Amazon API Gateway
- Importe a biblioteca psycopg2 para interagir com seu banco AWS Lambda de dados PostgreSQL
- Integre o Amazon API Gateway com o Amazon SQS para lidar com REST assíncrono APIs
- Processe eventos de forma assíncrona com o Amazon API Gateway e o AWS Lambda
- Processe eventos de forma assíncrona com o Amazon API Gateway e o Amazon DynamoDB Streams
- Processe eventos de forma assíncrona com o Amazon API Gateway, o Amazon SQS e o AWS Fargate
- Execute tarefas do AWS Systems Manager Automation de forma síncrona a partir do AWS Step Functions
- Execute leituras paralelas de objetos do S3 usando Python em uma função AWS Lambda
- Envie dados de telemetria de AWS Lambda para OpenSearch para análise e visualização em tempo real
- Configure um roteador celular sem servidor para uma arquitetura baseada em células
- Configure o acesso privado a um bucket do Amazon S3 por meio de um endpoint VPC
- Solucione problemas de estados AWS Step Functions usando o Amazon Bedrock
- Reúna os serviços da AWS usando uma abordagem de tecnologia sem servidor
- Mais padrões

Crie um aplicativo móvel React Native de tecnologia sem servidor usando o AWS Amplify

Criado por Deekshitulu Pentakota (AWS)

Resumo

Esse padrão mostra como criar um backend de tecnologia sem servidor para um aplicativo móvel React Native usando o AWS Amplify e os seguintes serviços da AWS:

- AWS AppSync
- Amazon Cognito
- Amazon DynamoDB

Depois de configurar e implantar o backend do aplicativo usando o Amplify, o Amazon Cognito autentica os usuários do aplicativo e os autoriza a acessar o aplicativo. AppSync Em seguida, a AWS interage com o aplicativo de front-end e com uma tabela de back-end do DynamoDB para criar e buscar dados.

> **Note**
>
> Esse padrão usa um aplicativo “ToDoList” simples como exemplo, mas você pode usar um procedimento semelhante para criar qualquer aplicativo móvel React Native.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Amplify Command Line Interface (Amplify CLI), instalada e configurada
- XCode (qualquer versão)
- Microsoft Visual Studio (qualquer versão, qualquer editor de código, qualquer editor de texto)
- Familiaridade com o Amplify
- Familiaridade com o Amazon Cognito
- Familiaridade com a AWS AppSync

- Familiaridade com o DynamoDB
- Familiaridade com Node.js
- Familiaridade com o npm
- Familiaridade com React e React Native
- Familiaridade com JavaScript e (ECMAScript 6) ES6
- Familiaridade com o GraphQL

Arquitetura

O diagrama a seguir mostra um exemplo de arquitetura para executar o backend de um aplicativo móvel React Native na Nuvem AWS:

O diagrama mostra a seguinte arquitetura:

1. O Amazon Cognito autentica os usuários do aplicativo e os autoriza a acessar o aplicativo.
2. Para criar e buscar dados, a AWS AppSync usa uma API GraphQL para interagir com o aplicativo de front-end e uma tabela de back-end do DynamoDB.

Ferramentas

Serviços da AWS

- O AWS Amplify é um conjunto de ferramentas e recursos desenvolvidos especificamente para permitir aos desenvolvedores de frontend para a web e dispositivos móveis criarem aplicações de pilha completa de forma rápida e fácil na AWS.
- AppSyncA AWS fornece uma interface GraphQL escalável que ajuda os desenvolvedores de aplicativos a combinar dados de várias fontes, incluindo Amazon DynamoDB, AWS Lambda e HTTP. APIs
- O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para suas aplicações Web e móveis.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.

Código

O código do aplicativo de amostra usado nesse padrão está disponível no ios-todo-app repositório GitHub aws-amplify-react-native-. Para usar os arquivos de amostra, siga as instruções na seção Épicos desse padrão.

Épicos

Crie e execute seu aplicativo React Native

Tarefa	Descrição	Habilidades necessárias
Configurar um ambiente de desenvolvimento React Native.	Para obter instruções, consulte Configurando o ambiente de desenvolvimento na documentação do React Native.	Desenvolvedor de aplicativos

Crie e execute o aplicativo móvel ToDoList React Native no iOS Simulator.	1. Crie um novo diretório de projeto de aplicativo móvel React Native em seu ambiente local executando o seguinte comando em uma nova janela de terminal:
	`npx react-native init ToDoListAmplify`
	2. Navegue até o diretório raiz do projeto executando o seguinte comando:
	`cd ToDoListAmplify`
	3. Execute o aplicativo executando o seguinte comando:
	`npx react-native run-ios`
		Desenvolvedor de aplicativos

Inicializar um ambiente de backend para a aplicação

Tarefa	Descrição	Habilidades necessárias

Crie os serviços de backend necessários para oferecer suporte ao aplicativo no Amplify.	1. Em seu ambiente local, execute o seguinte comando no diretório raiz do projeto (ToDoListAmplify):
	`amplify init`
	2. É exibido um prompt solicitando que você forneça informações sobre o aplicativo. Insira as informações necessárias com base no seu caso de uso. Depois, pressione Enter.
	
	Para a configuração do ToDoList aplicativo usada nesse padrão, aplique o exemplo de configuração a seguir.
	
	Exemplo de configurações do aplicativo React Native Amplify
	`? Name: ToDoListAmplify`
	`? Environment: dev`
	`? Default editor: Visual Studio Code`
	`? App type: javascript`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	``` ? Javascript framework : react-native ? Source Directory Path: src ? Distribution Directory Path: / ? Build Command: npm run-script build ? Start Command: npm run-script start ? Select the authentic ation method you want to use: AWS profile ? Please choose the profile you want to use: default ```	
	Para obter mais informaçõ es, consulte Criar um novo backend do Amplify na documentação do Amplify Dev Center.	
	Note O `amplify init` comando provisiona os seguintes recursos usando a AWS CloudFormation:	

Tarefa	Descrição	Habilidades necessárias
	• Funções do AWS Identity and Access Managemen t (IAM) para usuários autenticados e não autenticados (Auth Role e Unauth Role) • Um bucket do Amazon Simple Storage Service (Amazon S3) para implantaç ão (para o aplicativo de exemplo desse padrão, Amplify-meta.json) • Um ambiente de backend no Amplify Hosting	

Adicione a autenticação do Amazon Cognito ao seu aplicativo Amplify React Native

Tarefa	Descrição	Habilidades necessárias
Crie um serviço de autentica ção do Amazon Cognito.	1. Em seu ambiente local, execute o seguinte comando no diretório raiz do projeto (ToDoListA mplify): `amplify add auth` 2. É exibido um prompt solicitando que você forneça informações sobre as configurações do serviço de autenticação. Insira as informações necessárias com base no seu caso de	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	uso. Depois, pressione Enter.
	
	Para a configuração do ToDoList aplicativo usada nesse padrão, aplique o exemplo de configuração a seguir.
	
	Exemplo de configurações do serviço de autenticação
	
	`? Do you want to use the default authentication and security configuration? \`
	`Default configuration`
	
	`? How do you want users to be able to sign in? \`
	`Username`
	
	`? Do you want to configure advanced settings? \`
	`No, I am done`
	
	Note
	O `amplify add auth` comando cria as pastas, arquivos e arquivos de dependência necessários em uma pasta local (amplify)	

Tarefa	Descrição	Habilidades necessárias
	dentro do diretório raiz do projeto. Para a configuração do ToDoList aplicativo usada nesse padrão, o aws-exports.js é criado para essa finalidade.	

Implante o serviço do Amazon Cognito na Nuvem AWS.	1. No diretório raiz do projeto, execute o seguinte comando Amplify CLI:
	`amplify push`
	2. Uma solicitação para confirmar a implantação é exibida. Digite Sim. Depois, pressione Enter.
	Note
	Para ver os serviços implantados em seu projeto, acesse o console do Amplify executando o seguinte comando:
	`amplify console`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Instale as bibliotecas Amplify necessárias para o React Native e as CocoaPods dependências para iOS.	1. Instale as bibliotecas de cliente de código aberto do Amplify necessárias executando o seguinte comando no diretório raiz do projeto:
	`npm install aws-amplify aws-amplify-react-native \ amazon-cognito-identity-js @react-native-community/netinfo \ @react-native-async-storage/async-storage`
	2. Instale as CocoaPods dependências necessárias para iOS executando o seguinte comando:
	`npx pod-install`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Importe e configure o serviço Amplify.	No arquivo de ponto de entrada do aplicativo (por exemplo, App.js), importe e carregue o arquivo de configuração do serviço Amplify inserindo as seguintes linhas de código:
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	Note
	Se você receber um erro após importar o serviço Amplify no arquivo de ponto de entrada do aplicativo, interrompa o aplicativo. Em seguida, abra XCode e selecione ToDoListAmplifyo.xcworkspace na pasta iOS do projeto e execute o aplicativo.
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Atualize o arquivo de ponto de entrada do seu aplicativo para usar o componente withAuthenticator Higher-Order (HOC).	**Note** O `withAuthenticator` HOC fornece fluxos de trabalho de login, inscrição e esquecimento de senhas em seu aplicativo usando apenas algumas linhas de código. Para obter mais informações, consulte Opção 1: usar componentes de interface de usuário pré-criados no Amplify Dev Center. Além disso, componentes de ordem superior na documentação do React. 1. No arquivo de ponto de entrada do aplicativo (por exemplo, App.js), importe o HOC `withAuthenticator` inserindo as seguintes linhas de código: `import { withAuthenticator } from 'aws-amplify-react-native'`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	2. Exporte o HOC WithAuthenticator inserindo o seguinte código:
	
	`export default withAuthenticator(App)`
	
	Exemplo de código HOC WithAuthenticator
	
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	`import { withAuthenticator } from 'aws-amplify-react-native';`
	
	`const App = () => {`
	`  return null;`
	`};`
	
	`export default withAuthenticator(App);`
	
	Note
	No simulador iOS, o aplicativo mostra a tela de login fornecida	

Tarefa	Descrição	Habilidades necessárias
	pelo serviço Amazon Cognito.	
Teste a configuração do serviço de autenticação.	No iOS Simulator, faça o seguinte: 1. Crie uma nova conta no aplicativo usando um endereço de e-mail real. Um código de verificação é então enviado para o e-mail registrado. 2. Verifique a conta configurada usando o código que você recebe no e-mail de verificação. 3. Insira o nome e a senha de usuário do que você criou. Em seguida, escolha Entrar. Uma tela de boas-vindas é exibida. **Note** Você também pode abrir o console do Amazon Cognito e verificar se um novo usuário foi criado no Identity Pool ou não.	Desenvolvedor de aplicativos

Conecte uma AppSync API da AWS e um banco de dados do DynamoDB ao aplicativo

Tarefa	Descrição	Habilidades necessárias
Crie uma AppSync API da AWS e um banco de dados do DynamoDB.	1. Adicione uma AppSync API da AWS ao seu aplicativo e provisione automaticamente um banco de dados do DynamoDB executando o seguinte comando da CLI do Amplify a partir do diretório raiz do projeto: `amplify add api` 2. É exibido um prompt solicitando que você forneça informações sobre as configurações da API e do banco de dados. Insira as informações necessárias com base no seu caso de uso. Depois, pressione Enter. A CLI do Amplify abre o arquivo do esquema GraphQL em seu editor de texto. Para a configuração do ToDoList aplicativo usada nesse padrão, aplique o exemplo de configuração a seguir. Exemplo de configurações de API e banco de dados	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	? Please select from one of the below mentioned services: \ GraphQL ? Provide API name: todolistamplify ? Choose the default authorization type for the API \ Amazon Cognito User Pool Do you want to use the default authentication and security configura tion ? Default configuration How do you want users to be able to sign in? \ Username Do you want to configure advanced settings? \ No, I am done. ? Do you want to configure advanced settings for the GraphQL API \ No, I am done. ? Do you have an annotated GraphQL schema? \ No ? Choose a schema template: \	

Tarefa	Descrição	Habilidades necessárias

	Single object with fields (e.g., “Todo” with ID, name, description)
	
	? Do you want to edit the schema now? \
	Yes
	
	Exemplo de esquema GraphQL
	
	type Todo @model {
	id: ID!
	name: String!
	description: String
	}	

Tarefa	Descrição	Habilidades necessárias
Implante a AppSync API da AWS.	1. No diretório raiz do projeto, execute o seguinte comando Amplify CLI: `amplify push` 2. É exibido um prompt solicitando que você forneça mais informações sobre as configurações da API e do banco de dados. Insira as informações necessárias com base no seu caso de uso. Depois, pressione Enter. Agora, seu aplicativo pode interagir com a AppSync API da AWS. Para a configuração do ToDoList aplicativo usada nesse padrão, aplique o exemplo de configuração a seguir. Exemplo de configurações AppSync da API da AWS **Note** A configuração a seguir cria a API GraphQL na AWS AppSync e uma tabela Todo no Dynamo DB.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	? Are you sure you want to continue? Yes ? Do you want to generate code for your newly created GraphQL API Yes ? Choose the code generation language target javascript ? Enter the file name pattern of graphql queries, mutations and subscriptions src/graphql/**/*.js ? Do you want to generate/update all possible GraphQL operations - \ queries, mutations and subscriptions Yes ? Enter maximum statement depth \ [increase from default if your schema is deeply nested] 2	

Tarefa	Descrição	Habilidades necessárias
Conecte o front-end do aplicativo à AppSync API da AWS.	Para usar o ToDoList aplicativo de exemplo fornecido nesse padrão, copie o código do arquivo App.js no ios-todo-app GitHub repositório aws-amplify-react-native-. Em seguida, integre o código de exemplo em seu ambiente local. O código de exemplo fornecido no arquivo App.js do repositório faz o seguinte: • Mostra o formulário para criar um ToDo item com os campos Título e Descrição • Exibe a lista de itens pendentes (Título e Descrição) • Publica e busca dados usando métodos `aws-amplify`	Desenvolvedor de aplicativos

Recursos relacionados

- AWS Amplify
- Amazon Cognito
- AWS AppSync
- Amazon DynamoDB
- React (documentação do React)

Gerenciar locatários em vários produtos de SaaS em um único ambiente de gerenciamento

Criado por Ramanna Avancha (AWS), Jenifer Pascal (AWS), Kishan Kavala (AWS) e Anusha Mandava (AWS)

Resumo

Esse padrão mostra como gerenciar os ciclos de vida dos inquilinos em vários produtos de software como serviço (SaaS) em um único ambiente de gerenciamento na Nuvem AWS. A arquitetura de referência fornecida pode ajudar as organizações a reduzir a implementação de recursos redundantes e compartilhados em seus produtos SaaS individuais e fornecer eficiências de governança em grande escala.

Grandes empresas podem ter vários produtos SaaS em várias unidades de negócios. Esses produtos geralmente precisam ser provisionados para uso por locatários externos em diferentes níveis de assinatura. Sem uma solução comum para locatários, os administradores de TI devem gastar tempo gerenciando recursos indiferenciados em vários SaaS APIs, em vez de se concentrarem no desenvolvimento dos principais recursos do produto.

A solução comum para locatários fornecida nesse padrão pode ajudar a centralizar o gerenciamento de muitos dos recursos compartilhados do produto SaaS de uma organização, incluindo o seguinte:

- Segurança
- Provisionamento de locatários
- Armazenamento de dados do locatário
- Comunicações do locatário
- Gerenciamento de produtos
- Registro em log e monitoramento de métricas

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Conhecimento do Amazon Cognito ou de um provedor de identidades (IdP) terceirizado

- Conhecimento do Amazon API Gateway
- Conhecimento do AWS Lambda
- Conhecimento do Amazon DynamoDB
- Conhecimento do AWS Identity and Access Management (IAM)
- Conhecimento do AWS Step Functions
- Conhecimento da AWS CloudTrail e da Amazon CloudWatch
- Conhecimento de bibliotecas e códigos Python
- Conhecimento de SaaS APIs, incluindo os diferentes tipos de usuários (organizações, locatários, administradores e usuários de aplicativos), modelos de assinatura e modelos de isolamento de inquilinos
- Conhecimento dos requisitos de SaaS de vários produtos e das assinaturas de vários locatários de sua organização

Limitações

- As integrações entre a solução de locatário comum e os produtos SaaS individuais não são abordadas nesse padrão.
- Esse padrão implanta o serviço Amazon Cognito somente em uma única região da AWS.

Arquitetura

Pilha de tecnologias de destino

- Amazon API Gateway
- Amazon Cognito
- AWS CloudTrail
- Amazon CloudWatch
- Amazon DynamoDB
- IAM
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Notification Service (Amazon SNS)

- AWS Step Functions

Arquitetura de destino

O diagrama a seguir mostra um exemplo de fluxo de trabalho para gerenciar os ciclos de vida dos locatários em vários produtos SaaS em um único ambiente de gerenciamento na Nuvem AWS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário da AWS inicia o provisionamento de locatários, o provisionamento de produtos ou ações relacionadas à administração fazendo uma chamada para um endpoint do API Gateway.
2. O usuário é autenticado por um token de acesso restaurado de um grupo de usuários do Amazon Cognito ou de outro IdP.
3. As tarefas individuais de provisionamento ou administração são executadas por funções do Lambda que são integradas aos endpoints da API Gateway API.
4. A administração da solução comum APIs para inquilinos (para inquilinos, produtos e usuários) reúne todos os parâmetros de entrada, cabeçalhos e tokens necessários. Em seguida, a administração APIs invoca as funções Lambda associadas.
5. As permissões do IAM para as funções de administração APIs e do Lambda são validadas pelo serviço IAM.
6. As funções do Lambda armazenam e recuperam dados dos catálogos (para locatários, produtos e usuários) no DynamoDB e no Amazon S3.
7. Depois que as permissões são validadas, um fluxo de trabalho do AWS Step Functions é invocado para realizar uma tarefa específica. O exemplo no diagrama mostra um fluxo de trabalho de provisionamento de locatários.
8. As tarefas individuais do fluxo de trabalho do AWS Step Functions são executadas em um fluxo de trabalho predeterminado (máquina de estado).
9. Todos os dados essenciais necessários para executar a função do Lambda associada a cada tarefa de fluxo de trabalho são recuperados do DynamoDB ou do Amazon S3. Outros recursos da AWS talvez precisem ser provisionados usando um modelo da AWS CloudFormation .
10. Se necessário, o fluxo de trabalho envia uma solicitação para provisionar recursos adicionais da AWS para um produto SaaS específico para a conta da AWS desse produto.
11. Quando a solicitação é bem-sucedida ou falha, o fluxo de trabalho publica a atualização de status como uma mensagem para um tópico do Amazon SNS.

12. O Amazon SNS está inscrito no tópico do Amazon SNS do fluxo de trabalho Step Functions.
13. Em seguida, o Amazon SNS envia a atualização do status do fluxo de trabalho para o usuário da AWS.
14. Os registros das ações de cada serviço da AWS, incluindo uma trilha de auditoria das chamadas de API, são enviados para CloudWatch. Regras e alarmes específicos podem ser configurados CloudWatch para cada caso de uso.
15. Os logs são arquivados em buckets do Amazon S3 para fins de auditoria.

Automação e escala

Esse padrão usa um CloudFormation modelo para ajudar a automatizar a implantação da solução comum para locatários. O modelo também pode ajudá-lo a aumentar ou reduzir rapidamente os recursos associados.

Para obter mais informações, consulte Como trabalhar com CloudFormation modelos da AWS no Guia CloudFormation do usuário da AWS.

Ferramentas

Serviços da AWS

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para suas aplicações Web e móveis.
- CloudTrailA AWS ajuda você a auditar a governança, a conformidade e o risco operacional da sua conta da AWS.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando

necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O AWS Step Functions é um serviço de orquestração com tecnologia sem servidor que permite combinar funções do AWS Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios.

Práticas recomendadas

A solução nesse padrão usa um único ambiente de gerenciamento para gerenciar a integração de vários locatários e fornecer acesso a vários produtos SaaS. O ambiente de gerenciamento ajuda os usuários administrativos a gerenciar outros quatro ambientes específicos de atributos:

- Plano de segurança
- Plano de fluxo de trabalho
- Plano de comunicação
- Registro e ambiente de monitoramento

Épicos

Configurar o plano de segurança

Tarefa	Descrição	Habilidades necessárias
Estabeleça os requisitos para sua plataforma SaaS multilocatária.	Estabeleça requisitos detalhados para: • Locatários • Usuários • Perfis • Produtos de SaaS	Arquiteto de nuvem, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	• Assinaturas • Trocas de perfis	
Configurar o serviço do Amazon Cognito.	Siga as instruções em Introdução ao Amazon Cognito no Guia do Desenvolvedor do Amazon Cognito.	Arquiteto de nuvem
Configure as políticas do IAM necessárias.	Crie as políticas do IAM necessárias para o seu caso de uso. Em seguida, mapeie as políticas para funções do IAM no Amazon Cognito. Para obter mais informações, consulte Gerenciamento de acesso usando políticas e Controle de acesso baseado em funções no Guia do Desenvolvedor do Amazon Cognito.	Administrador de nuvem, arquiteto de nuvem, segurança do AWS IAM

Tarefa	Descrição	Habilidades necessárias
Configure as permissões de API necessárias.	Configure as permissões de acesso ao API Gateway usando perfis e políticas do IAM e autorizadores do Lambda. Para obter instruções, consulte as seguintes seções do Guia do Desenvolvedor do Amazon API Gateway: • Controlar o acesso a uma API com permissões do IAM • Usar os autorizadores do API Gateway Lambda	Administrador de nuvem, arquiteto de nuvem

Configurar o plano de dados

Tarefa	Descrição	Habilidades necessárias
Crie os catálogos de dados necessários.	1. Crie tabelas do DynamoDB para armazenar dados para os catálogos de usuários. Certifique-se de incluir atributos e funções do usuário. Além disso, certifique-se de realizar a modelagem de dados nas tabelas do catálogo para manter os atributos obrigatórios e opcionais para cada usuário e função. 2. Crie tabelas do DynamoDB para armazenar dados para	DBA

Tarefa	Descrição	Habilidades necessárias
	os catálogos de produtos. Certifique-se de modelar os casos de uso específicos para seus produtos SaaS. 3. Crie tabelas do DynamoDB para armazenar dados para os catálogos de locatários. Certifique-se de configura r modelos de assinatura para locatários, produtos e licenciamento para assinaturas e tags de vários SaaS. Para obter mais informaçõ es, consulte Configuração do DynamoDB no Guia do desenvolvedor Amazon DynamoDB.	

Configurar o ambiente de gerenciamento

Tarefa	Descrição	Habilidades necessárias
Crie funções Lambda e API Gateway APIs para executar as tarefas necessárias do plano de controle.	Crie funções Lambda e API Gateway separados APIs para adicionar, excluir e gerenciar o seguinte: • Usuários • Locatários • Produtos	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es, consulte Como usar o AWS Lambda com o Amazon API Gateway no Guia do desenvolvedor do AWS Lambda.	

Configurar o plano do fluxo de trabalho

Tarefa	Descrição	Habilidades necessárias
Identifique as tarefas que os fluxos de trabalho do AWS Step Functions devem executar.	Identifique e documente os requisitos detalhados do fluxo de trabalho do AWS Step Functions para o seguinte: • Usuários • Locatários • Produtos **Important** Certifique-se de que as principais partes interessadas aprovem os requisitos.	Proprietário do App
Crie os fluxos de trabalho necessários do AWS Step Functions.	1. Crie os fluxos de trabalho necessários para usuários, locatários e produtos no AWS Step Functions. Para obter mais informaçõ es, consulte o Guia do	Desenvolvedor de aplicativos, líder de criação

Tarefa	Descrição	Habilidades necessárias
	desenvolvedor do AWS Step Functions. 2. Identifique os mecanismos de repetição e tratamento de erros. Para obter mais informações, consulte Tratamento de erros, novas tentativas e adição de alertas a Step Function State Machines no blog da AWS. 3. Implemente as etapas do fluxo de trabalho usando as funções do Lambda. Para instruções, consulte Criação de uma máquina de estado Step Functions que usa o Lambda no Guia do desenvolvedor do AWS Step Functions. 4. Integre quaisquer serviços externos com o AWS Step Functions conforme necessário. 5. Mantenha o status de cada fluxo de trabalho em uma tabela do DynamoDB e comunique o status de cada fluxo de trabalho usando o Amazon SNS.	

Configurar o plano de comunicação

Tarefa	Descrição	Habilidades necessárias
Crie tópicos do Amazon SNS.	Crie tópicos do Amazon SNS para receber notificações sobre: • Status do fluxo de trabalho • Erros • Repetições Para obter mais informações, consulte Criar um tópico do SNS no Guia do desenvolvedor do Amazon SNS.	Proprietário do aplicativo, arquiteto de nuvem
Assine endpoints em cada tópico do Amazon SNS.	Para receber mensagens publicadas em um tópico do Amazon SNS, você precisa inscrever um endpoint em cada tópico. Para obter instruções, consulte Assinatura de um tópico do Amazon SNS no Guia do desenvolvedor do Amazon SNS.	Desenvolvedor de aplicativos, arquiteto de nuvem

Configurar o plano de registro em log e monitoramento

Tarefa	Descrição	Habilidades necessárias
Ative o registro para cada componente da solução comum de locatário.	Ative o registro no nível do componente para cada recurso na solução de	Desenvolvedor de aplicativos, administrador de sistemas da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	locatário comum que você criou. Para instruções, consulte: • Como faço para ativar CloudWatch os registros para solucionar problemas com minha API REST ou WebSocket API do API Gateway? (Centro de Conhecimentos da AWS) • Registro usando CloudWatch registros (Guia do desenvolvedor do AWS Step Functions) • Registro de funções do AWS Lambda em Python (Guia do Desenvolvedor do AWS Lambda) • Registro e monitoramento no Amazon Cognito ((Guia do Desenvolvedor do Amazon Cognito) • Monitoramento com a Amazon CloudWatch (Amazon DynamoDB Developer Guide) **Note** Você pode consolidar os registros de cada recurso em uma	

Tarefa	Descrição	Habilidades necessárias
	conta de registro centralizada usando as políticas do IAM. Para obter mais informações, consulte Registro centralizado e barreiras de proteção de várias contas.	

Provisione e implante a solução comum para locatários

Tarefa	Descrição	Habilidades necessárias
Crie CloudFormation modelos.	Automatize a implantação e a manutenção da solução de locatário comum completa e de todos os seus componentes usando CloudFormation modelos. Para obter mais informações, consulte o Guia CloudFormation do usuário da AWS.	Desenvolvedor de aplicativos, DevOps engenheiro, CloudFormation desenvolvedor

Recursos relacionados

- Controlar o acesso a uma API REST usando um grupo de usuários do Amazon Cognito como autorizador (Guia do desenvolvedor do Amazon API Gateway)
- Use autorizadores Lambda do API Gateway ((Guia do Desenvolvedor do Amazon API Gateway)
- Grupos de usuários do Amazon Cognito (Guia do Desenvolvedor do Amazon Cognito)
- CloudWatch Console entre contas e regiões (Guia do CloudWatch usuário da Amazon)

Crie uma EventBridge conexão entre contas da Amazon em uma organização

Criado por Sam Wilson (AWS) e Robert Stone (AWS)

Resumo

Grandes sistemas distribuídos usam EventBridge a Amazon para comunicar mudanças de estado entre várias contas da Amazon Web Services (AWS) em uma AWS Organizations organização. No entanto, geralmente EventBridge é capaz de atingir apenas endpoints ou consumidores no mesmo Conta da AWS. A exceção é um ônibus de eventos em uma conta diferente. Esse barramento de eventos é um alvo válido. Para consumir eventos de um barramento de eventos em outra conta, os eventos devem ser enviados do barramento de eventos da conta de origem para o barramento de eventos da conta de destino. Para evitar desafios ao gerenciar eventos críticos em aplicativos diferentes Contas da AWS, use a abordagem recomendada apresentada nesse padrão.

Esse padrão ilustra como implementar uma arquitetura orientada a eventos EventBridge que envolva vários Contas da AWS em uma organização. AWS Organizations O padrão usa o AWS Cloud Development Kit (AWS CDK) Toolkit e. AWS CloudFormation

EventBridge oferece um barramento de eventos sem servidor que ajuda você a receber, filtrar, transformar, rotear e entregar eventos. Um componente essencial das arquiteturas orientadas por eventos, EventBridge oferece suporte à separação entre produtores de mensagens e consumidores dessas mensagens. Em uma única conta, isso é simples. Uma estrutura de várias contas exige considerações adicionais para que eventos no barramento de eventos em uma conta sejam consumidos em outras contas dentro da mesma organização.

Para obter informações sobre considerações específicas da conta para produtores e consumidores, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Uma AWS Organizations organização com pelo menos dois associados Contas da AWS
- Uma função AWS Identity and Access Management (IAM) em ambos Contas da AWS que permite provisionar infraestrutura em ambos Contas da AWS usando AWS CloudFormation
- Git instalado localmente

- AWS Command Line Interface (AWS CLI) instalado localmente
- AWS CDK instalado localmente e inicializado em ambos Contas da AWS

Versões do produto

Esse padrão foi criado e testado usando as seguintes ferramentas e versões:

- AWS CDK Kit de ferramentas 2.126.0
- Node.js 18.19.0
- npm 10.2.3
- Python 3.12

Esse padrão deve funcionar com qualquer versão da AWS CDK v2 ou npm. As versões 13.0.0 a 13.6.0 do Node.js não são compatíveis com o. AWS CDK

Arquitetura

Arquitetura de destino

O diagrama a seguir mostra o fluxo de trabalho da arquitetura para enviar um evento de uma conta e consumi-lo em outra conta.

O fluxo de trabalho contém as seguintes etapas:

1. A AWS Lambda função Producer na conta Source coloca um evento no barramento de EventBridge eventos da conta.
2. A EventBridge regra entre contas encaminha o evento para um barramento de EventBridge eventos na conta de destino.
3. O barramento de EventBridge eventos na conta de destino tem uma regra Lambda de destino que invoca a função Consumer Lambda.

Uma prática recomendada é usar uma Dead Letter Queue (DLQ) para lidar com invocações com falha da função Consumer Lambda. No entanto, o DLQ foi omitido dessa solução para maior clareza. Para saber mais sobre como implementar uma DLQ em seus fluxos de trabalho e melhorar a capacidade de recuperação de falhas, consulte a postagem do blog Implementando padrões de tratamento de AWS Lambda erros.

Automação e escala

AWS CDK provisiona automaticamente a arquitetura necessária. EventBridge pode escalar para milhares de registros por segundo, dependendo do Região da AWS. Para obter mais informações, consulte a documentação de EventBridge cotas da Amazon.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código. Esse padrão usa o AWS CDK Toolkit, um kit de desenvolvimento em nuvem de linha de comando que ajuda você a interagir com seu AWS CDK aplicativo.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.

Outras ferramentas

- O Node.js é um ambiente de tempo de JavaScript execução orientado a eventos projetado para criar aplicativos de rede escaláveis.
- O npm é um registro de software executado em um ambiente Node.js e usado para compartilhar ou emprestar pacotes e gerenciar a implantação de pacotes privados.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub cross-account-eventbridge-in-organization.

Práticas recomendadas

Para conhecer as melhores práticas ao trabalhar com EventBridge, consulte os seguintes recursos:

- Melhores práticas para padrões de EventBridge eventos da Amazon
- Melhores práticas ao definir regras na Amazon EventBridge

Épicos

Prepare seu ambiente AWS CDK de implantação local

Tarefa	Descrição	Habilidades necessárias
Configure as credenciais locais para a conta de origem e a conta de destino.	Consulte Configurar novas configurações e credenciais e use o método de autenticação e credencial que faz mais sentido para seu ambiente. **Important** Certifique-se de configurar a autenticação da conta AWS CLI de origem e da conta de destino. Essas instruções pressupõem que você tenha configurado dois perfis da AWS localmente: `sourceAccount` `destinationAccount` e.	Desenvolvedor de aplicativos
Inicialize os dois Contas da AWS.	Para inicializar as contas, execute os seguintes comandos:	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`cdk bootstrap --profile sourceAccount` `cdk bootstrap --profile destinationAccount`	

Clone o código do padrão.	Para clonar o repositório, execute o seguinte comando:
	`git clone git@github.com:aws-samples/aws-cdk-examples.git`
	Em seguida, altere o diretório para a pasta do projeto recém-clonado:
	`cd aws-cdk-examples/python/cross-account-eventbridge-in-organization`
		Desenvolvedor de aplicativos

Implante ProducerStack na conta de origem

Tarefa	Descrição	Habilidades necessárias
Modifique `cdk.json` com seus detalhes AWS Organizations e da conta.	Na pasta raiz do projeto, faça as seguintes alterações em`cdk.json`: • `organization_id` – O ID da organização das contas envolvidas em sua implantação	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	• `event_bus _name –CrossAccount` , ou você pode renomeá-lo • `rules[].targets[]. arn` – O Conta da AWS ID da conta consumidora (conta de destino)	
Implante os ProducerStack recursos.	Execute o comando a seguir no diretório raiz do projeto: `cdk deploy ProducerS tack --profile sourceAccount` Quando solicitado, aceite as novas funções do IAM e outras permissões relaciona das à segurança criadas por meio de. AWS CloudForm ation	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Verifique se os ProducerStack recursos estão implantados.	Para verificar os recursos, faça o seguinte: 1. Em AWS Managemen t Console Para a conta Source, escolha CloudForm ation. 2. Na lista de pilhas, escolha ProducerStack. 3. Na guia Informações da pilha, verifique se o status da pilha é. `CREATE_CO MPLETE` Opcionalmente, na guia Recursos, revise os recursos configurados.	Desenvolvedor de aplicativos

ConsumerStack Implantar na conta de destino

Tarefa	Descrição	Habilidades necessárias
Implante os ConsumerStack recursos.	Execute o comando a seguir no diretório raiz do projeto: `cdk deploy ConsumerS tack --profile destinationAccount` Quando solicitado, aceite as novas funções do IAM e outras permissões relaciona das à segurança criadas por meio de. AWS CloudForm ation	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Verifique se os ConsumerStack recursos estão implantados	1. No console da conta de destino, escolha CloudFormation. 2. Na lista de pilhas, escolha ConsumerStack. 3. Na guia Informações da pilha, verifique se o status da pilha é. `CREATE_COMPLETE` Opcionalmente, na guia Recursos, revise os recursos configurados.	Desenvolvedor de aplicativos

Produza e consuma eventos

Tarefa	Descrição	Habilidades necessárias
Invoque a função Producer Lambda.	1. No console da conta Source, escolha Lambda. 2. Na lista de funções, escolha ProducerStack- ProducerLambda XXXX (XXXX representa uma sequência de caracteres gerada automaticamente pelo AWS CDK). 3. Selecione a guia Testar. 4. Na seção Evento de teste, escolha Teste. O conteúdo da área de texto Event JSON pode ser qualquer JSON válido fornecido à função Lambda	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	como carga útil. Nesse caso, o JSON padrão fornecido é suficiente. 5. Verifique se a mensagem Executando função: bem-sucedida aparece em um banner verde acima da seção Evento de teste.	

Tarefa	Descrição	Habilidades necessárias
Verifique se o evento foi recebido.	1. No console da conta de destino, escolha Lambda. 2. Na lista de funções, escolha ConsumerStack-ConsumerLambda XXXX (XXXX representa uma sequência de caracteres gerada automaticamente pelo AWS CDK). 3. Escolha a guia Monitor (Monitorar). 4. Na seção Monitor, escolha Exibir CloudWatch registros . 5. Na guia recém-aberta, escolha o nome do fluxo de log do fluxo de log mais recente. 6. Verifique se uma instrução de log, como a seguinte, aparece: `[DEBUG] 2024-04-08T19:08:10.091Z 9c16844a-f9de-444d-b621-86afe64d4cc8 Event: {'version':'0', 'id':'0b9faa96-973f-8be2-ecf8-75e4f328b980', 'detail-type':'TestType', 'source':'Producer', 'account'`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`:'XXXXXXXXXXXX', 'time':'2024-04-08 T19:08:09Z', 'region':'us-east-1', 'resources': [], 'detail': {'key1':'value1', 'key2':'value2', 'key3':'value3'}}`	

Limpeza

Tarefa	Descrição	Habilidades necessárias
Destrua os ConsumerStack recursos.	Se você estiver usando esse padrão como teste, limpe os recursos implantados para evitar custos adicionais. Execute o comando a seguir no diretório raiz do projeto: `cdk destroy ConsumerStack --profile destinationAccount` Você será solicitado a confirmar a exclusão da pilha.	Desenvolvedor de aplicativos
Destrua os ProducerStack recursos.	Execute o comando a seguir no diretório raiz do projeto: `cdk destroy ProducerStack --profile sourceAccount`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Você será solicitado a confirmar a exclusão da pilha.	

Solução de problemas

Problema	Solução
Nenhum evento foi recebido na conta de destino.	1. Verifique se o ID do Organizations fornecido está correto. 2. Verifique se a conta de origem faz parte da organização fornecida. 3. Verifique se as regras do barramento de eventos na conta de origem estão mapeadas para as informações corretas na conta de destino.
A invocação de uma função Lambda a partir do console retorna o seguinte erro: `User: arn:aws:iam::123456789012:user/XXXXX is not authorized to perform: lambda:Invoke`	Entre em contato com seu Conta da AWS administrador para receber as permissões de `lambda:Invoke` ação apropriadas na função `ProducerStack-ProducerLambdaXXXX` Lambda.

Recursos relacionados

Referências

- AWS Organizations Guia do usuário
- Padrões de EventBridge eventos da Amazon
- Regras na Amazon EventBridge

Tutoriais e vídeos

- Tutorial: Criação e configuração de uma organização

- AWS re:Invent 2023 — Padrões avançados baseados em eventos com a Amazon (01-R) EventBridge COM3

Mais informações

Regra do produtor

Na conta Source, um barramento de EventBridge eventos é criado para aceitar mensagens dos produtores (conforme mostrado na seção Arquitetura). Uma regra com as permissões do IAM associadas é criada nesse barramento de eventos. As regras têm como alvo o barramento de EventBridge eventos na conta de destino com base na seguinte `cdk.json` estrutura:

```
"rules": [
  {
    "id": "CrossAccount",
    "sources": ["Producer"],
    "detail_types": ["TestType"],
    "targets": [
      {
        "id": "ConsumerEventBus",
        "arn": "arn:aws:events:us-east-2:012345678901:event-bus/CrossAccount"
      }
    ]
  }
]
```

Para cada barramento de evento consumidor, o padrão do evento e o barramento do evento de destino devem ser incluídos.

Padrão de evento

Os padrões de eventos filtram a quais eventos essa regra se aplicará. Para fins deste exemplo, as fontes de eventos e o registro `detail_types` identificam quais eventos devem ser transmitidos do barramento de eventos da conta de origem para o barramento de eventos da conta de destino.

Ônibus do evento alvo

Essa regra tem como alvo um barramento de eventos que existe em outra conta. O nome completo `arn` (Amazon Resource Name) é necessário para identificar de forma exclusiva o barramento do evento de destino e `id` é o ID lógico usado por. AWS CloudFormation O barramento de eventos de destino não precisa realmente existir no momento da criação da regra de destino.

Considerações específicas da conta de destino

Na conta de destino, um barramento de EventBridge eventos é criado para receber mensagens do barramento de eventos da conta de origem. Para permitir que os eventos sejam publicados a partir da conta Source, você deve criar uma política baseada em recursos:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowOrgToPutEvents",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "events:PutEvents",
    "Resource": "arn:aws:events:us-east-2:012345678901:event-bus/CrossAccount",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-XXXXXXXXX"
      }
    }
  }]
}
```

É especialmente importante conceder a `events:PutEvents` permissão, que permite que qualquer outra conta na mesma organização publique eventos nesse barramento de eventos. A configuração `aws:PrincipalOrgId` como ID da organização concede as permissões necessárias.

Padrão de evento

Você pode modificar o padrão de evento incluído para atender ao seu caso de uso:

```
rule = events.Rule(
    self,
    self.id + 'Rule' + rule_definition['id'],
    event_bus=event_bus,
    event_pattern=events.EventPattern(
        source=rule_definition['sources'],
        detail_type=rule_definition['detail_types'],
    )
)
```

Para reduzir o processamento desnecessário, o padrão de eventos deve especificar que somente os eventos a serem processados pela conta de destino sejam transmitidos para o barramento de eventos da conta de destino.

Política baseada em recursos

Este exemplo usa o ID da organização para controlar quais contas têm permissão para colocar eventos no barramento de eventos da conta de destino. Considere usar uma política mais restritiva, como especificar a conta de origem.

EventBridge cotas

Lembre-se das seguintes cotas:

- 300 regras por barramento de eventos é a cota padrão. Isso pode ser expandido se necessário, mas deve se adequar à maioria dos casos de uso.
- Cinco alvos por regra é o máximo permitido. Recomendamos que os arquitetos de aplicativos usem uma regra distinta para cada conta de destino para oferecer suporte a um controle refinado sobre o padrão do evento.

Entregue registros do DynamoDB para o Amazon S3 usando o Kinesis Data Streams e o Firehose com AWS CDK

Criado por Shashank Shrivastava (AWS) e Daniel Matuki da Cunha (AWS)

Resumo

Esse padrão fornece código de amostra e um aplicativo para entrega de registros do Amazon DynamoDB para o Amazon Simple Storage Service (Amazon S3) usando o Amazon Kinesis Data Streams e o Amazon Data Firehose. A abordagem do padrão usa construções AWS Cloud Development Kit (AWS CDK) L3 e inclui um exemplo de como realizar a transformação de dados AWS Lambda antes que os dados sejam entregues ao bucket S3 de destino na Amazon Web Services ()AWS Cloud.

O Kinesis Data Streams registra alterações no nível de item em tabelas do DynamoDB e as replica no fluxo de dados do Kinesis requerido. Seus aplicativos podem acessar o fluxo de dados do Kinesis e visualizar as alterações no nível do item em tempo quase real. O Kinesis Data Streams também fornece acesso a outros serviços do Amazon Kinesis, como Firehose e Amazon Managed Service para Apache Flink. Isso significa desenvolver aplicativos para fornecer painéis em tempo real, gerar alertas, implementar definições de preço e de publicidade dinâmicas, além de executar análises de dados sofisticadas.

Você pode usar esse padrão para seus casos de uso de integração de dados. Por exemplo, veículos de transporte ou equipamentos industriais podem enviar grandes volumes de dados para uma tabela do DynamoDB. Esses dados podem então ser transformados e armazenados em um data lake hospedado no Amazon S3. Em seguida, você pode consultar e processar os dados e prever possíveis defeitos usando serviços sem servidor, como Amazon Athena, Amazon Redshift Spectrum, Amazon Rekognition e. AWS Glue

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Command Line Interface (AWS CLI), instalado e configurado. Para obter mais informações, consulte Introdução ao AWS CLI na AWS CLI documentação.
- Node.js (18.x+) e npm, instalados e configurados. Para obter mais informações, consulte Como baixar e instalar o Node.js e o npm na documentação do `npm`.

- aws-cdk (2.x+), instalado e configurado. Para obter mais informações, consulte Introdução ao AWS CDK na AWS CDK documentação.
- O repositório GitHub aws-dynamodb-kinesisfirehose-sde 3 ingestões, clonado e configurado em sua máquina local.
- Dados de amostra existentes para a tabela do DynamoDB. Deve usar o seguinte formato: `{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}`

Arquitetura

O diagrama a seguir mostra um exemplo de fluxo de trabalho para entrega de registros do DynamoDB para o Amazon S3 usando o Kinesis Data Streams e o Firehose.

O diagrama mostra o seguinte fluxo de trabalho:

1. Os dados são ingeridos usando o Amazon API Gateway como proxy para o DynamoDB. Você também pode usar qualquer outra origem para ingerir dados no DynamoDB.
2. As alterações no nível do item são geradas quase em tempo real no Kinesis Data Streams para entrega ao Amazon S3.
3. O Kinesis Data Streams envia os registros para a Firehose para transformação e entrega.
4. Uma função do Lambda converte os registros de um formato de registro do DynamoDB para o formato JSON, que contém somente os nomes e valores dos atributos do item de registro.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da AWS Cloud em código.
- AWS CDK O Toolkit é um kit de desenvolvimento em nuvem de linha de comando que ajuda você a interagir com seu AWS CDK aplicativo.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS

Repositório de código

O código desse padrão está disponível no repositório de GitHub aws-dynamodb-kinesisfirehose-s3 ingestões.

Épicos

Instalar e configurar o código de amostra

Tarefa	Descrição	Habilidades necessárias

Instale as dependências.	Em sua máquina local, instale as dependências dos arquivos `package.json` nos diretórios `pattern/aws-dynamodb-kinesisstreams-s3` e `sample-application` e executando os seguintes comandos:
	`cd <project_root>/pattern/aws-dynamodb-kinesisstreams-s3`
	`npm install && npm run build`
	`cd <project_root>/sample-application/`
	`npm install && npm run build`
		Desenvolvedor de aplicativos, AWS geral

Gere o CloudFormation modelo.	1. Execute o comando `cd <project_root>/sample-application/` .	Desenvolvedor de aplicativos, AWS geral, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	2. Execute o `cdk synth` comando para gerar o CloudFormation modelo. 3. A saída `AwsDynamodbKinesisfirehoseS3IngestionStack.template.json` é armazenada no diretório `cdk.out`. 4. Use AWS CDK ou o AWS Management Console para processar o modelo em CloudFormation.	

Implantar os recursos

Tarefa	Descrição	Habilidades necessárias
Verifique e implante os recursos.	1. Execute o `cdk diff` comando para identificar os tipos de recursos criados pela AWS CDK construção. 2. Execute o comando `cdk deploy` para implantar os recursos.	Desenvolvedor de aplicativos, AWS geral, AWS DevOps

Ingira dados na tabela do DynamoDB para testar a solução

Tarefa	Descrição	Habilidades necessárias
Inclua dados de amostra na tabela do DynamoDB.	Envie uma solicitação para sua tabela do DynamoDB	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	executando o seguinte comando em: AWS CLI
	
	`aws dynamodb put-item --table-name <your_table_name> --item '{"<table_partition_key>": {"S": "<partition_key_ID>"},"MessageData":{"S": "<data>"}}'`
	
	exemplo:
	
	`aws dynamodb put-item --table-name SourceData_table --item '{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}'`
	
	Por padrão, o `put-item` não retornará nenhum valor como saída se a operação for bem-sucedida. Se a operação falhar, ela retornará um erro. Os dados são armazenados no DynamoDB e depois enviados para o Kinesis Data Streams e o Firehose.	

Tarefa	Descrição	Habilidades necessárias
	Note Você usa abordagens diferentes para adicionar dados em uma tabela do DynamoDB. Para obter mais informações, consulte Carregar dados em tabelas na documentação do DynamoDB.	
Verifique se um novo objeto é criado no bucket do S3.	Faça login AWS Management Console e monitore o bucket do S3 para verificar se um novo objeto foi criado com os dados que você enviou. Para obter mais informações, consulte GetObject a documentação do Amazon S3.	Desenvolvedor de aplicativos, AWS geral

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Limpar os recursos.	Execute o comando `cdk destroy` para excluir todos os recursos usados por esse padrão.	Desenvolvedor de aplicativos, AWS geral

Recursos relacionados

- s3- static-site-stack .ts (repositório) GitHub
- aws-apigateway-dynamodb módulo (GitHub repositório)
- aws-kinesisstreams-kinesisfirehose-sMódulo 3 (GitHub repositório)
- Alterar a captura de dados para o DynamoDB Streams (documentação do DynamoDB)
- Usando o Kinesis Data Streams para capturar alterações no DynamoDB (documentação do DynamoDB)

Implemente o controle de versão de API baseado em caminhos usando domínios personalizados no Amazon API Gateway

Criado por Corey Schnedl (AWS), Anbazhagan Ponnuswamy (AWS), Marcelo Barbosa (AWS), Gaurav Samudra (AWS), Mario Lopez Martinez (AWS) e Abhilash Vinod (AWS)

Resumo

Esse padrão demonstra como você pode usar o recurso de mapeamentos de API de domínios personalizados para implementar uma solução de versionamento de API baseada em caminhos para o Amazon API Gateway.

O Amazon API Gateway é um serviço totalmente gerenciado que você pode usar para criar, publicar, manter, monitorar e proteger APIs em qualquer escala. Ao usar o recurso de domínio personalizado do serviço, você pode criar nomes de domínio personalizados que são mais simples e mais intuitivos URLs que você pode fornecer aos usuários da API. Você pode usar mapeamentos de API para conectar os estágios da API a um nome de domínio personalizado. Depois de criar um nome de domínio e configurar os registros DNS, você usa mapeamentos de API para enviar tráfego para você APIs por meio do seu nome de domínio personalizado.

Depois que uma API se torna disponível publicamente, os consumidores a usam. À medida que uma API pública evolui, seu contrato de serviço também evolui para refletir novos recursos e capacidades. No entanto, não é aconselhável alterar ou remover recursos existentes. Qualquer alteração significativa pode afetar os aplicativos do consumidor e interrompê-los em tempo de execução. O controle de versão da API é importante para evitar a quebra da compatibilidade com versões anteriores e a quebra de um contrato.

Você precisa de uma estratégia clara de controle de versão da API para ajudar os consumidores a adotá-las. O controle de versão APIs usando o método baseado em caminhos URLs é a abordagem mais simples e comumente usada. Nesse tipo de controle de versão, as versões são definidas explicitamente como parte da API. URIs O exemplo a seguir URLs mostra como um consumidor pode usar o URI para especificar uma versão da API para sua solicitação:

```
https://api.example.com/api/v1/orders
```

```
https://api.example.com/api/v2/orders
```

```
https://api.example.com/api/vX/orders
```

Esse padrão usa o AWS Cloud Development Kit (AWS CDK) para criar, implantar e testar um exemplo de implementação de uma solução escalável de versionamento baseada em caminhos para sua API. AWS CDK é uma estrutura de desenvolvimento de software de código aberto para modelar e provisionar seus recursos de aplicativos em nuvem usando linguagens de programação conhecidas.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- A propriedade de um domínio é necessária para usar o repositório de amostra desse padrão e usar a funcionalidade de domínio personalizado do Amazon API Gateway. Você pode usar o Amazon Route 53 para criar e gerenciar seus domínios para sua organização. Para obter informações sobre como registrar ou transferir um domínio com o Route 53, consulte Registro de novos domínios na documentação do Route 53.
- Antes de configurar um nome de domínio personalizado para uma API, você deve ter um certificado SSL/TLS pronto. AWS Certificate Manager
- É necessário criar ou atualizar o registro de recursos do provedor DNS para ser mapeado ao endpoint da API. Sem esse mapeamento, as solicitações de API vinculadas ao nome de domínio personalizado não podem chegar ao API Gateway.

Limitações

- Não há suporte para nomes de domínio personalizados para uso privado APIs.
- Um nome de domínio personalizado deve ser exclusivo Região da AWS em todas as áreas Contas da AWS.
- Para configurar mapeamentos de API com vários níveis, é necessário usar um nome de domínio regional personalizado e a política de segurança do TLS 1.2.
- Em um mapeamento de API, o nome de domínio personalizado e o mapeado APIs devem estar no mesmo Conta da AWS.
- Os mapeamentos da API devem conter somente letras, números e os seguintes caracteres: `$-_.+!*'()/`
- O comprimento máximo para o caminho em um mapeamento de API é de 300 caracteres.
- É possível ter 200 mapeamentos de API com vários níveis para cada nome de domínio.

- Você só pode APIs mapear HTTP para um nome de domínio personalizado regional com a política de segurança TLS 1.2.
- Você não pode WebSocket APIs mapear para o mesmo nome de domínio personalizado de uma API HTTP ou API REST.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- Esse exemplo de implementação é usado AWS CDK na TypeScript versão 2.149.0.

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho da arquitetura.

O diagrama ilustra o seguinte:

1. O usuário da API envia uma solicitação para o Amazon API Gateway com um nome de domínio personalizado.
2. O API Gateway roteia dinamicamente a solicitação do usuário para uma instância e um estágio apropriados do API Gateway, com base no caminho indicado na URL da solicitação. A tabela a seguir mostra um exemplo de como os diferentes caminhos baseados em URL podem ser roteados para estágios específicos para diferentes instâncias do API Gateway.

API	Estágio	Path	Endpoint padrão
Cálculo APIv1	api	apiv1	Habilitada
Cálculo APIv2	api	API v2	Habilitada
Cálculo APIv X	api	APIvX	Habilitada

3. A instância de destino do API Gateway processa a solicitação e retorna o resultado ao usuário.

Automação e escala

Recomendamos que você use AWS CloudFormation pilhas separadas para cada versão da sua API. Com essa abordagem, você pode ter um isolamento completo entre o back-end, APIs que pode ser roteado pelo recurso de mapeamento personalizado da API de domínio. Uma vantagem dessa abordagem é que diferentes versões da sua API podem ser implantadas ou removidas de forma independente, sem o risco de modificar outra API. Essa abordagem aumenta a resiliência por meio do isolamento das CloudFormation pilhas. Além disso, ele fornece diferentes opções de back-end para sua API AWS Lambda AWS Fargate, como endpoints HTTP e ações de. Serviços da AWS

Você pode usar estratégias de ramificação do Git, como o Gitflow, em combinação com CloudFormation pilhas isoladas para gerenciar o código-fonte implantado em diferentes versões da API. Ao usar essa opção, você pode manter versões diferentes da sua API sem a necessidade de duplicar o código-fonte para novas versões. Com o Gitflow, você pode adicionar tags aos commits no seu repositório git à medida que os lançamentos são realizados. Como resultado, você tem uma visão geral completa do código-fonte relacionado a uma versão específica. Como as atualizações precisam ser realizadas, você pode verificar o código de uma versão específica, fazer atualizações e, em seguida, implantar o código-fonte atualizado na CloudFormation pilha que se alinha à versão principal correspondente. Essa abordagem reduz o risco de quebrar outra versão da API porque cada versão da API tem código-fonte isolado e é implantada em CloudFormation pilhas separadas.

Ferramentas

Serviços da AWS

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- AWS Certificate Manager (ACM) ajuda você a criar, armazenar e renovar certificados e chaves SSL/TLS X.509 públicos e privados que protegem seus sites e aplicativos. AWS
- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software de código aberto para definir sua infraestrutura de nuvem em código e provisioná-la por meio dela. AWS CloudFormation A implementação de amostra desse padrão usa o AWS CDK in TypeScript. Trabalhar com o AWS CDK in TypeScript usa ferramentas familiares, incluindo o TypeScript compilador Microsoft (`tsc`), o Node.js e o gerenciador de pacotes node (`npm`). Se preferir, você pode usar o Yarn, embora os exemplos desse padrão `npm` usem. Os módulos que compõem a AWS Construct Library são distribuídos por meio do `npm` repositório npmjs.org.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS

- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.
- AWS WAFé um firewall de aplicativo web que ajuda você a monitorar solicitações HTTP e HTTPS que são encaminhadas para seus recursos protegidos de aplicativos web.

Outras ferramentas

- Bruno é um cliente de teste de API de código aberto e compatível com git.
- O cdk-nag é um utilitário de código aberto que verifica as melhores práticas AWS CDK dos aplicativos usando pacotes de regras.

Repositório de código

O código desse padrão está disponível no repositório GitHub path-based-versioning-with-api-gateway.

Práticas recomendadas

- Use um pipeline robusto de integração contínua e entrega contínua (CI/CD) para automatizar o teste e a implantação de suas CloudFormation pilhas criadas com o. AWS CDK Para obter mais informações relacionadas a essa recomendação, consulte o AWS DevOps Well-Architected Guidance.
- AWS WAF é um firewall gerenciado que se integra facilmente a serviços como o Amazon API Gateway. Embora AWS WAF não seja um componente necessário para que esse padrão de controle de versão funcione, recomendamos como prática recomendada de segurança incluí-lo no API AWS WAF Gateway.
- Incentive os consumidores da API a atualizarem regularmente para a versão mais recente da sua API, para que as versões mais antigas da API possam ser descontinuadas e removidas com eficiência.
- Antes de usar essa abordagem em um ambiente de produção, implemente uma estratégia de firewall e autorização para sua API.
- Implemente o acesso ao gerenciamento de seus AWS recursos Conta da AWS usando o modelo de acesso com privilégios mínimos.

- Para aplicar as melhores práticas e recomendações de segurança para aplicativos criados com o AWS CDK, recomendamos que você use o utilitário cdk-nag.

Épicos

Prepare seu ambiente local

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositório de aplicativos de amostra, execute o seguinte comando: `git clone https://github.com/aws-samples/path-based-versioning-with-api-gateway`	Desenvolvedor de aplicativos
Navegue até o repositório clonado.	Para navegar até o local da pasta do repositório clonado, execute o seguinte comando: `cd api-gateway-custom-domain-versioning`	Desenvolvedor de aplicativos
Instale as dependências necessárias.	Para instalar as dependências necessárias, execute o seguinte comando: `npm install`	Desenvolvedor de aplicativos

Implante a pilha de CloudFormation roteamento

Tarefa	Descrição	Habilidades necessárias
Inicie a implantação da pilha de roteamento.	Para iniciar a implantação da pilha de CloudFormation roteamento`CustomDomainRouterStack`, execute o comando a seguir, substituindo-`example.com` o pelo nome do domínio que você possui: `npx cdk deploy CustomDomainRouterStack --parameters PrerequisiteDomainName=example.com` **Note** A implantação da pilha não será bem-sucedida até que a seguinte tarefa de validação de DNS do domínio seja executada com êxito.	Desenvolvedor de aplicativos

Confirmar a propriedade de um domínio

Tarefa	Descrição	Habilidades necessárias
Verifique a propriedade do seu domínio.	O certificado permanecerá em um status de validação pendente até que você prove	Desenvolvedor de aplicativos, administrador de sistemas da AWS, administrador de rede

Tarefa	Descrição	Habilidades necessárias
	a propriedade do domínio associado. Para provar a propriedade, adicione registros CNAME à zona hospedada associada ao domínio. Para obter mais informações, consulte Validação de DNS na AWS Certificate Manager documentação. Adicionar os registros apropriados permite que a `CustomDomainRouterStack` implantação seja bem-sucedida.	

Tarefa	Descrição	Habilidades necessárias
Crie um registro de alias para apontar para seu domínio personalizado do API Gateway.	Depois que o certificado for emitido e validado com sucesso, crie um registro DNS que aponte para seu URL de domínio personalizado do Amazon API Gateway. O URL do domínio personalizado é gerado exclusivamente pelo provisionamento do domínio personalizado e é especificado como um parâmetro de saída. CloudFormation Veja a seguir um exemplo do registro: Política de roteamento: roteamento simples Nome do registro: `demo.api-gateway-custom-domain-versioning.example.com` Alias: Yes Tipo de registro: um registro DNS do tipo “A” que aponta para um recurso AWS Valor: `d-xxxxxxxxxx.execute-api.xx-xxxx-x.amazonaws.com` TTL (segundos): 300	Desenvolvedor de aplicativos, administrador de sistemas da AWS, administrador de rede

Implemente CloudFormation pilhas e invoque a API

Tarefa	Descrição	Habilidades necessárias

Implante a pilha `ApiStackV1` .	Para implantar a `ApiStackV1` pilha, use o seguinte comando:
	`npm run deploy-v1`
	O código CDK a seguir adiciona mapeamento de API:
	`var apiMapping = new CfnApiMapping(this, "ApiMapping", { apiId: this.lambdaRestApi.restApiId, domainName: props.customDomainName.domainName, stage: "api", apiMappingKey: "api/v1", });`
		Desenvolvedor de aplicativos

Implante a pilha `ApiStackV2` .	Para implantar a `ApiStackV2` pilha, use o seguinte comando: `npm run deploy-v2`	Desenvolvedor de aplicativos
Invoque a API .	Para invocar a API e testar os endpoints da API usando Bruno, consulte as instruções em Informações adicionais.	Desenvolvedor de aplicativos

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Limpar os recursos	Para destruir os recursos associados a esse aplicativo de amostra, use o seguinte comando: `npx cdk destroy --all` **Note** Certifique-se de limpar todos os registros DNS do Route 53 que foram adicionados manualmente para o processo de verificação da propriedade do domínio.	Desenvolvedor de aplicativos

Solução de problemas

Problema	Solução
A implantação do `CustomDomainRouterStack` expira porque o certificado não pode ser validado.	Certifique-se de ter adicionado os registros CNAME de validação de DNS adequados, conforme descrito na tarefa anterior. Seu novo certificado pode continuar exibindo o status de Validação pendente por até 30 minutos após a adição dos registros de validação de DNS. Para obter mais informações, consulte Validação de DNS na AWS Certificate Manager documentação.

Recursos relacionados

- Implementando o controle de versão do API Gateway baseado em cabeçalho com a CloudFront Amazon — AWS Esta postagem no blog sobre computação oferece uma estratégia de controle de versão baseada em cabeçalho como alternativa à estratégia de controle de versão baseada em caminhos descrita nesse padrão.
- AWS CDK Workshop — Este workshop introdutório se concentra na criação e implantação de aplicativos AWS usando o. AWS Cloud Development Kit (AWS CDK) Este workshop é compatível com Go, Python e. TypeScript

Mais informações

Testando sua API com Bruno

Recomendamos que você use o Bruno, uma ferramenta de teste de API de código aberto, para verificar se o roteamento baseado em caminho está funcionando corretamente para o aplicativo de amostra. Esse padrão fornece uma coleção de amostras para facilitar o teste da sua API de amostra.

Para invocar e testar sua API, use as seguintes etapas:

1. Instale o Bruno.
2. Abra Bruno.
3. No repositório de código desse padrão, selecione Bruno/sample-API - e abra a coleção. Gateway-Custom-Domain-Versioning
4. Para ver o menu suspenso Ambientes no canto superior direito da interface do usuário (UI), selecione qualquer solicitação na coleção.
5. No menu suspenso Ambientes, selecione Configurar.
6. Substitua o `REPLACE_ME_WITH_YOUR_DOMAIN` valor pelo seu domínio personalizado.
7. Escolha Salvar e, em seguida, feche a seção Configuração.
8. Para Ambiente Sandbox, verifique se a opção Ativo está selecionada.
9. Invoque sua API usando o botão -> para a solicitação selecionada.
10. Anote como a validação (transmissão de valores não numéricos) é tratada na V1 em comparação com a V2.

Para ver capturas de tela de exemplos de invocação de API e comparação da validação de V1 e V2, consulte Testando sua API de amostra no `README.md` arquivo no repositório de código desse padrão.

Importe a biblioteca psycopg2 para interagir com seu banco AWS Lambda de dados PostgreSQL

Criado por Louis Hourcade (AWS)

Resumo

Psycopg é um adaptador de banco de dados PostgresSQL para Python. Os desenvolvedores usam a `psycopg2` biblioteca para escrever aplicativos Python que interagem com bancos de dados PostgreSQL.

Na Amazon Web Services (AWS), os desenvolvedores também usam AWS Lambdapara executar código para aplicativos ou serviços de back-end. O Lambda é um serviço de computação sem servidor e orientado por eventos que executa código sem a necessidade de provisionar ou gerenciar servidores.

Por padrão, quando você cria uma nova função que usa um tempo de execução do Python (versão 3.9, 3.8 ou 3.7), o ambiente de execução do Lambda é criado a partir de uma imagem base do Lambda fornecida pela. AWS Bibliotecas, como `pandas` ou`psycopg2`, não estão incluídas na imagem base. Para usar uma biblioteca, você precisa agrupá-la em um pacote personalizado e anexá-la ao Lambda.

Há várias maneiras de agrupar e anexar uma biblioteca, incluindo as seguintes:

- Implante sua função Lambda a partir de um arquivo de arquivos.zip.
- Implante sua função Lambda a partir de uma imagem de contêiner personalizada.
- Crie uma camada Lambda e anexe-a à sua função Lambda.

Esse padrão demonstra as duas primeiras opções.

Com um pacote de implantação do.zip, adicionar a `pandas` biblioteca à sua função Lambda é relativamente simples. Crie uma pasta em sua máquina Linux, adicione o script Lambda junto com a `pandas` biblioteca e as dependências da biblioteca à pasta, compacte a pasta e forneça-a como fonte para sua função Lambda.

Embora o uso de um pacote de implantação.zip seja uma prática comum, essa abordagem não funciona para a `psycopg2` biblioteca. Esse padrão mostra primeiro o erro que você recebe ao usar um pacote de implantação .zip para adicionar a `psycopg2` biblioteca à sua função Lambda. Em

seguida, o padrão mostra como implantar o Lambda a partir de um Dockerfile e editar a imagem do Lambda para fazer a biblioteca funcionar. `psycopg2`

Para obter informações sobre os três recursos que o padrão implanta, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS com permissões suficientes para implantar os AWS recursos usados por esse padrão
- AWS Cloud Development Kit (AWS CDK) instalado globalmente executando `npm install -g aws-cdk`
- Um cliente Git
- Python
- Docker

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Versões do produto

- Versão de tempo de execução do AWS Lambda: Python 3.8 (o padrão pode ser adaptado para outras versões do Python).
- Psycopg2 versão 2.9.3
- Pandas versão 1.5.2

Arquitetura

Visão geral da solução

Para ilustrar os desafios que você pode enfrentar ao usar a `psycopg2` biblioteca no Lambda, o padrão implanta duas funções do Lambda:

- Uma função Lambda com o tempo de execução do Python 3.8 criado a partir de um arquivo.zip. As `pandas` bibliotecas `psycopg2` e são instaladas nesse pacote de implantação .zip usando pip.
- Uma função Lambda com o tempo de execução do Python 3.8 criado a partir de um Dockerfile. O Dockerfile instala as `pandas` bibliotecas `psycopg2` e na imagem do contêiner Lambda.

A primeira função do Lambda instala a `pandas` biblioteca e suas dependências em um arquivo.zip, e o Lambda pode usar essa biblioteca.

A segunda função do Lambda demonstra que, ao criar uma imagem de contêiner para sua função do Lambda, você pode executar as bibliotecas e `pandas` no Lambda. `psycopg2`

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da AWS Cloud em código.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- pandas é uma ferramenta de código aberto baseada em Python para análise e manipulação de dados.
- O Psycopg é um adaptador de banco de dados PostgreSQL para a linguagem Python, projetado para aplicativos multiencadeados. Esse padrão usa Psycopy 2.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório import-psycopg2 - - em. in-lambda-to-interact with-postgres-database GitHub

Práticas recomendadas

Esse padrão fornece um exemplo prático de uso AWS CDK para criar uma função Lambda a partir de um Dockerfile. Se você reutilizar esse código em seu aplicativo, certifique-se de que os recursos implantados atendam a todos os requisitos de segurança. Use ferramentas como o Checkov, que verifica as configurações da infraestrutura em nuvem para encontrar configurações incorretas antes que a infraestrutura seja implantada.

Épicos

Clone o repositório e configure a implantação

Tarefa	Descrição	Habilidades necessárias

Clonar o repositório.	Para clonar o GitHub repositório em sua máquina local, execute os seguintes comandos:
	`git clone https://github.com/aws-samples/import-psycopg2-in-lambda-to-interact-with-postgres-database.git`
	`cd AWS-lambda-psycopg2`
		AWS geral

Configure sua implantação.	Edite o `app.py` arquivo com informações sobre Conta da AWS:
	`aws_acccount = "AWS_ACCOUNT_ID"`
	`region = "AWS_REGION"`
	`# Select the CPU architecture you are using to build the image (ARM or X86)`
	`architecture = "ARM"`
		AWS geral

Inicialize sua conta da AWS e implante o aplicativo

Tarefa	Descrição	Habilidades necessárias
Inicialize seu. Conta da AWS	Se você ainda não inicializou seu ambiente AWS, execute os seguintes comandos com as AWS credenciais da sua conta: AWS `cdk bootstrap aws://<tooling-account-id>/<aws-region>`	AWS geral
Implante o código.	Para implantar o AWS CDK aplicativo, execute o seguinte comando: `cdk deploy AWSLambdaPyscopg2`	AWS geral

Teste as funções do Lambda no AWS Management Console

Tarefa	Descrição	Habilidades necessárias
Teste a função Lambda criada a partir do arquivo.zip.	Para testar a função Lambda que foi criada a partir do arquivo.zip, faça o seguinte: 1. Faça login no console e abra o console Lambda em. https://console.aws.amazon.com/lambda/ 2. Selecione a função `lambda-from-zip` Lambda.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	3. Crie um evento de teste para invocar a função. 4. Quando invocada, a função deve gerar um erro que inclua a seguinte mensagem: `"errorMessage": Unable to import module 'lambda_code': libpq.so.5: cannot open shared object, "stackTrace": [] "errorType": Runtime.ImportModuleError",` 5. Abra o CloudWatch console da Amazon em https://console.aws.amazon.com/cloudwatch/. Os CloudWatch registros mostram que a `pandas` biblioteca foi importada com sucesso, mas que a importação da `psycopg2` biblioteca falhou. Como o Lambda não encontra as bibliotecas PostgreSQL necessárias na imagem padrão, ele não pode usar a biblioteca. `psycopg2`	

Tarefa	Descrição	Habilidades necessárias

Teste a função Lambda criada a partir do Dockerfile.	Para usar a `psycopg2` biblioteca em sua função Lambda, você deve editar a Lambda Amazon Machine Image (AMI).
	
	Para testar a função Lambda que foi criada a partir do Dockerfile, faça o seguinte:
	
	1. Faça login no console e abra o console Lambda.
	2. Selecione a função `lambda-from-docker` Lambda.
	3. Crie um evento de teste para invocar a função.
	4. Quando invocada, a função deve ser executada com êxito.
	
	O código a seguir mostra o Dockerfile que o AWS CDK modelo cria:
	
	`# Start from lambda Python3.8 image`
	`FROM public.ecr.aws/lambda/python:3.8`
	
	`# Copy the lambda code, together with its requirements`
	`COPY lambda/requirements.txt ${LAMBDA_TASK_ROOT}`
		AWS geral

Tarefa	Descrição	Habilidades necessárias

	<pre>COPY lambda/lambda_code
	.py ${LAMBDA_TASK_ROOT
	}
	
	# Install postgresql-
	devel in your image
	RUN yum install -y gcc
	 postgresql-devel
	
	# install the requireme
	nts for the Lambda code
	RUN pip3 install -r
	 requirements.txt
	 --target "${LAMBDA
	_TASK_ROOT}"
	
	# Command can be
	 overwritten by
	 providing a different
	 command in the template
	 directly.
	CMD ["lambda_code.hand
	ler"]</pre>
	O Dockerfile usa a imagem AWS Lambda fornecida para o tempo de execução do Python 3.8 e instala o postgresql-devel, que contém as bibliotecas necessárias para compilar aplicativos que interagem diretamente com o servidor de gerenciamento do PostgreSQL. O Dockerfile também instala as `psycopg2` bibliotecas `pandas` e, que são indicadas no arquivo. `requirements.txt`	

Recursos relacionados

- AWS CDK documentação
- AWS Lambda documentação

Mais informações

Nesse padrão, o AWS CDK modelo fornece uma AWS pilha com três recursos:

- Uma função AWS Identity and Access Management (IAM) para as funções Lambda.
- Uma função Lambda com um tempo de execução do Python 3.8. A função é implantada a partir do pacote de `Constructs/lambda/lambda_deploy.zip` implantação.
- Uma função Lambda com um tempo de execução do Python 3.8. A função é implantada a partir do Dockerfile sob a pasta `Constructs`

O script para ambas as funções do Lambda verifica se as `psycopg2` bibliotecas `pandas` e foram importadas com sucesso:

```
import pandas
print("pandas successfully imported")

import psycopg2
print("psycopg2 successfully imported")

def handler(event, context):
    """Function that checks whether psycopg2  and pandas are successfully imported or
 not"""
    return {"Status": "psycopg2 and pandas successfully imported"}
```

O pacote `lambda_deploy.zip` de implantação é criado com o script `Constructs/lambda/build.sh` bash. Esse script cria uma pasta, copia o script Lambda, instala as `psycopg2` bibliotecas `pandas` e gera o arquivo.zip. Para gerar você mesmo o arquivo.zip, execute esse script bash e reimplante a pilha. AWS CDK

O Dockerfile começa com a imagem base AWS fornecida para o Lambda com um tempo de execução do Python 3.8. O Dockerfile instala as `psycopg2` bibliotecas `pandas` e em cima da imagem padrão.

Integre o Amazon API Gateway com o Amazon SQS para lidar com REST assíncrono APIs

Criado por Natalia Colantonio Favero (AWS) e Gustavo Martim (AWS)

Resumo

Quando você implanta o REST APIs, às vezes você precisa expor uma fila de mensagens que os aplicativos cliente possam publicar. Por exemplo, você pode ter problemas com a latência de terceiros APIs e atrasos nas respostas, ou talvez queira evitar o tempo de resposta das consultas ao banco de dados ou evitar escalar o servidor quando há um grande número de consultas simultâneas. APIs Nesses cenários, os aplicativos cliente que publicam na fila só precisam saber que a API recebeu os dados, não o que acontece depois que os dados são recebidos.

Esse padrão cria um endpoint da API REST usando o Amazon API Gateway para enviar uma mensagem para o Amazon Simple Queue Service (Amazon SQS). Ele cria uma easy-to-implement integração entre os dois serviços que evita o acesso direto à fila do SQS.

Pré-requisitos e limitações

- Uma AWS conta ativa

Arquitetura

O diagrama ilustra essas etapas:

1. Solicite um endpoint da API POST REST usando uma ferramenta como o Postman, outra API ou outras tecnologias.
2. O API Gateway publica uma mensagem, que é recebida no corpo da solicitação, na fila.
3. O Amazon SQS recebe a mensagem e envia uma resposta ao API Gateway com um código de sucesso ou falha.

Ferramentas

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.

- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.

Épicos

Criar uma fila SQS

Tarefa	Descrição	Habilidades necessárias
Crie sua fila.	Para criar uma fila SQS que receba as mensagens da API REST: 1. Faça login no Conta da AWS. 2. Abra o console do Amazon SQS em. https://console.aws.amazon.com/sqs/ 3. Selecione Criar fila. 4. Na página Criar fila, escolha a correta Região da AWS na lista suspensa Região. 5. Para Tipo, mantenha a configuração padrão (Padrão). 6. Insira um Name (Nome) para a fila. 7. Mantenha os valores padrão para todas as outras configurações. 8. Selecione Criar fila.	Desenvolvedor de aplicativos

Forneça acesso ao Amazon SQS

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM.	Essa função do IAM dá aos recursos do API Gateway acesso total ao Amazon SQS. 1. Abra o console do IAM em https://console.aws.amazon.com/iam/. 2. No painel de navegação, selecione Perfil e então, Criar perfil. 3. Em Tipo de Entidade Confiável, escolha AWS service (Serviço da AWS). 4. Em Caso de uso, escolha API Gateway na lista suspensa e escolha Avançar, Avançar. 5. Em Nome da função, insira AWSGatewayRoleForSQS e uma descrição opcional e escolha Criar função. 6. No painel Roles, pesquise por AWSGatewayRoleForSQS e marque sua caixa de seleção. 7. Na seção Políticas de permissões, escolha Adicionar permissões, Anexar políticas.	Desenvolvedor de aplicativos, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	8. Pesquise o Amazon SQSFull Access e selecione-o. 9. Escolha Adicionar permissões. 10. Na seção Resumo do AWSGatewayRoleForSQS, copie o Amazon Resource Number (ARN). Você usará esse ID em uma etapa posterior.	

Criar uma API REST

Tarefa	Descrição	Habilidades necessárias
Crie uma API REST.	Essa é a API REST para a qual as solicitações HTTP são enviadas. 1. Abra o console do API Gateway em https://console.aws.amazon.com/apigateway/. 2. Na seção API REST, escolha Construir. 3. Em Nome da API, insira um nome e uma descrição opcional para sua API, mantenha todas as outras configurações padrão e escolha Criar API.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Conecte o API Gateway ao Amazon SQS.	Essa etapa permite que a mensagem flua de dentro do corpo da solicitação HTTP para o Amazon SQS. 1. No console do API Gateway, escolha a API que você criou. 2. Na página Recursos, na seção Métodos, escolha Criar método. 3. Em Tipo de método, escolha POST. 4. Em Tipo de integraçã o, escolha AWS service (Serviço da AWS). 5. Para Região da AWS, escolha a região em que você criou sua fila SQS. 6. Para AWS service (Serviço da AWS), escolha Simple Queue Service (SQS). 7. Para o método HTTP, escolha POST. 8. Em Tipo de ação, escolha Usar substituição de caminho. 9. <name of SQS queue>Em Path override, insira/<AWS account ID>. 10 Em Função de execução, cole o ARN da função que você criou anteriormente.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	11 Escolha Criar método.	

Teste a API REST

Tarefa	Descrição	Habilidades necessárias

Teste a API REST.	Execute um teste para verificar a falta de configuração:
	1. No console do API Gateway, escolha a API REST que você criou.
	2. No painel Recursos, escolha o método POST.
	3. Selecione a guia Testar. (Use a seta para a direita se a guia não for exibida.)
	4. Em Corpo da solicitação, cole o seguinte código JSON:
	`{ "message": "lorem ipsum" }`
	5. Escolha Testar.
	Você receberá um erro semelhante ao seguinte:
	`<UnknownOperationException/>`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Altere a integração da API para encaminhar a solicitação corretamente para o Amazon SQS.	Conclua a configuração para corrigir o erro de integração: 1. No console do API Gateway, escolha a API que você criou e, em seguida, escolha POST. 2. A seção Execução de métodos mostra o mapeamento visual entre o API Gateway e o Amazon SQS. Nessa seção, escolha Solicitação de integração e, em seguida, escolha Editar. 3. Expanda a seção de cabeçalhos HTTP e escolha o parâmetro Adicionar cabeçalho de solicitação. • Em Nome, especifique Content-Type. • Em Mapeado de, digite x-www-form-urlenco ded'application/ '. Certifique-se de incluir as aspas simples. • Marque a caixa de seleção Armazenamento em cache. 4. Expanda a seção Modelos de mapeamento. • Escolha Add mapping template (Adicionar modelo de mapeamento).	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	• Em Tipo de conteúdo, insira application/json. • Para o corpo do modelo, cole este código: `Action=SendMessage&MessageBody=$input.body` • Escolha Salvar.	

Tarefa	Descrição	Habilidades necessárias
Teste e valide a mensagem no Amazon SQS.	Execute um teste para confirmar que o teste foi concluído com êxito: 1. No console do API Gateway, escolha a API REST que você criou. 2. No painel Recursos, escolha o método POST. 3. Selecione a guia Testar. (Use a seta para a direita se a guia não for exibida.) 4. Em Corpo da solicitação, cole o seguinte código JSON: `{ "message": "lorem ipsum" }` 5. Escolha Testar. 6. Abra o console do Amazon SQS. 7. No painel de navegação, escolha Filas e escolha sua fila. 8. Escolha Enviar e receber mensagens. 9. Escolha Poll for messages (Sondagem de mensagens). 10. Selecione Messagem. Ele deve exibir o seguinte:	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`Body { "message": "lorem ipsum" }`	

Tarefa	Descrição	Habilidades necessárias

Teste o API Gateway com um caractere especial.	Execute um teste que inclua caracteres especiais (como &) que não sejam aceitáveis em uma mensagem:
	1. No console do API Gateway, escolha sua API.
	2. Repita o teste da etapa anterior usando o seguinte código JSON:
	`{ "message": "lorem ipsum &" }`
	3. Escolha Testar.
	Você receberá um erro como o seguinte:
	`{ "Error": { "Code": "AccessDenied", "Message": "Access to the resource https://sqs.us-east-2.amazonaws.com/976166761794/Apg2 is denied.", "Type": "Sender" }, "RequestId": "e83c9c67-bcf6-5e9a-91e9-c737094b17ab"`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	<pre>}</pre> Isso ocorre porque caractere s especiais não são suportado s por padrão no corpo da mensagem. Na próxima etapa, você configurará o API Gateway para oferecer suporte a caracteres especiais . Para obter mais informaçõ es sobre conversões de tipo de conteúdo, consulte a documentação do API Gateway.	

Tarefa	Descrição	Habilidades necessárias

Altere a configuração da API para oferecer suporte a caracteres especiais.	Ajuste a configuração para aceitar caracteres especiais na mensagem:
	1. No console do API Gateway, escolha a API que você criou e, em seguida, escolha POST.
	2. Selecione Solicitação de integração e, depois, Editar.
	3. Altere o tratamento de conteúdo para converter em texto.
	4. Na seção Modelos de mapeamento:
	• Em Tipo de conteúdo, insira application/json.
	• Para Corpo do modelo, especifique:
	`Action=SendMessage&MessageBody=$util.urlEncode($input.body)`
	• Escolha Salvar.
	5. Selecione a guia Testar.
	6. Em Corpo da solicitação, insira o código JSON anterior:
	`{ " message": "lorem ipsum &" }`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	7. Escolha Testar. 8. Abra o console do Amazon SQS. 9. Selecione sua fila e, em seguida, escolha Enviar e receber mensagens, Sondagem de mensagens, Mensagem como anteriormente. A nova mensagem deve incluir o caractere especial.	

Implemente a API REST

Tarefa	Descrição	Habilidades necessárias
Implantar a API.	Para implantar a API REST: 1. Abra o console do API Gateway. 2. Selecione a API. 3. Escolha Implantar API. Para obter mais informações sobre essa etapa, consulte a documentação do API Gateway.	Desenvolvedor de aplicativos
Teste com uma ferramenta externa.	Execute um teste com uma ferramenta externa para confirmar se a mensagem foi recebida com sucesso:	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	1. Abra uma ferramenta como Postman, Insomnia ou cURL. 2. Execute sua API. 3. Abra o console do Amazon SQS. 4. Selecione sua fila. 5. Carregue mensagens para ver a nova mensagem.	

Limpar

Tarefa	Descrição	Habilidades necessárias
Exclua a API.	No console do API Gateway, escolha a API que você criou e, em seguida, escolha Excluir.	Desenvolvedor de aplicativos
Exclua o perfil do IAM.	No console do IAM, no painel Roles, selecione AWSGatewayRoleForSQS e escolha Delete.	Desenvolvedor de aplicativos
Exclua a fila SQS.	No console do Amazon SQS, no painel Filas, escolha a fila SQS que você criou e, em seguida, escolha Excluir.	Desenvolvedor de aplicativos

Recursos relacionados

- SQS- SendMessage (documentação do API Gateway)
- Conversões de tipo de conteúdo no API Gateway (documentação do API Gateway)

- variáveis $util (documentação do API Gateway)
- Como faço para integrar uma API REST do API Gateway com o Amazon SQS e resolver erros comuns? (AWS Re:postar artigo)

Processe eventos de forma assíncrona com o Amazon API Gateway e o AWS Lambda

Criado por Andrea Meroni (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) e Michael Wallner (AWS)

Resumo

O Amazon API Gateway é um serviço totalmente gerenciado que os desenvolvedores podem usar para criar, publicar, manter, monitorar e proteger APIs em qualquer escala. Ele lida com as tarefas envolvidas na aceitação e processamento de até centenas de milhares de chamadas de API simultâneas.

Uma cota de serviço importante do API Gateway é o tempo limite de integração. O tempo limite é o tempo máximo em que um serviço de back-end deve retornar uma resposta antes que a API REST retorne um erro. O limite rígido de 29 segundos geralmente é aceitável para cargas de trabalho síncronas. No entanto, esse limite representa um desafio para os desenvolvedores que desejam usar o API Gateway com cargas de trabalho assíncronas.

Esse padrão mostra um exemplo de arquitetura para processar eventos de forma assíncrona usando o API Gateway e. AWS Lambda A arquitetura suporta a execução de trabalhos de processamento com duração de até 15 minutos e usa uma API REST básica como interface.

O Projen é usado para configurar o ambiente de desenvolvimento local e implantar a arquitetura de exemplo em um destino Conta da AWS, em combinação com o AWS Cloud Development Kit (AWS CDK) Toolkit, o Docker e o Node.js. O Projen configura automaticamente um ambiente virtual Python com pré-confirmação e as ferramentas usadas para garantia de qualidade de código, verificação de segurança e teste de unidade. Para obter mais informações, consulte a seção Ferramentas.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- As seguintes ferramentas instaladas em sua estação de trabalho:
  - AWS Cloud Development Kit (AWS CDK) Kit de ferramentas versão 2.85.0
  - Docker versão 20.10.21
  - Node.js versão 18.13.0

- Versão do projeto 0.71.111
- Python versão 3.9.16

Limitações

- O tempo de execução máximo de um trabalho é limitado pelo tempo de execução máximo das funções Lambda (15 minutos).
- O número máximo de solicitações de trabalho simultâneas é limitado pela simultaneidade reservada da função Lambda.

Arquitetura

O diagrama a seguir mostra a interação da API de trabalhos com as funções Lambda de processamento e tratamento de erros de eventos, com eventos armazenados em um arquivo de eventos da Amazon. EventBridge

Um fluxo de trabalho típico inclui as seguintes etapas:

1. Você se autentica no AWS Identity and Access Management (IAM) e obtém credenciais de segurança.
2. Você envia uma `POST` solicitação HTTP para o endpoint da API `/jobs` jobs, especificando os parâmetros do trabalho no corpo da solicitação.
3. A API de jobs, que é uma API REST do API Gateway, retorna para você uma resposta HTTP que contém o identificador do trabalho.
4. A API de trabalhos invoca de forma assíncrona a função Lambda de processamento de eventos.
5. A função de processamento de eventos processa o evento e, em seguida, coloca os resultados do trabalho na tabela de trabalhos do Amazon DynamoDB
6. Você envia uma `GET` solicitação HTTP para o endpoint da API de `/jobs/{jobId}` trabalhos, com o identificador do trabalho da etapa 3 como`{jobId}`.
7. A API de jobs consulta a tabela do `jobs` DynamoDB para recuperar os resultados do trabalho.
8. A API de trabalhos retorna uma resposta HTTP que contém os resultados do trabalho.
9. Se o processamento do evento falhar, a função de processamento de eventos enviará o evento para a função de tratamento de erros.
10. A função de tratamento de erros coloca os parâmetros do trabalho na tabela do DynamoDB`jobs`.

11. Você pode recuperar os parâmetros do trabalho enviando uma `GET` solicitação HTTP para o endpoint da API `/jobs/{jobId}` jobs.
12. Se o tratamento de erros falhar, a função de tratamento de erros enviará o evento para um arquivo de EventBridge eventos.

    Você pode reproduzir os eventos arquivados usando. EventBridge

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir com os serviços da AWS por meio de comandos em seu shell de linha de comando.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, funções Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Outras ferramentas

- autopep8 formata automaticamente o código Python com base no guia de estilo Python Enhancement Proposal (PEP) 8.
- O Bandit escaneia o código Python para encontrar problemas comuns de segurança.
- O Commitizen é um verificador e gerador de commits do Git. `CHANGELOG`
- cfn-lint é um linter AWS CloudFormation
- O Checkov é uma ferramenta estática de análise de código que verifica a infraestrutura como código (IaC) em busca de configurações incorretas de segurança e conformidade.

- jq é uma ferramenta de linha de comando para analisar JSON.
- O Postman é uma plataforma de API.
- pre-commit é um gerenciador de ganchos do Git.
- O Projen é um gerador de projetos.
- pytest é uma estrutura Python para escrever testes pequenos e legíveis.

Repositório de código

Esse exemplo de código de arquitetura pode ser encontrado no Processamento GitHub assíncrono de eventos com o API Gateway e o repositório Lambda.

Práticas recomendadas

- Esse exemplo de arquitetura não inclui o monitoramento da infraestrutura implantada. Se seu caso de uso exigir monitoramento, avalie a adição de construções de monitoramento CDK ou outra solução de monitoramento.
- Esse exemplo de arquitetura usa permissões do IAM para controlar o acesso à API de trabalhos. Qualquer pessoa autorizada a assumir o `JobsAPIInvokeRole` poderá invocar a API de trabalhos. Como tal, o mecanismo de controle de acesso é binário. Se seu caso de uso exigir um modelo de autorização mais complexo, avalie usando um mecanismo de controle de acesso diferente.
- Quando um usuário envia uma `POST` solicitação HTTP para o endpoint da API `/jobs` jobs, os dados de entrada são validados em dois níveis diferentes:
  - O Amazon API Gateway é responsável pela validação da primeira solicitação.
  - A função de processamento de eventos executa a segunda solicitação.

    Nenhuma validação é realizada quando o usuário faz uma `GET` solicitação HTTP para o endpoint da API `/jobs/{jobId}` jobs. Se seu caso de uso exigir validação adicional de entrada e um maior nível de segurança, avalie o uso do AWS WAF para proteger sua API.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositór io localmente, execute o seguinte comando: `git clone https://g ithub.com/aws-samp les/asynchronous-e vent-processing-api- gateway-lambda-cdk.git`	DevOps engenheiro

Configure o projeto.	Mude o diretório para a raiz do repositório e configure o ambiente virtual Python e todas as ferramentas usando o Projen:
	`cd asynchronous-event -processing-api-ga teway-api-gateway- lambda-cdk`
	`npx projen`
		DevOps engenheiro

Instale ganchos de pré-confi rmação.	Para instalar ganchos de pré-confirmação, faça o seguinte: 1. Ative o ambiente virtual Python: `source .env/bin/ activate` 2. Instale os ganchos de pré-confirmação:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`pre-commit install` `pre-commit install --hook-type commit-msg`	

Implemente a arquitetura de exemplo

Tarefa	Descrição	Habilidades necessárias
Bootstrap AWS CDK.	Para inicializar AWS CDK no seu Conta da AWS, execute o seguinte comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Implante a arquitetura de exemplo.	Para implantar a arquitetura de exemplo no seu Conta da AWS, execute o seguinte comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Teste a arquitetura

Tarefa	Descrição	Habilidades necessárias
Instale os pré-requisitos de teste.	Instale em sua estação de trabalho o AWS Command Line Interface (AWS CLI), o Postman e o jq.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	O uso do Postman para testar essa arquitetura de exemplo é sugerido, mas não obrigatório. Se você escolher uma ferramenta alternativa de teste de API, certifique-se de que ela seja compatível com a autenticação AWS Signature versão 4 e consulte os endpoints de API expostos que podem ser inspecionados exportando a API REST.	

Tarefa	Descrição	Habilidades necessárias
Suponha que `JobsAPIInvokeRole` o.	Suponha `JobsAPIInvokeRole` que o que foi impresso como saída do comando deploy: `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Configure o Postman.	1. Para importar a coleção Postman incluída no repositório, siga as instruções na documentação do Postman. 2. Defina `JobsAPI` as variáveis com os seguintes valores: • `accessKey` – O valor do `Credentials.AccessKeyId` atributo do `assume-role` comando • `baseUrl`– O valor da `JobsApiJobsAPIEndpoint` saída do comando deploy, sem a barra final • `region`– O valor de Região da AWS onde você implantou a arquitetura de exemplo • `seconds`– O valor do parâmetro de entrada para o trabalho de exemplo. Deve ser um número inteiro positivo • `secretKey` – O valor do `Credentials.SecretAccessKey` atributo do `assume-role` comando • `sessionToken` – O valor do `Credentia`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`ls.SessionToken` atributo do `assume-role` comando	
Teste a arquitetura de exemplo.	Para testar a arquitetura de exemplo, envie solicitações para a API de trabalhos. Para obter mais informações, consulte a documentação do Postman.	DevOps engenheiro

Solução de problemas

Problema	Solução
A destruição e a reimplantação subsequente da arquitetura de exemplo falham porque o grupo de CloudWatch logs do Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` já existe.	1. Se necessário, exporte seus dados de log para o Amazon S3. 2. Exclua o grupo CloudWatch de registros de registros `/aws/apigateway/JobsAPIAccessLogs` . 3. Reimplante a arquitetura de exemplo.

Recursos relacionados

- Modelo de mapeamento do API Gateway e referência de variável de registro de acesso
- Configurar a invocação assíncrona da função Lambda de back-end

Processe eventos de forma assíncrona com o Amazon API Gateway e o Amazon DynamoDB Streams

Criado por Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) e Michael Wallner (AWS)

Resumo

O Amazon API Gateway é um serviço totalmente gerenciado que os desenvolvedores podem usar para criar, publicar, manter, monitorar e proteger APIs em qualquer escala. Ele lida com as tarefas envolvidas na aceitação e processamento de até centenas de milhares de chamadas de API simultâneas.

Uma cota de serviço importante do API Gateway é o tempo limite de integração. O tempo limite é o tempo máximo em que um serviço de back-end deve retornar uma resposta antes que a API REST retorne um erro. O limite rígido de 29 segundos geralmente é aceitável para cargas de trabalho síncronas. No entanto, esse limite representa um desafio para os desenvolvedores que desejam usar o API Gateway com cargas de trabalho assíncronas.

Esse padrão mostra um exemplo de arquitetura para processar eventos de forma assíncrona usando API Gateway, Amazon DynamoDB Streams e. AWS Lambda A arquitetura suporta a execução de trabalhos de processamento paralelo com os mesmos parâmetros de entrada e usa uma API REST básica como interface. Neste exemplo, usar o Lambda como back-end limita a duração dos trabalhos a 15 minutos. Você pode evitar esse limite usando um serviço alternativo para processar eventos recebidos (por exemplo, AWS Fargate).

O Projen é usado para configurar o ambiente de desenvolvimento local e implantar a arquitetura de exemplo em um destino Conta da AWS, em combinação com o AWS Cloud Development Kit (AWS CDK) Toolkit, o Docker e o Node.js. O Projen configura automaticamente um ambiente virtual Python com pré-confirmação e as ferramentas usadas para garantia de qualidade de código, verificação de segurança e teste de unidade. Para obter mais informações, consulte a seção Ferramentas.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- As seguintes ferramentas instaladas em sua estação de trabalho:

- AWS Cloud Development Kit (AWS CDK) Kit de ferramentas versão 2.85.0 ou posterior
- Docker versão 20.10.21 ou posterior
- Node.js versão 18 ou posterior
- Projen versão 0.71.111 ou posterior
- Python versão 3.9.16 ou posterior

Limitações

- O número máximo recomendado de leitores para o DynamoDB Streams é dois para evitar limitações.
- O tempo de execução máximo de um trabalho é limitado pelo tempo de execução máximo das funções Lambda (15 minutos).
- O número máximo de solicitações de trabalho simultâneas é limitado pela simultaneidade reservada das funções do Lambda.

Arquitetura

Arquitetura

O diagrama a seguir mostra a interação da API de jobs com o DynamoDB Streams e as funções Lambda de processamento de eventos e tratamento de erros, com eventos armazenados em um arquivo de eventos da Amazon. EventBridge

Um fluxo de trabalho típico inclui as seguintes etapas:

1. Você se autentica no AWS Identity and Access Management (IAM) e obtém credenciais de segurança.
2. Você envia uma `POST` solicitação HTTP para o endpoint da API `/jobs` jobs, especificando os parâmetros do trabalho no corpo da solicitação.
3. A API de trabalhos retorna para você uma resposta HTTP que contém o identificador do trabalho.
4. A API de trabalhos coloca os parâmetros do trabalho na tabela do `jobs_table` Amazon DynamoDB.
5. A tabela do `jobs_table` DynamoDB Stream do DynamoDB invoca as funções Lambda de processamento de eventos.

6. As funções Lambda de processamento de eventos processam o evento e, em seguida, colocam os resultados do trabalho na tabela do DynamoDB. `jobs_table` Para ajudar a garantir resultados consistentes, as funções de processamento de eventos implementam um mecanismo de bloqueio otimista.
7. Você envia uma `GET` solicitação HTTP para o endpoint da API de `/jobs/{jobId}` trabalhos, com o identificador do trabalho da etapa 3 como`{jobId}`.
8. A API de jobs consulta a tabela do `jobs_table` DynamoDB para recuperar os resultados do trabalho.
9. A API de trabalhos retorna uma resposta HTTP que contém os resultados do trabalho.
10. Se o processamento do evento falhar, o mapeamento de origem da função de processamento de eventos envia o evento para o tópico de tratamento de erros do Amazon Simple Notification Service (Amazon SNS).
11. O tópico SNS de tratamento de erros envia o evento de forma assíncrona para a função de tratamento de erros.
12. A função de tratamento de erros coloca os parâmetros do trabalho na tabela do DynamoDB`jobs_table`.

    Você pode recuperar os parâmetros do trabalho enviando uma `GET` solicitação HTTP para o endpoint da API `/jobs/{jobId}` jobs.
13. Se o tratamento de erros falhar, a função de tratamento de erros enviará o evento para um arquivo da Amazon EventBridge .

    Você pode reproduzir os eventos arquivados usando. EventBridge

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da AWS Cloud em código.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, funções do Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras contas da AWS.

- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.

Outras ferramentas

- autopep8 formata automaticamente o código Python com base no guia de estilo Python Enhancement Proposal (PEP) 8.
- O Bandit escaneia o código Python para encontrar problemas comuns de segurança.
- O Commitizen é um verificador e gerador de commits do Git. `CHANGELOG`
- cfn-lint é um linter AWS CloudFormation
- O Checkov é uma ferramenta estática de análise de código que verifica a infraestrutura como código (IaC) em busca de configurações incorretas de segurança e conformidade.
- jq é uma ferramenta de linha de comando para analisar JSON.
- O Postman é uma plataforma de API.
- pre-commit é um gerenciador de ganchos do Git.
- O Projen é um gerador de projetos.
- pytest é uma estrutura Python para escrever testes pequenos e legíveis.

Repositório de código

Esse exemplo de código de arquitetura pode ser encontrado no repositório GitHub Asynchronous Processing with API Gateway e DynamoDB Streams.

Práticas recomendadas

- Esse exemplo de arquitetura não inclui o monitoramento da infraestrutura implantada. Se seu caso de uso exigir monitoramento, avalie a adição de construções de monitoramento CDK ou outra solução de monitoramento.
- Esse exemplo de arquitetura usa permissões do IAM para controlar o acesso à API de trabalhos. Qualquer pessoa autorizada a assumir o `JobsAPIInvokeRole` poderá invocar a API de trabalhos. Como tal, o mecanismo de controle de acesso é binário. Se seu caso de uso exigir

um modelo de autorização mais complexo, avalie usando um mecanismo de controle de acesso diferente.

- Quando um usuário envia uma `POST` solicitação HTTP para o endpoint da API `/jobs` jobs, os dados de entrada são validados em dois níveis diferentes:
  - O API Gateway é responsável pela validação da primeira solicitação.
  - A função de processamento de eventos executa a segunda solicitação.

  Nenhuma validação é realizada quando o usuário faz uma `GET` solicitação HTTP para o endpoint da API `/jobs/{jobId}` jobs. Se seu caso de uso exigir validação adicional de entrada e um maior nível de segurança, avalie o uso AWS WAF para proteger sua API.

- Para evitar a limitação, a documentação do DynamoDB Streams desencoraja os usuários de lerem com mais de dois consumidores o fragmento do mesmo stream. Para ampliar o número de consumidores, recomendamos o uso do Amazon Kinesis Data Streams.
- O bloqueio otimista foi usado neste exemplo para garantir atualizações consistentes dos itens na tabela do DynamoDB`jobs_table`. Dependendo do requisito do caso de uso, talvez seja necessário implementar mecanismos de travamento mais confiáveis, como travamento pessimista.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositór io localmente, execute o seguinte comando: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-dynamodb-streams-cdk.git`	DevOps engenheiro
Configure o projeto.	Mude o diretório para a raiz do repositório e configure	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	o ambiente virtual Python e todas as ferramentas usando o Projen:
	`cd asynchronous-event-processing-api-gateway-api-gateway-dynamodb-streams-cdk`
	`npx projen`	

Instale ganchos de pré-confirmação.	Para instalar ganchos de pré-confirmação, faça o seguinte:
	1. Ative o ambiente virtual Python:
	`source .env/bin/activate`
	2. Instale os ganchos de pré-confirmação:
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`
		DevOps engenheiro

Implemente a arquitetura de exemplo

Tarefa	Descrição	Habilidades necessárias
Bootstrap AWS CDK.	Para inicializar AWS CDKno seu Conta da AWS, execute o seguinte comando:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	
Implante a arquitetura de exemplo.	Para implantar a arquitetura de exemplo no seu Conta da AWS, execute o seguinte comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Teste a arquitetura

Tarefa	Descrição	Habilidades necessárias
Instale os pré-requisitos de teste.	Instale em sua estação de trabalho o AWS Command Line Interface (AWS CLI), o Postman e o jq. O uso do Postman para testar essa arquitetura de exemplo é sugerido, mas não obrigatório. Se você escolher uma ferramenta alternativa de teste de API, certifique-se de que ela seja compatível com a autenticação do AWS Signature versão 4 e consulte os endpoints de API expostos que podem ser inspecionados exportando a API REST.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Suponha que `JobsAPIInvokeRole` o.	Suponha `JobsAPIInvokeRole` que o que foi impresso como saída do `deploy` comando: `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Configure o Postman.	• Para importar a coleção Postman incluída no repositório, siga as instruções na documentação do Postman.
	• Defina `JobsAPI` as variáveis com os seguintes valores:
	  • `accessKey` – O valor do `Credentials.AccessKeyId` atributo do `assume-role` comando.
	  • `baseUrl`– O valor da `JobsApiJobsAPIEndpoint` saída do `deploy` comando, sem a barra final.
	  • `region`– O valor de Região da AWS onde você implantou a arquitetura de exemplo.
	  • `seconds`– O valor do parâmetro de entrada para o trabalho de exemplo. Deve ser um número inteiro positivo.
	  • `secretKey` – O valor do `Credentials.SecretAccessKey` atributo do `assume-role` comando.
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• `sessionToken` – O valor do `Credentials.SessionToken` atributo do `assume-role` comando.	
Teste a arquitetura de exemplo.	Para testar a arquitetura de exemplo, envie solicitações para a API de trabalhos. Para obter mais informações, consulte a documentação do Postman.	DevOps engenheiro

Solução de problemas

Problema	Solução
A destruição e a reimplantação subsequente da arquitetura de exemplo falham porque o grupo de CloudWatch logs do Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` já existe.	1. Se necessário, exporte seus dados de log para o Amazon Simple Storage Service (Amazon S3). 2. Exclua o grupo CloudWatch de registros de registros `/aws/apigateway/JobsAPIAccessLogs` . 3. Reimplante a arquitetura de exemplo.

Recursos relacionados

- Modelo de mapeamento do API Gateway e referência de variável de registro de acesso
- Alterar a captura de dados para o DynamoDB Streams
- Bloqueio otimista com número de versão
- Usando o Kinesis Data Streams para capturar alterações no DynamoDB

Processe eventos de forma assíncrona com o Amazon API Gateway, o Amazon SQS e o AWS Fargate

Criado por Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) e Michael Wallner (AWS)

Resumo

O Amazon API Gateway é um serviço totalmente gerenciado que os desenvolvedores podem usar para criar, publicar, manter, monitorar e proteger APIs em qualquer escala. Ele lida com as tarefas envolvidas na aceitação e processamento de até centenas de milhares de chamadas de API simultâneas.

Uma cota de serviço importante do API Gateway é o tempo limite de integração. O tempo limite é o tempo máximo em que um serviço de back-end deve retornar uma resposta antes que a API REST retorne um erro. O limite rígido de 29 segundos geralmente é aceitável para cargas de trabalho síncronas. No entanto, esse limite representa um desafio para os desenvolvedores que desejam usar o API Gateway com cargas de trabalho assíncronas.

Esse padrão mostra um exemplo de arquitetura para processar eventos de forma assíncrona usando o API Gateway, o Amazon Simple Queue Service (Amazon SQS) e. AWS Fargate A arquitetura suporta a execução de trabalhos de processamento sem restrições de duração e usa uma API REST básica como interface.

O Projen é usado para configurar o ambiente de desenvolvimento local e implantar a arquitetura de exemplo em um destino Conta da AWS, em combinação com o AWS Cloud Development Kit (AWS CDK)Docker e o Node.js. O Projen configura automaticamente um ambiente virtual Python com pré-confirmação e as ferramentas usadas para garantia de qualidade de código, verificação de segurança e teste de unidade. Para obter mais informações, consulte a seção Ferramentas.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- As seguintes ferramentas instaladas em sua estação de trabalho:
  - AWS Cloud Development Kit (AWS CDK) Kit de ferramentas versão 2.85.0 ou posterior
  - Docker versão 20.10.21 ou posterior

- Node.js versão 18 ou posterior
- Projen versão 0.71.111 ou posterior
- Python versão 3.9.16 ou posterior

Limitações

- Os trabalhos simultâneos são limitados a 500 tarefas por minuto, que é o número máximo de tarefas que o Fargate pode provisionar.

Arquitetura

O diagrama a seguir mostra a interação da API de trabalhos com a tabela do `jobs` Amazon DynamoDB, o serviço Fargate de processamento de eventos e a função de tratamento de erros. AWS Lambda Os eventos são armazenados em um arquivo de EventBridge eventos da Amazon.

Um fluxo de trabalho típico inclui as seguintes etapas:

1. Você se autentica no AWS Identity and Access Management (IAM) e obtém credenciais de segurança.
2. Você envia uma `POST` solicitação HTTP para o endpoint da API `/jobs` jobs, especificando os parâmetros do trabalho no corpo da solicitação.
3. A API de jobs, que é uma API REST do API Gateway, retorna para você uma resposta HTTP que contém o identificador do trabalho.
4. A API de trabalhos envia uma mensagem para a fila do SQS.
5. Fargate extrai a mensagem da fila do SQS, processa o evento e, em seguida, coloca os resultados do trabalho na tabela do DynamoDB. `jobs`
6. Você envia uma `GET` solicitação HTTP para o endpoint da API de `/jobs/{jobId}` trabalhos, com o identificador do trabalho da etapa 3 como`{jobId}`.
7. A API de jobs consulta a tabela do `jobs` DynamoDB para recuperar os resultados do trabalho.
8. A API de trabalhos retorna uma resposta HTTP que contém os resultados do trabalho.
9. Se o processamento do evento falhar, a fila SQS enviará o evento para a fila de cartas mortas (DLQ).
10. Um EventBridge evento inicia a função de tratamento de erros.
11. A função de tratamento de erros coloca os parâmetros do trabalho na tabela do DynamoDB`jobs`.

12. Você pode recuperar os parâmetros do trabalho enviando uma `GET` solicitação HTTP para o endpoint da API `/jobs/{jobId}` jobs.
13. Se o tratamento de erros falhar, a função de tratamento de erros enviará o evento para um EventBridge arquivo.

    Você pode reproduzir os eventos arquivados usando. EventBridge

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- AWS Fargateajuda você a executar contêineres sem precisar gerenciar servidores ou instâncias do Amazon Elastic Compute Cloud EC2 (Amazon). É usado em conjunto com o Amazon Elastic Container Service (Amazon ECS).
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, funções Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.

Outras ferramentas

- autopep8 formata automaticamente o código Python com base no guia de estilo Python Enhancement Proposal (PEP) 8.
- O Bandit escaneia o código Python para encontrar problemas comuns de segurança.
- O Commitizen é um verificador e gerador de commits do Git. `CHANGELOG`

- cfn-lint é um linter AWS CloudFormation
- O Checkov é uma ferramenta estática de análise de código que verifica a infraestrutura como código (IaC) em busca de configurações incorretas de segurança e conformidade.
- jq é uma ferramenta de linha de comando para analisar JSON.
- O Postman é uma plataforma de API.
- pre-commit é um gerenciador de ganchos do Git.
- O Projen é um gerador de projetos.
- pytest é uma estrutura Python para escrever testes pequenos e legíveis.

Repositório de código

Esse exemplo de código de arquitetura pode ser encontrado no repositório GitHub Asynchronous Processing with API Gateway e SQS.

Práticas recomendadas

- Esse exemplo de arquitetura não inclui o monitoramento da infraestrutura implantada. Se seu caso de uso exigir monitoramento, avalie a adição de construções de monitoramento CDK ou outra solução de monitoramento.
- Esse exemplo de arquitetura usa permissões do IAM para controlar o acesso à API de trabalhos. Qualquer pessoa autorizada a assumir o `JobsAPIInvokeRole` poderá invocar a API de trabalhos. Como tal, o mecanismo de controle de acesso é binário. Se seu caso de uso exigir um modelo de autorização mais complexo, avalie usando um mecanismo de controle de acesso diferente.
- Quando um usuário envia uma `POST` solicitação HTTP para o endpoint da API `/jobs` jobs, os dados de entrada são validados em dois níveis diferentes:
  - O API Gateway é responsável pela validação da primeira solicitação.
  - A função de processamento de eventos executa a segunda solicitação.

    Nenhuma validação é realizada quando o usuário faz uma `GET` solicitação HTTP para o endpoint da API `/jobs/{jobId}` jobs. Se seu caso de uso exigir validação adicional de entrada e um maior nível de segurança, avalie o uso AWS WAF para proteger sua API.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositór io localmente, execute o seguinte comando: `git clone https://g ithub.com/aws-samp les/asynchronous-e vent-processing-api- gateway-sqs-cdk.git`	DevOps engenheiro

Configure o projeto.	Mude o diretório para a raiz do repositório e configure o ambiente virtual Python e todas as ferramentas usando o Projen:
	`cd asynchronous-event -processing-api-ga teway-api-gateway- sqs-cdk`
	`npx projen`
		DevOps engenheiro

Instale ganchos de pré-confi rmação.	Para instalar ganchos de pré-confirmação, faça o seguinte: 1. Ative o ambiente virtual Python: `source .env/bin/ activate` 2. Instale os ganchos de pré-confirmação:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`pre-commit install` `pre-commit install --hook-type commit-msg`	

Implemente a arquitetura de exemplo

Tarefa	Descrição	Habilidades necessárias
Bootstrap AWS CDK.	Para inicializar AWS CDKno seu Conta da AWS, execute o seguinte comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Implante a arquitetura de exemplo.	Para implantar a arquitetura de exemplo no seu Conta da AWS, execute o seguinte comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Teste a arquitetura

Tarefa	Descrição	Habilidades necessárias
Instale os pré-requisitos de teste.	Instale em sua estação de trabalho o AWS Command Line Interface (AWS CLI), o Postman e o jq.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	O uso do Postman para testar essa arquitetura de exemplo é sugerido, mas não obrigatório. Se você escolher uma ferramenta alternativa de teste de API, certifique-se de que ela seja compatível com a autenticação AWS Signature versão 4 e consulte os endpoints de API expostos que podem ser inspecionados exportando a API REST.	

Tarefa	Descrição	Habilidades necessárias
Suponha que `JobsAPIInvokeRole` o.	Suponha `JobsAPIInvokeRole` que o que foi impresso como saída do `deploy` comando: `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Configure o Postman.	• Para importar a coleção Postman incluída no repositório, siga as instruções na documentação do Postman.
	• Defina `JobsAPI` as variáveis com os seguintes valores:
	  • `accessKey` – O valor do `Credentials.AccessKeyId` atributo do `assume-role` comando.
	  • `baseUrl`– O valor da `JobsApiJobsAPIEndpoint` saída do `deploy` comando, sem a barra final.
	  • `region`– O valor de Região da AWS onde você implantou a arquitetura de exemplo.
	  • `seconds`– O valor do parâmetro de entrada para o trabalho de exemplo. Deve ser um número inteiro positivo.
	  • `secretKey` – O valor do `Credentials.SecretAccessKey` atributo do `assume-role` comando.
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• `sessionToken` – O valor do `Credentials.SessionToken` atributo do `assume-role` comando.	
Teste a arquitetura de exemplo.	Para testar a arquitetura de exemplo, envie solicitações para a API de trabalhos. Para obter mais informações, consulte a documentação do Postman.	DevOps engenheiro

Solução de problemas

Problema	Solução
A destruição e a reimplantação subsequente da arquitetura de exemplo falham porque o grupo de CloudWatch logs do Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` já existe.	1. Se necessário, exporte seus dados de log para o Amazon Simple Storage Service (Amazon S3). 2. Exclua o grupo CloudWatch de registros de registros `/aws/apigateway/JobsAPIAccessLogs` . 3. Reimplante a arquitetura de exemplo.
A destruição e a reimplantação subsequente da arquitetura de exemplo falham porque o grupo de CloudWatch registros de registros `/aws/ecs/EventProcessingServiceLogs` já existe.	1. Se necessário, exporte seus dados de log para o Amazon S3. 2. Excluir o grupo CloudWatch de registros de registros `/aws/ecs/EventProcessingServiceLogs.` 3. Reimplante a arquitetura de exemplo.

Recursos relacionados

- Modelo de mapeamento do API Gateway e referência de variável de registro de acesso
- Como faço para integrar uma API REST do API Gateway com o Amazon SQS e resolver erros comuns?

Execute tarefas do AWS Systems Manager Automation de forma síncrona a partir do AWS Step Functions

Criado por Elie El khoury (AWS)

Resumo

Esse padrão explica como integrar AWS Step Functions com AWS Systems Manager o. Ele usa integrações de serviços do AWS SDK para chamar a startAutomationExecutionAPI Systems Manager com um token de tarefa de um fluxo de trabalho de uma máquina de estado e faz uma pausa até que o token retorne com uma chamada bem-sucedida ou com falha. Para demonstrar a integração, esse padrão implementa um invólucro de documento de automação (runbook) ao redor do `AWS-RunPowerShellScript` documento `AWS-RunShellScript` ou e é usado `.waitForTaskToken` para chamar ou de forma síncrona. `AWS-RunShellScript` `AWS-RunPowerShellScript` Para obter mais informações sobre as integrações de serviços do AWS SDK no Step Functions, consulte o AWS Step Functions Developer Guide.

O Step Functions é um serviço de fluxo de trabalho visual de baixo código que você pode usar para criar aplicativos distribuídos, automatizar processos de negócios e de TI e criar pipelines de dados e aprendizado de máquina usando serviços. AWS Os fluxos de trabalho gerenciam falhas, novas tentativas, paralelização, integrações de serviços e observabilidade para que você possa se concentrar em uma lógica de negócios de maior valor.

A automação, uma capacidade do AWS Systems Manager, simplifica tarefas comuns de manutenção, implantação e remediação, Serviços da AWS como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift e Amazon Simple Storage Service (Amazon S3). Com o Automation, você tem controle granular sobre a simultaneidade de suas automações. Por exemplo, você pode especificar quantos recursos a destinar simultaneamente e quantos erros podem ocorrer antes que uma automação seja interrompida.

Para obter detalhes da implementação, incluindo etapas, parâmetros e exemplos do runbook, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Uma AWS conta ativa

- AWS Identity and Access Management Permissões (IAM) para acessar Step Functions e Systems Manager
- Uma EC2 instância com o Systems Manager Agent (SSM Agent) instalado na instância
- Um perfil de instância do IAM para Systems Manager anexado à instância em que você planeja executar o runbook
- Um papel de Step Functions que tem as seguintes permissões do IAM (que seguem o princípio do privilégio mínimo):

```
{
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "*"
 }
```

Versões do produto

- Esquema do documento SSM versão 0.3 ou mais recente
- SSM Agent versão 2.3.672.0 ou mais recente

Arquitetura

Pilha de tecnologias de destino

- AWS Step Functions
- AWS Systems Manager Automation

Arquitetura de destino

Automação e escala

- Esse padrão fornece um AWS CloudFormation modelo que você pode usar para implantar os runbooks em várias instâncias. (Consulte o repositório de implementação do GitHub Step Functions e do Systems Manager.)

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala.

Código

O código desse padrão está disponível no repositório de implementação do GitHub Step Functions and Systems Manager.

Épicos

Crie runbooks

Tarefa	Descrição	Habilidades necessárias
Baixe o CloudFormation modelo.	Baixe o `ssm-automation-documents.cfn.json` modelo da `cloudformation` pasta do GitHub repositório.	AWS DevOps
Crie runbooks.	Faça login no AWS Management Console, abra o AWS CloudFormation console e implante o modelo. Para obter mais informações sobre	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	a implantação CloudForm ation de modelos, consulte Criação de uma pilha no AWS CloudFormation console na CloudFormation documenta ção. O CloudFormation modelo implanta três recursos: • `SfnRunCommandByIns tanceIds` — Runbook que permite executar `AWS-RunShellScript` ou usar `AWS-RunPo werShellScript` a instância IDs. • `SfnRunCommandByTar gets` — Runbook que permite correr `AWS-RunSh ellScript` ou `AWS-RunPowerShellScript` usar alvos. • `SSMSyncRole` — A função do IAM assumida pelos runbooks.	

Criar um exemplo de máquina de estado

Tarefa	Descrição	Habilidades necessárias
Criar uma máquina de estado de teste.	Siga as instruções no Guia do AWS Step Functions desenvolvedor para criar e	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	executar uma máquina de estado. Para a definição, use o código a seguir. Certifiqu e-se de atualizar o valor `InstanceIds` com o ID de uma instância válida habilitad a para o Systems Manager em sua conta. `{ "Comment": "A description of my state machine", "StartAt": "StartAutomationWaitForCallBack", "States": { "StartAutomationWaitForCallBack": { "Type": "Task", "Resource": "arn:aws:states:::aws-sdk:ssm:startAutomationExecution.waitForTaskToken", "Parameters": { "DocumentName": "SfnRunCommandByInstanceIds", "Parameters": { "InstanceIds": ["i-1234567890abcdef0"], "taskToken.$": "States.Array($$.Task.Token)", "workingDirectory": [`	

Tarefa	Descrição	Habilidades necessárias
	"/home/ssm-user/"], "Commands": ["echo \"This is a test running automation waitForTaskToken\" >> automation.log", "sleep 100"], "executionTimeout": ["10800"], "deliveryTimeout": ["30"], "shell": ["Shell"] } }, "End": true } } } Esse código chama o runbook para executar dois comandos que demonstram a chamada `waitForTaskToken` para Systems Manager Automation. O valor do `shell` parâmetro (`ShellouPowerShell`) determina se o documento de automação é executado `AWS-`	

Tarefa	Descrição	Habilidades necessárias
	`RunShellScript` ou `AWS-RunPowerShellScript`. A tarefa grava "Este é um waitForTask token de automação de execução de teste" no `/home/ssm-user/automation.log` arquivo e, em seguida, dorme por 100 segundos antes de responder com o token da tarefa e liberar a próxima tarefa no fluxo de trabalho. Se você quiser chamar o runbook `SfnRunCommandByTargets` em vez disso, substitua a seção `Parameters` do código anterior pela seguinte: `"Parameters": { "Targets": [ { "Key": "InstanceIds", "Values": [ "i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE" ] } ],`	

Tarefa	Descrição	Habilidades necessárias
Atualize o perfil do IAM para a máquina de estado.	A etapa anterior cria automaticamente um perfil do IAM dedicado para a máquina de estado. No entanto, ele não concede permissões para chamar o runbook. Atualize o perfil adicionando as seguintes permissões: `{ "Effect": "Allow", "Action": "ssm:StartAutomationExecution", "Resource": "*" }`	AWS DevOps
Valide as chamadas síncronas.	Execute a máquina de estado para validar a chamada síncrona entre Step Functions e Systems Manager Automation. Para obter um exemplo de resultado, consulte a seção Informações adicionais.	AWS DevOps

Recursos relacionados

- Introdução ao AWS Step Functions (Guia AWS Step Functions do desenvolvedor)
- Aguarde um retorno de chamada com o token da tarefa (Guia do AWS Step Functions desenvolvedor, padrões de integração de serviços)
- Chamadas de API send_task_success and send_task_failure (documentação do Boto3)
- AWS Systems Manager Automação (Guia AWS Systems Manager do usuário)

Mais informações

Detalhes da implantação

Esse padrão fornece um CloudFormation modelo que implanta dois runbooks do Systems Manager:

- `SfnRunCommandByInstanceIds`executa o `AWS-RunPowerShellScript` comando `AWS-RunShellScript` or usando instance IDs.
- `SfnRunCommandByTargets`executa o `AWS-RunPowerShellScript` comando `AWS-RunShellScript` or usando alvos.

Cada runbook implementa quatro etapas para obter uma chamada síncrona ao usar a `.waitForTaskToken` opção em Step Functions.

Etapa	Ação	Descrição
1	`Branch`	Verifica o valor do `shell` parâmetro (`Shell`ou`PowerShell`) para decidir se deve ser executado `AWS-RunShellScript` no Linux ou `AWS-RunPowerShellScript` no Windows.
2	`RunCommand_Shell` ou `RunCommand_PowerShell`	Recebe várias entradas e executa o `RunPowerShellScript` comando `RunShellScript` or. Para obter mais informações, verifique a guia Detalhes do documento `RunCommand_Shell` ou `RunCommand_PowerShell` Automação no console do Systems Manager.

3	`SendTaskFailure`	É executado quando a etapa 2 é abortada ou cancelada. Ele chama a API send_task_failure do Step Functions, que aceita três parâmetros como entrada: o token aprovado pela máquina de estado, o erro de falha e uma descrição da causa da falha.
4	`SendTaskSuccess`	É executado quando a etapa 2 é bem-sucedida. Ele chama a API send_task_success do Step Functions, que aceita o token passado pela máquina de estado como entrada.

Parâmetros do runbook

`SfnRunCommandByInstanceIds`livro de corrida:

Nome do parâmetro	Tipo	Opcional ou obrigatório	Descrição
`shell`	String	Obrigatório	O shell de instâncias para decidir se deve ser executado `AWS-RunShellScript` no Linux ou `AWS-RunPowerShellScript` no Windows.
`deliveryTimeout`	Inteiro	Opcional	O tempo, em segundos, de espera pela entrega de um comando ao agente SSM em

			uma instância. Esse parâmetro tem um valor mínimo de 30 (0,5 minuto) e um valor máximo de 2592000 (720 horas).
`executionTimeout`	String	Opcional	O tempo em segundos para um comando ser concluído antes de ser considerado como tendo falhado. O valor padrão é 3600 (1 hora). O valor máximo é 172800 (48 horas).
`workingDirectory`	String	Opcional	O caminho para o diretório de trabalho em sua instância.
`Commands`	StringList	Obrigatório	O script ou comando do shell a ser executado.
`InstanceIds`	StringList	Obrigatório	A IDs das instâncias em que você deseja executar o comando.
`taskToken`	String	Obrigatório	O token de tarefa a ser usado para respostas de retorno de chamada.

`SfnRunCommandByTargets`livro de corrida:

Nome	Tipo	Opcional ou obrigatório	Descrição
`shell`	String	Obrigatório	O shell de instâncias para decidir se deve ser executado `AWS-RunShellScript` no Linux ou `AWS-RunPowerShellScript` no Windows.
`deliveryTimeout`	Inteiro	Opcional	O tempo, em segundos, de espera pela entrega de um comando ao agente SSM em uma instância. Esse parâmetro tem um valor mínimo de 30 (0,5 minuto) e um valor máximo de 2592000 (720 horas).
`executionTimeout`	Inteiro	Opcional	O tempo em segundos para um comando ser concluído antes de ser considerado como tendo falhado. O valor padrão é 3600 (1 hora). O valor máximo é 172800 (48 horas).
`workingDirectory`	String	Opcional	O caminho para o diretório de trabalho em sua instância.

`Commands`	StringList	Obrigatório	O script ou comando do shell a ser executado.
`Targets`	MapList	Obrigatório	Uma matriz de critérios de pesquisa que identifica instâncias usando os pares de chave-valor que você especificar. Por exemplo: `[{"Key":"InstanceIds","Values":["i-02573cafcfEXAMPLE","i-0471e04240EXAMPLE"]}]`
`taskToken`	String	Obrigatório	O token de tarefa a ser usado para respostas de retorno de chamada.

Exemplo de saída

A tabela a seguir fornece um exemplo de saída da Step Function. Ele mostra que o tempo total de execução é superior a 100 segundos entre a etapa 5 (`TaskSubmitted`) e a etapa 6 (`TaskSucceeded`). Isso demonstra que a função step aguardou a conclusão do `sleep 100` comando antes de passar para a próxima tarefa no fluxo de trabalho.

ID	Tipo	Etapa	Recurso	Tempo decorrido (ms)	Timestamp

1	ExecutionStarted		-	0	11 de março de 2022 14:50:34.303
2	TaskStateEntered	StartAutomationWaitForCallBack	-	40	11 de março de 2022 14:50:34.343
3	TaskScheduled	StartAutomationWaitForCallBack	-	40	11 de março de 2022 14:50:34.343
4	TaskStarted	StartAutomationWaitForCallBack	-	154	11 de março de 2022 14:50:34.457
5	TaskSubmitted	StartAutomationWaitForCallBack	-	657	11 de março de 2022 14:50:34.960
6	TaskSucceeded	StartAutomationWaitForCallBack	-	103835	11 de março de 2022 14:52:18.138
7	TaskStateExited	StartAutomationWaitForCallBack	-	103860	11 de março de 2022 14:52:18.163
8	ExecutionSucceeded		-	103897	11 de março de 2022 14:52:18.200

Execute leituras paralelas de objetos do S3 usando Python em uma função AWS Lambda

Criado por Eduardo Bortoluzzi (AWS)

Resumo

Você pode usar esse padrão para recuperar e resumir uma lista de documentos dos buckets do Amazon Simple Storage Service (Amazon S3) em tempo real. O padrão fornece código de exemplo para objetos de leitura paralela de buckets do S3 na Amazon Web Services ()AWS. O padrão mostra como executar eficientemente tarefas vinculadas à E/S com AWS Lambda funções usando Python.

Uma empresa financeira usou esse padrão em uma solução interativa para aprovar ou rejeitar manualmente transações financeiras correlacionadas em tempo real. Os documentos da transação financeira foram armazenados em um bucket S3 relacionado ao mercado. Um operador selecionou uma lista de documentos do bucket do S3, analisou o valor total das transações calculadas pela solução e decidiu aprovar ou rejeitar o lote selecionado.

As tarefas vinculadas à E/S oferecem suporte a vários threads. Neste código de exemplo, o concurrent.futures. ThreadPoolExecutoré usado com no máximo 30 encadeamentos simultâneos, embora as funções do Lambda suportem até 1.024 encadeamentos (com um desses encadeamentos sendo seu processo principal). Esse limite ocorre porque muitos threads criam problemas de latência devido à mudança de contexto e à utilização de recursos de computação. Você também precisa aumentar o máximo de conexões do pool `botocore` para que todos os threads possam realizar o download do objeto S3 simultaneamente.

O código de exemplo usa um objeto de 8,3 KB, com dados JSON, em um bucket do S3. O objeto é lido várias vezes. Depois que a função Lambda lê o objeto, os dados JSON são decodificados em um objeto Python. Em dezembro de 2024, o resultado após a execução deste exemplo foi de 1.000 leituras processadas em 2,3 segundos e 10.000 leituras processadas em 27 segundos usando uma função Lambda configurada com 2.304 MB de memória. AWS Lambda suporta configurações de memória de 128 MB a 10.240 MB (10 GB), embora aumentar a memória Lambda para além de 2.304 MB não tenha ajudado a diminuir o tempo de execução dessa tarefa específica vinculada à E/S.

A ferramenta AWS Lambda Power Tuning foi usada para testar diferentes configurações de memória Lambda e verificar a melhor performance-to-cost proporção para a tarefa. Para obter os resultados dos testes, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Proficiência com desenvolvimento em Python

Limitações

- Uma função Lambda pode ter no máximo 1.024 processos ou threads de execução.
- Contas da AWS Os novos têm um limite de memória Lambda de 3.008 MB. Ajuste a ferramenta AWS Lambda Power Tuning adequadamente. Para obter mais informações, consulte a seção Solução de problemas.
- O Amazon S3 tem um limite de 5.500 solicitações GET/HEAD por segundo por prefixo particionado.

Versões do produto

- Python 3.9 ou superior
- AWS Cloud Development Kit (AWS CDK) v2
- AWS Command Line Interface (AWS CLI) versão 2
- AWS Lambda Power Tuning 4.3.6 (opcional)

Arquitetura

Pilha de tecnologias de destino

- AWS Lambda
- Amazon S3
- AWS Step Functions (se o AWS Lambda Power Tuning estiver implantado)

Arquitetura de destino

O diagrama a seguir mostra uma função Lambda que lê objetos de um bucket do S3 em paralelo. O diagrama também tem um fluxo de trabalho Step Functions para a ferramenta AWS Lambda Power

Tuning ajustar a memória da função Lambda. Esse ajuste fino ajuda a alcançar um bom equilíbrio entre custo e desempenho.

Automação e escala

As funções Lambda escalam rapidamente quando necessário. Para evitar erros 503 de desaceleração do Amazon S3 durante a alta demanda, recomendamos colocar alguns limites na escalabilidade.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK) v2 é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código. A infraestrutura de exemplo foi criada para ser implantada com AWS CDK.
- AWS Command Line InterfaceAWS CLIé uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando. Nesse padrão, a AWS CLI versão 2 é usada para fazer upload de um arquivo JSON de exemplo.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- Amazon Simple Storage Service O Amazon S3 é um serviço de armazenamento de objetos baseado em nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar funções AWS Lambda e outros serviços da AWS para criar aplicativos essenciais para os negócios.

Outras ferramentas

- Python é uma linguagem de programação de computador de uso geral. A reutilização de threads de trabalho ociosos foi introduzida na versão 3.8 do Python, e o código da função Lambda nesse padrão foi criado para a versão 3.9 e posterior do Python.

Repositório de código

O código desse padrão está disponível no aws-lambda-parallel-download GitHub repositório.

Práticas recomendadas

- Essa AWS CDK construção depende das suas permissões Conta da AWS de usuário para implantar a infraestrutura. Se você planeja usar AWS CDK Pipelines ou implantações entre contas, consulte Sintetizadores Stack.
- Esse aplicativo de exemplo não tem os registros de acesso habilitados no bucket do S3. É uma prática recomendada ativar os registros de acesso no código de produção.

Épicos

Prepare o ambiente de desenvolvimento

Tarefa	Descrição	Habilidades necessárias
Verifique a versão instalada do Python.	Esse código foi testado especificamente no Python 3.9 e no Python 3.13 e deve funcionar em todas as versões entre essas versões. Para verificar sua versão do Python, execute `python3 -V` em seu terminal e instale uma versão mais recente, se necessário. Para verificar se os módulos necessários estão instalados, execute`python3 -c "import pip, venv"`. Nenhuma mensagem de erro significa que os módulos estão instalados corretame	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	nte e você está pronto para executar este exemplo.	
Instalar AWS CDK.	Para instalar o, AWS CDK se ainda não estiver instalado , siga as instruções em Introdução ao AWS CDK. Para confirmar se a AWS CDK versão instalada é 2.0 ou posterior, execute`cdk --version`.	Arquiteto de nuvem
Inicialize seu ambiente da .	Para inicializar seu ambiente, se isso ainda não tiver sido feito, siga as instruções em Inicialize seu ambiente para uso com o. AWS CDK	Arquiteto de nuvem

Clone o repositório de exemplo

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar a versão mais recente do repositório, execute o seguinte comando: `git clone --depth 1 --branch v1.2.0 \ git@github.com:aws-samples/aws-lambda-parallel-download.git`	Arquiteto de nuvem
Altere o diretório de trabalho para o repositório clonado.	Execute o seguinte comando:	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`cd aws-lambda-paralle l-download`	
Crie o ambiente virtual Python.	Para criar um ambiente virtual Python, execute o seguinte comando: `python3 -m venv .venv`	Arquiteto de nuvem
Ative o ambiente virtual.	Para ativar o ambiente virtual, execute o seguinte comando: `source .venv/bin/ activate`	Arquiteto de nuvem
Instale as dependências.	Para instalar as dependênc ias do Python, execute o comando: `pip` `pip install -r requireme nts.txt`	Arquiteto de nuvem
Navegue pelo código.	(Opcional) O código de exemplo que baixa um objeto do bucket do S3 está em `resources/parallel .py` . O código da infraestr utura está na `parallel_ download` pasta.	Arquiteto de nuvem

Implemente e teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Implante o aplicativo.	Executar `cdk deploy`. Anote as AWS CDK saídas: • `ParallelDownloadStack.LambdaFunctionARN` • `ParallelDownloadStack.SampleS3BucketName` • `ParallelDownloadStack.StateMachineARN`	Arquiteto de nuvem
Faça upload de um arquivo JSON de exemplo.	O repositório contém um exemplo de arquivo JSON de cerca de 9 KB. Para fazer upload do arquivo no bucket do S3 da pilha criada, execute o seguinte comando: `aws s3 cp sample.json s3://<ParallelDownloadStack.SampleS3BucketName>` `<ParallelDownloadStack.SampleS3BucketName>` Substitua pelo valor correspondente da AWS CDK saída.	Arquiteto de nuvem
Execute o aplicativo.	Para executar o aplicativo, faça o seguinte:	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	1. Faça login no AWS Management Console, navegue até o console Lambda e localize a função Lambda que tem o ARN da saída. AWS CDK `ParallelDownloadStack.LambdaFunction` ARN 2. Na guia Teste, altere o JSON do evento para o seguinte: `{"objectKey": "sample.json"}` 3. Escolha Testar. 4. Para ver o resultado, escolha detalhes. Os detalhes mostrarão as estatísticas do download paralelo, as informações da execução e os registros.	
Adicione o número de downloads.	(Opcional) Para executar 1.500 chamadas get object, use o seguinte JSON no evento JSON do parâmetro: `Test` `{"repeat": 1500, "objectKey": "sample.json"}`	Arquiteto de nuvem

Opcional: Execute o AWS Lambda Power Tuning

Tarefa	Descrição	Habilidades necessárias
Execute a ferramenta AWS Lambda Power Tuning.	1. Faça login no console e navegue até Step Functions . 2. Localize a máquina de estado com o ARN da AWS CDK saída. `ParallelDownloadStack.StateMachineARN` 3. Escolha Iniciar execução e cole o seguinte JSON: `{ "lambdaARN": "<ParallelDownloadStack.LambdaFunctionARN>", "num": 10, "strategy": "balanced", "payload": {"repeat": 2000, "objectKey": "sample.json"} }` Lembre-se de `<ParallelDownloadStack.LambdaFunctionARN>` substituir pelo valor da AWS CDK saída. Ao final da execução, o resultado estará na guia de entrada e saída de execução.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Veja os resultados do AWS Lambda Power Tuning em um gráfico.	Na guia Entrada e saída de execução, copie o link da `visualization` proprieda de e cole-o em uma nova guia do navegador.	Arquiteto de nuvem

Limpeza

Tarefa	Descrição	Habilidades necessárias
Remova os objetos do bucket do S3.	Antes de destruir os recursos implantados, você remove todos os objetos do bucket do S3: `aws s3 rm s3://<ParallelDownloadStack.SampleS3BucketName> \ --recursive` Lembre-se de `<ParallelDownloadStack.SampleS3BucketName>` substituir pelo valor das AWS CDK saídas.	Arquiteto de nuvem
Destrua os recursos.	Para destruir todos os recursos que foram criados para esse piloto, execute o seguinte comando: `cdk destroy`	Arquiteto de nuvem

Solução de problemas

Problema	Solução
`'MemorySize' value failed to satisfy constraint: Member must have value less than or equal to 3008`	Para novas contas, talvez você não consiga configurar mais de 3.008 MB em suas funções do Lambda. Para testar usando o AWS Lambda Power Tuning, adicione a seguinte propriedade no JSON de entrada ao iniciar a execução do Step Functions: `"powerValues": [ 512, 1024, 1536, 2048, 2560, 3008 ]`

Recursos relacionados

- Python — concurrent.futures. ThreadPoolExecutor
- Cotas Lambda — configuração, implantação e execução de funções
- Trabalhando com o AWS CDK em Python
- Funções de criação de perfil com AWS Lambda Power Tuning

Mais informações

Código

O trecho de código a seguir executa o processamento paralelo de E/S:

```
with ThreadPoolExecutor(max_workers=MAX_WORKERS) as executor:
  for result in executor.map(a_function, (the_arguments)):
    ...
```

Eles `ThreadPoolExecutor` reutilizam os tópicos quando eles ficam disponíveis.

Testes e resultados

Esses testes foram realizados em dezembro de 2024.

O primeiro teste processou 2.500 leituras de objetos, com o seguinte resultado.

A partir de 3.009 MB, o nível de tempo de processamento permaneceu quase o mesmo em qualquer aumento de memória, mas o custo aumentou à medida que o tamanho da memória aumentou.

Outro teste investigou o intervalo entre 1.536 MB e 3.072 MB de memória, usando valores que eram múltiplos de 256 MB e processando 10.000 leituras de objetos, com os seguintes resultados.

A melhor performance-to-cost proporção foi com a configuração Lambda de 2.304 MB de memória.

Para comparação, um processo sequencial de 2.500 leituras de objetos levou 47 segundos. O processo paralelo usando a configuração Lambda de 2.304 MB levou 7 segundos, o que é 85% menos.

Envie dados de telemetria de AWS Lambda para OpenSearch para análise e visualização em tempo real

Criado por Tabby Ward (AWS), Guy Bachar (AWS) e David Kilzer (AWS)

Resumo

Os aplicativos modernos estão se tornando cada vez mais distribuídos e orientados por eventos, o que reforça a necessidade de monitoramento e observabilidade em tempo real. AWS Lambda é um serviço de computação sem servidor que desempenha um papel crucial na criação de arquiteturas escaláveis e orientadas por eventos. No entanto, monitorar e solucionar problemas de funções do Lambda pode ser um desafio se você confiar exclusivamente no Amazon CloudWatch Logs, que pode introduzir latência e períodos de retenção limitados.

Para enfrentar esse desafio, AWS introduziu a API de telemetria Lambda, que permite que as funções do Lambda enviem dados de telemetria diretamente para ferramentas de monitoramento e observabilidade de terceiros. Essa API suporta streaming em tempo real de registros, métricas e rastreamentos e fornece uma visão abrangente e oportuna do desempenho e da integridade de suas funções do Lambda.

Esse padrão explica como integrar a API de telemetria Lambda com OpenSearch, que é um mecanismo de pesquisa e análise distribuído de código aberto. OpenSearch oferece uma plataforma poderosa e escalável para ingerir, armazenar e analisar grandes volumes de dados, o que a torna a escolha ideal para dados de telemetria Lambda. Especificamente, esse padrão demonstra como enviar registros de uma função do Lambda escrita em Python diretamente para OpenSearch um cluster usando uma extensão do Lambda fornecida pela. AWS Essa solução é flexível e personalizável, para que você possa criar sua própria extensão Lambda ou alterar o código-fonte de amostra para alterar o formato de saída conforme desejado.

O padrão explica como instalar e configurar a integração da API de telemetria Lambda e inclui as melhores práticas de segurança OpenSearch, otimização de custos e escalabilidade. O objetivo é ajudar você a obter insights mais profundos sobre suas funções do Lambda e aprimorar a observabilidade geral de seus aplicativos sem servidor.

> **Note**
>
> Esse padrão se concentra na integração da API de telemetria Lambda com a API gerenciada. OpenSearch No entanto, os princípios e técnicas discutidos também são aplicáveis ao autogerenciamento OpenSearch e ao Elasticsearch.

Pré-requisitos e limitações

Antes de iniciar o processo de integração, verifique se você tem os seguintes pré-requisitos em vigor:

Conta da AWS: um ativo Conta da AWS com as permissões apropriadas para criar e gerenciar os seguintes AWS recursos:

- AWS Lambda
- AWS Identity and Access Management (IAM)
- Amazon OpenSearch Service (se você estiver usando um OpenSearch cluster gerenciado)

OpenSearch agrupamento:

- Você pode usar um OpenSearch cluster autogerenciado existente ou um serviço gerenciado, como o OpenSearch Service.
- Se você estiver usando o OpenSearch Serviço, configure seu OpenSearch cluster seguindo as instruções em Introdução ao Amazon OpenSearch Service na documentação do OpenSearch Serviço.
- Certifique-se de que o OpenSearch cluster esteja acessível a partir da sua função Lambda e esteja configurado com as configurações de segurança necessárias, como políticas de acesso, criptografia e autenticação.
- Configure o OpenSearch cluster com os mapeamentos e configurações de índice necessários para ingerir os dados de telemetria do Lambda. Para obter mais informações, consulte Carregamento de dados de streaming no Amazon OpenSearch Service na documentação do OpenSearch serviço.

Conectividade de rede:

- Certifique-se de que sua função Lambda tenha a conectividade de rede necessária para acessar o OpenSearch cluster. Para obter orientação sobre como definir as configurações da nuvem privada virtual (VPC), consulte Lançamento de seus domínios do Amazon OpenSearch Service em uma VPC na documentação do serviço. OpenSearch

Funções e políticas do IAM:

- Crie uma função do IAM com as permissões necessárias para que sua função Lambda acesse o OpenSearch cluster e acesse suas credenciais armazenadas nele. AWS Secrets Manager
- Anexe as políticas apropriadas do IAM à função, como a `AWSLambdaBasicExecutionRole` política e quaisquer permissões adicionais necessárias para interagir com ela OpenSearch.
- Verifique se as permissões do IAM concedidas à sua função Lambda permitem que ela grave dados no OpenSearch cluster. Para obter informações sobre o gerenciamento de permissões do IAM, consulte Definição de permissões de funções do Lambda com uma função de execução na documentação do Lambda.

Conhecimento da linguagem de programação:

- Você precisará de conhecimentos básicos de Python (ou da linguagem de programação de sua escolha) para entender e modificar o código de amostra da função Lambda e da extensão Lambda.

Ambiente de desenvolvimento:

- Configure um ambiente de desenvolvimento local com as ferramentas e dependências necessárias para criar e implantar funções e extensões do Lambda.

AWS CLI ou AWS Management Console:

- Instale e configure o AWS Command Line Interface (AWS CLI) ou use o AWS Management Console com as credenciais apropriadas para interagir com o necessário Serviços da AWS.

Monitoramento e registro:

- Familiarize-se com as melhores práticas de monitoramento e registro AWS, incluindo serviços como a Amazon CloudWatch e AWS CloudTrail para fins de monitoramento e auditoria.

- Verifique CloudWatch os registros da sua função Lambda para identificar quaisquer erros ou exceções relacionados à integração da API de telemetria do Lambda. Para obter orientação sobre solução de problemas, consulte a documentação da API de telemetria Lambda.

Arquitetura

Esse padrão usa o OpenSearch Service para armazenar registros e dados de telemetria que são gerados pelas funções do Lambda. Essa abordagem permite que você transmita rapidamente os registros diretamente para o seu OpenSearch cluster, o que reduz a latência e os custos associados ao uso do CloudWatch Logs como intermediário.

> **Note**
>
> Seu código de extensão do Lambda pode enviar a telemetria para o OpenSearch Serviço, usando diretamente a OpenSearch API ou usando uma biblioteca cliente. OpenSearch A extensão Lambda pode usar as operações em massa suportadas pela OpenSearch API para agrupar eventos de telemetria e enviá-los ao OpenSearch Serviço em uma única solicitação.

O diagrama de fluxo de trabalho a seguir ilustra o fluxo de trabalho de log para funções Lambda quando você usa OpenSearch um cluster como endpoint.

A arquitetura inclui os seguintes componentes:

- Função Lambda: a função sem servidor que gera registros e dados de telemetria durante a execução.
- Extensão Lambda: uma extensão baseada em Python que usa a API de telemetria Lambda para se integrar diretamente ao cluster. OpenSearch Essa extensão é executada junto com a função Lambda no mesmo ambiente de execução.
- API de telemetria do Lambda: a API que permite que as extensões do Lambda enviem dados de telemetria, incluindo registros, métricas e rastreamentos, diretamente para ferramentas de monitoramento e observabilidade de terceiros.

- Cluster Amazon OpenSearch Service: um OpenSearch cluster gerenciado hospedado em AWS. Esse cluster é responsável por ingerir, armazenar e indexar os dados de log transmitidos da função Lambda por meio da extensão Lambda.

O fluxo de trabalho consiste nas seguintes etapas:

1. A função Lambda é chamada e gera registros e dados de telemetria durante sua execução.
2. A extensão Lambda é executada junto com a função de capturar os registros e os dados de telemetria usando a API de telemetria Lambda.
3. A extensão Lambda estabelece uma conexão segura com o cluster de OpenSearch serviços e transmite os dados de log em tempo real.
4. O cluster OpenSearch de serviços ingere, indexa e armazena os dados de log para disponibilizá-los para pesquisa, análise e visualização por meio do uso de ferramentas como o Kibana ou outros aplicativos compatíveis.

Ao contornar os CloudWatch registros e enviar dados de registro diretamente para o OpenSearch cluster, essa solução oferece vários benefícios:

- Streaming e análise de registros em tempo real, permitindo uma solução de problemas mais rápida e uma melhor observabilidade.
- Latência reduzida e possíveis limitações de retenção associadas aos CloudWatch registros.
- Flexibilidade para personalizar a extensão Lambda ou criar sua própria extensão para formatos de saída específicos ou processamento adicional.
- Integração com os recursos de pesquisa, análise e visualização do OpenSearch Service para análise e monitoramento de registros.

A seção Epics fornece step-by-step instruções para configurar a extensão Lambda, configurar a função Lambda e integrar-se ao cluster de serviços. OpenSearch Para considerações de segurança, estratégias de otimização de custos e dicas para monitorar e solucionar problemas da solução, consulte a seção Práticas recomendadas.

Ferramentas

Serviços da AWS

- O AWS Lambda é um serviço de computação que permite executar código sem o provisionamento ou gerenciamento de servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- O Amazon OpenSearch Service é um serviço totalmente gerenciado fornecido pela empresa AWS que facilita a implantação, a operação e a escalabilidade de OpenSearch clusters na nuvem.
- As extensões do Lambda ampliam a funcionalidade de suas funções do Lambda executando código personalizado junto com elas. Você pode usar extensões do Lambda para integrar o Lambda com várias ferramentas de monitoramento, observabilidade, segurança e governança.
- AWS Lambda A API de telemetria permite que você use extensões para capturar dados aprimorados de monitoramento e observabilidade diretamente do Lambda e enviá-los para um destino de sua escolha.
- AWS CloudFormationajuda você a modelar e configurar seus AWS recursos para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos.

Repositórios de códigos

- AWS Lambda As extensões incluem demonstrações e exemplos de projetos da AWS and AWS Partners para ajudar você a começar a criar suas próprias extensões.
- O exemplo de integrações de telemetria do Lambda para fornece OpenSearch um exemplo de extensão do Lambda que demonstra como enviar registros de uma função do Lambda para um cluster. OpenSearch

Outras ferramentas

- OpenSearché um mecanismo de pesquisa e análise distribuído de código aberto que fornece uma plataforma poderosa para ingerir, armazenar e analisar grandes volumes de dados.
- O Kibana é uma ferramenta de exploração e visualização de dados de código aberto com a qual você pode usar. OpenSearch Observe que a implementação de visualização e análise está além do escopo desse padrão. Para obter mais informações, consulte a documentação do Kibana e outros recursos.

Práticas recomendadas

Ao integrar a API de telemetria Lambda com OpenSearch, considere as seguintes melhores práticas.

Segurança e controle de acesso

- Comunicação segura: criptografe todas as comunicações entre suas funções do Lambda e OpenSearch o cluster usando HTTPS. Defina as configurações SSL/TLS necessárias em sua extensão e configuração do Lambda. OpenSearch
- Permissões do IAM:
  - As extensões são executadas no mesmo ambiente de execução da função Lambda, então elas herdam o mesmo nível de acesso a recursos, como sistema de arquivos, rede e variáveis de ambiente.
  - Conceda as permissões mínimas necessárias do IAM às suas funções do Lambda para acessar a API de telemetria do Lambda e gravar dados no cluster. OpenSearch Use o princípio do privilégio mínimo para limitar o escopo das permissões.
- OpenSearch controle de acesso: implemente um controle de acesso refinado em seu OpenSearch cluster para restringir o acesso a dados confidenciais. Use os recursos de segurança integrados, como autenticação de usuário, controle de acesso baseado em funções e permissões em nível de índice, no. OpenSearch
- Extensões confiáveis: sempre instale extensões somente de uma fonte confiável. Use ferramentas de infraestrutura como código (IaC) AWS CloudFormation para simplificar o processo de anexar a mesma configuração de extensão, incluindo permissões do IAM, a várias funções do Lambda. As ferramentas do IaC também fornecem um registro de auditoria das extensões e versões usadas anteriormente.
- Tratamento de dados confidenciais: ao criar extensões, evite registrar dados confidenciais. Limpe as cargas e os metadados antes de registrá-los ou mantê-los para fins de auditoria.

Otimização de custo

- Monitoramento e alertas: configure mecanismos de monitoramento e alerta para rastrear o volume de dados enviados a OpenSearch partir de suas funções do Lambda. Isso ajudará você a identificar e lidar com possíveis excessos de custos.
- Retenção de dados: considere cuidadosamente o período de retenção de dados apropriado para seus dados de telemetria do Lambda em. OpenSearch Períodos de retenção mais longos podem aumentar os custos de armazenamento, portanto, equilibre suas necessidades de observabilidade com a otimização de custos.

- Compressão e indexação: habilite a compactação de dados e otimize sua estratégia de OpenSearch indexação para reduzir o espaço de armazenamento de seus dados de telemetria Lambda.
- Confiança reduzida em CloudWatch: Ao integrar diretamente a API de telemetria Lambda OpenSearch, você pode potencialmente reduzir sua dependência de CloudWatch registros, o que pode resultar em economia de custos. Isso ocorre porque a API de telemetria Lambda permite que você envie registros diretamente para OpenSearch, o que elimina a necessidade de armazenar e processar os dados. CloudWatch

Escalabilidade e confiabilidade

- Processamento assíncrono: use padrões de processamento assíncrono, como Amazon Simple Queue Service (Amazon SQS) ou Amazon Kinesis, para dissociar a execução da função Lambda da ingestão de dados. OpenSearch Isso ajuda a manter a capacidade de resposta das funções do Lambda e melhora a confiabilidade geral do sistema.
- OpenSearch escalabilidade de cluster: monitore o desempenho e a utilização de recursos do seu OpenSearch cluster e aumente-o ou diminua-o conforme necessário para lidar com o volume crescente de dados de telemetria Lambda.
- Failover e recuperação de desastres: implemente uma estratégia robusta de recuperação de desastres para seu OpenSearch cluster, incluindo backups regulares e a capacidade de restaurar dados rapidamente em caso de falha.

Observabilidade e monitoramento

- Painéis e visualizações: use o Kibana ou outras ferramentas de painel para criar painéis e visualizações personalizados que forneçam informações sobre o desempenho e a integridade de suas funções do Lambda com base nos dados de telemetria. OpenSearch
- Alertas e notificações: configure alertas e notificações para monitorar proativamente anomalias, erros ou problemas de desempenho em suas funções do Lambda. Integre esses alertas e notificações aos seus processos existentes de gerenciamento de incidentes.
- Rastreamento e correlação: garanta que seus dados de telemetria do Lambda incluam informações de rastreamento relevantes, como solicitação IDs ou correlação, para permitir a end-to-end observabilidade e a solução de problemas em seus IDs aplicativos distribuídos sem servidor.

Seguindo essas melhores práticas, você pode garantir que sua integração da API de telemetria Lambda OpenSearch seja segura, econômica e escalável, além de fornecer observabilidade abrangente para seus aplicativos sem servidor.

Épicos

Crie e implante a camada de extensão Lambda

Tarefa	Descrição	Habilidades necessárias
Baixe o código-fonte.	Baixe as extensões de amostra do repositório AWS Lambda de extensões.	Desenvolvedor de aplicativos, arquiteto de nuvem
Navegue para a pasta `python-example-telemetry-opensearch-extension` .	O repositório de AWS Lambda extensões que você baixou contém vários exemplos de vários casos de uso e tempos de execução de linguagem . Navegue até a pasta python-example-telemetry-opensearch-extension para usar a extensão OpenSearch Python, que envia registros para o. OpenSearch	Desenvolvedor de aplicativos, arquiteto de nuvem
Adicione permissões para executar o endpoint da extensão.	Execute o comando a seguir para tornar o endpoint da extensão executável: `chmod +x python-example-telemetry-opensearch-extension/extension.py`	Desenvolvedor de aplicativos, arquiteto de nuvem
Instale as dependências da extensão localmente.	Execute o comando a seguir para instalar dependências locais para o código Python:	Desenvolvedor de aplicativos, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`pip3 install -r python-example-telemetry-opensearch-extension/requirements.txt -t ./python-example-telemetry-opensearch-extension/` Essas dependências serão montadas junto com o código da extensão.	

Crie um pacote.zip para a extensão para implantá-la como uma camada.	O arquivo de extensão.zip deve conter um diretório raiz chamado`extensions/`, onde o executável da extensão está localizado, e outro diretório raiz chamado`python-example-telemetry-opensearch-extension/`, onde a lógica central da extensão e suas dependências estão localizadas.
	
	Crie o pacote.zip para a extensão:
	
	`chmod +x extensions/python-example-telemetry-opensearch-extension`
	`zip -r extension.zip extensions python-example-telemetry-opensearch-extension`
		Desenvolvedor de aplicativos, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Implante a extensão como uma camada Lambda.	Publique a camada usando seu arquivo de extensão.zip e o seguinte comando: `aws lambda publish-layer-version \ --layer-name "python-example-telemetry-opensearch-extension" \ --zip-file "fileb://extension.zip"`	Desenvolvedor de aplicativos, arquiteto de nuvem

Integre a extensão à sua função

Tarefa	Descrição	Habilidades necessárias
Adicione a camada à função.	1. Faça login AWS Management Console e abra a página Funções do AWS Lambda console. 2. Selecione sua função. 3. Em Layers (Camadas), selecione Add a layer (Adicionar uma camada). 4. Em Escolha uma camada, escolha Camadas personalizadas como fonte de camada e adicione sua camada. Para obter mais informações sobre como adicionar uma camada à sua função	Desenvolvedor de aplicativos, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	do Lambda, consulte a documentação do Lambda.	

Tarefa	Descrição	Habilidades necessárias
Defina as variáveis de ambiente para a função.	Na página da função, escolha a guia Configuração e adicione as seguintes variáveis de ambiente à sua função: • `URL`— O URI do seu OpenSearch endpoint para onde seus registros serão enviados. • `AUTH_SECRET` — O ARN de suas OpenSearch credenciais armazenadas em. AWS Secrets Manager Isso deve ser armazenado como um par de valores-c have e ter duas chaves: e. `username` `password` • `PLATFORM_INDEX` ,`FUNCTION_INDEX` , e `EXTENSION_INDEX` — Os nomes dos índices que armazenarão seus dados de telemetri a, registros de funções e registros de extensão. Certifique-se de que eles sigam os critérios de nomenclatura adequados. Caso contrário, seus índices não serão criados. • `DISPATCH_MIN_BATCH_SIZE` — O número de eventos de log que você	Desenvolvedor de aplicativos, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	deseja agrupar. No entanto, quando a função for encerrada, seus registros serão enviados independentemente dessa configuração.	

Adicione declarações de registro e teste sua função

Tarefa	Descrição	Habilidades necessárias

Adicione instruções de registro à sua função.	Adicione instruções de registro à sua função usando um dos mecanismos de registro integrados ou o módulo de registro de sua escolha.
	
	Aqui estão alguns exemplos de mensagens de registro em Python:
	
	`print("Your Log Message Here")`
	`logger = logging.getLogger(__name__)`
	
	`logger.info("Test Info Log.")`
	`logger.error("Test Error Log.")`
		Desenvolvedor de aplicativos, arquiteto de nuvem

Teste a função do .	1. Na página de função, selecione a guia Test (Testar). 2. Crie um evento de teste para sua função e execute	Desenvolvedor de aplicativos, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	o teste. Para obter mais informações, consulte Testando funções do Lambda no console na documentação do Lambda. Você deve ver Função de execução: bem-sucedida se tudo funcionar corretamente.	

Visualize seus logins OpenSearch

Tarefa	Descrição	Habilidades necessárias
Consulte seus índices.	Em OpenSearch, execute o comando a seguir para consultar seus índices: `SELECT * FROM index-name` Seus registros devem ser exibidos nos resultados da consulta.	Arquiteto de nuvem

Solução de problemas

Problema	Solução
Problemas de conectividade	• Confirme se sua função Lambda tem a conectividade de rede necessária para acessar o OpenSearch cluster. Consulte a documentação do OpenSearch serviço

Problema	Solução
	para obter orientação sobre como definir as configurações de VPC. • Verifique se as permissões do IAM concedidas à sua função Lambda permitem que ela grave dados no OpenSearch cluster. Consulte a documentação do Lambda para obter informações sobre o gerenciamento de permissões do IAM.
Erros de ingestão de dados	• Verifique CloudWatch os registros da sua função Lambda para identificar quaisquer erros ou exceções relacionados à integração da API de telemetria do Lambda. Consulte a documentação da API de telemetria Lambda para obter orientação sobre solução de problemas. • Verifique se o OpenSearch cluster está configurado corretamente e tem os mapeamentos e configurações de índice necessários para ingerir os dados de telemetria do Lambda. Consulte a OpenSearch documentação para obter mais informações.

Recursos relacionados

- Exemplo de integrações de telemetria Lambda para (repositório) OpenSearch GitHub
- Aumente as funções do Lambda usando extensões do Lambda (documentação do Lambda)
- API de telemetria Lambda (documentação do Lambda)
- Apresentando a API de AWS Lambda telemetria (AWS postagem no blog)
- Integrando a API de AWS Lambda telemetria com o Prometheus e (postagem no blog) OpenSearch AWS

Mais informações

Alterando a estrutura do registro

Por padrão, a extensão envia registros como um documento aninhado. OpenSearch Isso permite que você realize consultas aninhadas para recuperar valores de colunas individuais.

Se a saída de log padrão não atender às suas necessidades específicas, você poderá personalizá-la modificando o código-fonte da extensão Lambda fornecida pela. AWS AWS incentiva os clientes a adaptar a produção para atender às necessidades de seus negócios. Para alterar a saída do log, localize a `dispatch_to_opensearch` função no `telemetry_dispatcher.py` arquivo dentro do código-fonte da extensão e faça as alterações necessárias.

Configure um roteador celular sem servidor para uma arquitetura baseada em células

Criado por Mian Tariq (AWS) e Ioannis Lioupras (AWS)

Resumo

Como ponto de entrada para um sistema global de aplicativos baseados em células, o roteador celular é responsável por atribuir eficientemente os usuários às células apropriadas e fornecer os terminais aos usuários. O roteador celular executa funções como armazenar user-to-cell mapeamentos, monitorar a capacidade da célula e solicitar novas células quando necessário. É importante manter a funcionalidade do roteador celular durante possíveis interrupções.

A estrutura de design do roteador celular nesse padrão se concentra na resiliência, escalabilidade e otimização geral do desempenho. O padrão usa roteamento estático, em que os clientes armazenam os endpoints no login inicial e se comunicam diretamente com as células. Esse desacoplamento aumenta a resiliência do sistema, ajudando a garantir a funcionalidade ininterrupta do aplicativo baseado em células durante uma deficiência no roteador celular.

Esse padrão usa um AWS CloudFormation modelo para implantar a arquitetura. Para obter detalhes sobre o que o modelo implanta ou sobre como implantar a mesma configuração usando o AWS Management Console, consulte a seção Informações adicionais.

> **Important**
>
> A demonstração, o código e o AWS CloudFormation modelo apresentados nesse padrão são destinados apenas para fins explicativos. O material fornecido tem o único objetivo de ilustrar o padrão de design e auxiliar na compreensão. A demonstração e o código não estão prontos para produção e não devem ser usados para nenhuma atividade de produção ao vivo. Qualquer tentativa de usar o código ou a demonstração em um ambiente de produção é fortemente desencorajada e é por sua conta e risco. Recomendamos consultar os profissionais adequados e realizar testes completos antes de implementar esse padrão ou qualquer um de seus componentes em um ambiente de produção.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS)
- A versão mais recente do AWS Command Line Interface (AWS CLI)
- Credenciais da AWS com as permissões necessárias para criar a AWS CloudFormation pilha, AWS Lambda as funções e os recursos relacionados

Versões do produto

- Python 3.12

Arquitetura

O diagrama a seguir mostra um design de alto nível do roteador celular.

O diagrama percorre o seguinte fluxo de trabalho:

1. O usuário entra em contato com o Amazon API Gateway, que serve como frente para os endpoints da API do roteador celular.
2. O Amazon Cognito gerencia a autenticação e a autorização.
3. O AWS Step Functions fluxo de trabalho consiste nos seguintes componentes:
   - Orchestrator – Os `Orchestrator` usos AWS Step Functions para criar um fluxo de trabalho ou máquina de estado. O fluxo de trabalho é acionado pela API do roteador celular. Ele `Orchestrator` executa funções do Lambda com base no caminho do recurso.
   - Dispatcher – A função `Dispatcher` Lambda identifica e atribui uma célula estática por novo usuário registrado. A função pesquisa a célula com o menor número de usuários, a atribui ao usuário e retorna os endpoints.
   - Mapeador – A `Mapper` operação manipula os user-to-cell mapeamentos no banco de dados do `RoutingDB` Amazon DynamoDB que foi criado pelo modelo. AWS CloudFormation Quando acionada, a `Mapper` função fornece aos usuários já atribuídos seus endpoints.
   - Scaler – A `Scaler` função acompanha a ocupação da célula e a capacidade disponível. Quando necessário, a `Scaler` função pode enviar uma solicitação por meio do Amazon Simple Queue Service (Amazon SQS) para a camada Provision and Deploy para solicitar novas células.
   - Validador – A `Validator` função valida os terminais da célula e detecta possíveis problemas.

4. Ele `RoutingDB` armazena informações e atributos da célula (endpoints de API Região da AWS, estado, métricas).
5. Quando a capacidade disponível das células excede um limite, o roteador celular solicita serviços de provisionamento e implantação por meio do Amazon SQS para criar novas células.

Quando novas células são criadas, elas são `RoutingDB` atualizadas a partir da camada Provisionar e Implantar. No entanto, esse processo está além do escopo desse padrão. Para obter uma visão geral das premissas do projeto de arquitetura baseada em células e detalhes sobre o design do roteador celular usado nesse padrão, consulte a seção Informações adicionais.

Ferramentas

Serviços da AWS

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para suas aplicações Web e móveis.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar funções do Lambda e outras para criar aplicativos essenciais para os negócios. Serviços da AWS

Outras ferramentas

- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub Serverless-Cell-Router.

Práticas recomendadas

Para obter as melhores práticas ao criar arquiteturas baseadas em células, consulte a seguinte orientação do Well-Architected AWS :

- Reduzindo o escopo do impacto com a arquitetura baseada em células
- AWS Pilar de confiabilidade do Well-Architected Framework REL1: 0-BP04 Use arquiteturas de anteparo para limitar o escopo do impacto

Épicos

Preparar arquivos de origem

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de código de exemplo.	Para clonar o Serverless-Cell-Router GitHub repositório no seu computador, use o seguinte comando: `git clone https://github.com/aws-samples/Serverless-Cell-Router/`	Desenvolvedor
Configure credenciais AWS CLI temporárias.	Configure o AWS CLI com credenciais para o seu Conta da AWS. Este passo a passo usa credenciais temporárias fornecidas pela linha de comando do AWS IAM Identity Center ou pela opção	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	de acesso programático. Isso define as variáveis de `AWS_SESSION_TOKEN` AWS ambiente `AWS_ACCES S_KEY_ID AWS_SECRE T_ACCESS_KEY` ,, e com as credenciais apropriadas para uso com o. AWS CLI	
Criar um bucket do S3.	Crie um bucket do S3 que será usado para armazenar e acessar as funções do Serverless-Cell-Router Lambda para implantação pelo AWS CloudFormation modelo. Para criar o bucket do S3, use o seguinte comando: `aws s3api create-bucket --bucket <bucket name> --region eu-central-1 --create-bucket-co nfiguration LocationC onstraint=eu-centr al-1`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias

Crie arquivos.zip.	Crie um arquivo.zip para cada função Lambda localizada no diretório Functions. Esses arquivos.zip serão usados para implantar as funções do Lambda. Em um Mac, use os seguintes `zip` comandos:
	`zip -j mapper-scr.zip Functions/Mapper.py`
	`zip -j dispatcher-scr.zip Functions/Dispatcher.py`
	`zip -j scaler-scr.zip Functions/Scaler.py`
	`zip -j cp validator-scr.zip Functions/Validator.py`
	`zip -j dynamodbDummyData-scr.zip Functions/DynamodbDummyData.py`
		Desenvolvedor

Tarefa	Descrição	Habilidades necessárias

Copie os arquivos.zip para o bucket do S3.	Para copiar todos os arquivos. zip da função Lambda para o bucket do S3, use os seguintes comandos:
	`aws s3 cp mapper-scr.zip s3://<bucket name>`
	`aws s3 cp dispatcher-scr.zip s3://<bucket name>`
	`aws s3 cp scaler-scr.zip s3://<bucket name>`
	`aws s3 cp validator-scr.zip s3://<bucket name>`
	`aws s3 cp dynamodbDummyData-scr.zip s3://<bucket name>`
		Desenvolvedor

Crie a AWS CloudFormation pilha

Tarefa	Descrição	Habilidades necessárias

Implante o AWS CloudFormation modelo.	Para implantar o AWS CloudFormation modelo, execute o seguinte AWS CLI comando:
	`aws cloudformation create-stack --stack-name serverless.cell-router \`
	`--template-body file://Serverless-Cell-Router-Stack-v10.yaml \`
		Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`--capabilities CAPABILITY_IAM \ --parameters ParameterKey=LambdaFunctionMapperS3KeyParameterSCR,ParameterValue=mapper-scr.zip \ ParameterKey=LambdaFunctionDispatcherS3KeyParameterSCR,ParameterValue=dispatcher-scr.zip \ ParameterKey=LambdaFunctionScalerS3KeyParameterSCR,ParameterValue=scaler-scr.zip \ ParameterKey=LambdaFunctionAddDynamoDBDummyItemsS3KeyParameterSCR,ParameterValue=dynamodbDummyData-scr.zip \ ParameterKey=LambdaFunctionsS3BucketParameterSCR,ParameterValue=<S3 bucket storing lambda zip files> \ ParameterKey=CognitoDomain,ParameterValue=<Cognito Domain Name> \ --region <enter your aws region id, e.g. "eu-central-1">`	

Tarefa	Descrição	Habilidades necessárias
Verifique o andamento.	Faça login no AWS Management Console, abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation/e verifique o progresso do desenvolvimento da pilha. Quando o status for `CREATE_COMPLETE` , a pilha foi implantada com sucesso.	Desenvolvedor

Avalie e verifique

Tarefa	Descrição	Habilidades necessárias
Atribua células ao usuário.	Para iniciar o`Orchestrator` , execute o seguinte comando curl: `curl -X POST \ -H "Authorization: Bearer {User id_token}" \ https://xxxxxx.execute-api.eu-central-1.amazonaws.com/Cell_Router_Development/cells` Isso `Orchestrator` aciona a execução da `Dispatcher` função. O`Dispatcher` , por sua vez, verifica a existência do usuário. Se o usuário for encontrado, ele `Dispatche`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`r` retornará o ID da célula e o endpoint URLs associados. Se o usuário não for encontrado, ele `Dispatcher` aloca uma célula para o usuário e envia o ID da célula para a `Scaler` função para avaliação da capacidade residual da célula atribuída. A resposta da `Scaler` função é a seguinte: `"cellID : cell-0002 , endPoint_1 : https://xxxxx.execute-api.eu-north-1.amazonaws.com/ , endPoint_2 : https://xxxxxxx.execute-api.eu-central-1.amazonaws.com/"`	

Tarefa	Descrição	Habilidades necessárias

Recupere as células do usuário.	Para usar o `Orchestrator` para executar a `Mapper` função, execute o seguinte comando:
	
	`curl -X POST \ -H "Authorization: Bearer {User id_token}" \ https://xxxxxxxx x.execute-api.eu-central-1.amazonaws.com/Cell_Router_Development/mapper`
	
	O `Orchestrator` pesquisa a célula atribuída ao usuário e retorna o ID da célula e URLs a seguinte resposta:
	
	`"cellID : cell-0002 , endPoint_1 : https://xxxxx.execute-api.eu-north-1.amazonaws.com/ , endPoint_2 : https://xxxxxxx.execute-api.eu-central-1.amazonaws.com/"`
		Desenvolvedor

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpe os recursos.	Para evitar cobranças adicionais em sua conta, faça o seguinte: 1. Esvazie o bucket do S3 que você criou para as funções do Lambda. 2. Exclua o bucket . 3. Exclua a AWS CloudForm ation pilha.	Desenvolvedor de aplicativos

Recursos relacionados

Referências

- Estabilidade estática usando zonas de disponibilidade
- Limites de isolamento de falhas da AWS: estabilidade estática

Vídeo

Physalia: arquitetura baseada em células para fornecer maior disponibilidade no Amazon EBS

https://www.youtube-nocookie.com/embed/6 Eu sei? RZMFic controles = 0

Mais informações

Instalações de design de arquitetura baseada em células

Embora esse padrão se concentre no roteador celular, é importante entender todo o ambiente. O ambiente é estruturado em três camadas distintas:

- A camada de roteamento, ou camada fina, que contém o roteador celular
- A camada celular, compreendendo várias células
- A camada de provisionamento e implantação, que provisiona células e implanta o aplicativo

Cada camada mantém a funcionalidade mesmo no caso de deficiências que afetem outras camadas. Contas da AWS serve como um limite de isolamento de falhas.

O diagrama a seguir mostra as camadas em um nível alto. A camada Célula e a camada Provisionar e Implantar estão fora do escopo desse padrão.

Para obter mais informações sobre a arquitetura baseada em células, consulte Reduzindo o escopo do impacto com a arquitetura baseada em células: roteamento de células.

Padrão de design de roteador celular

O roteador celular é um componente compartilhado entre as células. Para mitigar possíveis impactos, é importante que a camada de roteamento use um design simplista e escalável horizontalmente que seja o mais fino possível. Servindo como ponto de entrada do sistema, a camada de roteamento consiste somente nos componentes necessários para atribuir eficientemente os usuários às células apropriadas. Os componentes dessa camada não se envolvem no gerenciamento ou na criação de células.

Esse padrão usa roteamento estático, o que significa que o cliente armazena em cache os endpoints no login inicial e, posteriormente, estabelece comunicação direta com a célula. Interações periódicas entre o cliente e o roteador celular são iniciadas para confirmar o status atual ou recuperar quaisquer atualizações. Esse desacoplamento intencional permite operações ininterruptas para os usuários existentes em caso de inatividade do roteador celular e fornece funcionalidade e resiliência contínuas dentro do sistema.

Nesse padrão, o roteador celular suporta as seguintes funcionalidades:

- Recuperando dados de células do banco de dados de células na camada Provisionar e Implantar e armazenar ou atualizar o banco de dados local.
- Atribuindo uma célula a cada novo usuário registrado do aplicativo usando o algoritmo de atribuição de células.
- Armazenando o user-to-cells mapeamento no banco de dados local.
- Verificar a capacidade das células durante a atribuição do usuário e elevar um evento para a máquina de venda automática na camada Provision and Deploy para criar células.
- Usando o algoritmo de critérios de criação de células para fornecer essa funcionalidade.
- Responder às solicitações do usuário recém-registrado fornecendo as URLs células estáticas. Eles URLs serão armazenados em cache no cliente com um tempo de vida (TTL).

- Responder às solicitações existentes do usuário de um URL inválido fornecendo um URL novo ou atualizado.

Para entender melhor o roteador celular de demonstração configurado pelo AWS CloudFormation modelo, revise os seguintes componentes e etapas:

1. Configure e configure o grupo de usuários do Amazon Cognito.
2. Configure e configure a API API Gateway para o roteador celular.
3. Crie uma tabela do DynamoDB.
4. Crie e configure uma fila SQS.
5. Implemente `Orchestrator` o.
6. Implemente as funções do Lambda:`Dispatcher`,,`Scaler`,`Mapper`. `Validator`
7. Avalie e verifique.

O pressuposto é que a camada Provisionar e Implantar já esteja estabelecida. Seus detalhes de implementação estão além do escopo desse artefato.

Como esses componentes são configurados e configurados por um AWS CloudFormation modelo, as etapas a seguir são apresentadas de forma descritiva e de alto nível. A suposição é que você tenha as AWS habilidades necessárias para concluir a instalação e a configuração.

1. Configurar e configurar o grupo de usuários do Amazon Cognito

Faça login no e abra AWS Management Console o console do Amazon Cognito em. https://console.aws.amazon.com/cognito/ Configure e configure um grupo de usuários do Amazon Cognito chamado`CellRouterPool`, com integração de aplicativos, interface de usuário hospedada e as permissões necessárias.

2. Configurar e configurar a API API Gateway para o roteador celular

Abra o console do API Gateway em https://console.aws.amazon.com/apigateway/. Configure e configure uma API chamada`CellRouter`, usando um autorizador do Amazon Cognito integrado ao grupo de usuários do Amazon Cognito. `CellRouterPool` Implemente os seguintes elementos:

- `CellRouter`Recursos de API, incluindo `POST` métodos
- Integração com o fluxo de trabalho Step Functions implementado na etapa 5
- Autorização por meio do autorizador do Amazon Cognito

- Mapeamentos de solicitações e respostas de integração
- Alocação das permissões necessárias

3. Criar uma tabela do DynamoDB

Abra o console do DynamoDB https://console.aws.amazon.com/dynamodb/em e crie uma tabela padrão do DynamoDB chamada com a seguinte configuração: `tbl_router`

- Chave de partição – `marketId`
- Chave de classificação – `cellId`
- Modo de capacidade – Provisionado
- Point-in-time recovery (PITR) – Desligado

Na guia Índices, crie um índice secundário global chamado`marketId-currentCapacity-index`. A função `Scaler` Lambda usará o índice para realizar pesquisas eficientes na célula com o menor número de usuários atribuídos.

Crie a estrutura da tabela com os seguintes atributos:

- `marketId`– Europa
- `cellId`– célula-0002
- `currentCapacity`– 2
- `endPoint_1`– <your endpoint for the first Region>
- `endPoint_2`– <your endpoint for the second Region>
- `IsHealthy`– Verdadeiro
- `maxCapacity`– 10
- `regionCode_1` – `eu-north-1`
- `regionCode_2` – `eu-central-1`
- `userIds`– <your email address>

4. Criar e configurar uma fila SQS

Abra o console do Amazon SQS em https://console.aws.amazon.com/sqs/e crie uma fila SQS padrão chamada configurada com criptografia de chave do **`CellProvisioning`** Amazon SQS.

5. Implemente o orquestrador

Desenvolva um fluxo de trabalho Step Functions `Orchestrator` para servir como o roteador. O fluxo de trabalho pode ser chamado por meio da API do roteador celular. O fluxo de trabalho executa as funções Lambda designadas com base no caminho do recurso. Integre a função step com a API API Gateway para o roteador `CellRouter` celular e configure as permissões necessárias para invocar as funções Lambda.

O diagrama mostra o fluxo de trabalho. O estado de escolha invoca uma das funções Lambda. Se a função Lambda for bem-sucedida, o fluxo de trabalho será encerrado. Se a função Lambda falhar, o estado de falha será chamado.

6. Implemente as funções Lambda

Implemente as `Dispatcher` `Validator` funções `MapperScaler`,, e. Ao configurar cada função na demonstração, defina uma função para a função e atribua as permissões necessárias para realizar as operações necessárias na tabela do DynamoDB`tbl_router`. Além disso, integre cada função ao fluxo de trabalho`Orchestrator`.

Função de expedidor

A `Dispatcher` função é responsável por identificar e atribuir uma única célula estática para cada novo usuário cadastrado. Quando um novo usuário se registra no aplicativo global, a solicitação vai para a `Dispatcher` função. A função processa a solicitação usando critérios de avaliação predefinidos, como os seguintes:

1. Região – Selecione a célula no mercado em que o usuário está localizado. Por exemplo, se o usuário estiver acessando o aplicativo global da Europa, selecione uma célula que use Regiões da AWS na Europa.
2. Proximidade ou latência – Selecione a célula mais próxima do usuário. Por exemplo, se o usuário estiver acessando o aplicativo da Holanda, a função considera uma célula que usa Frankfurt e Irlanda. A decisão sobre qual célula está mais próxima é baseada em métricas como latência entre a localização do usuário e as regiões da célula. Neste exemplo de padrão, as informações são alimentadas estaticamente a partir da camada Provisionar e Implantar.
3. Health – A `Dispatcher` função verifica se a célula selecionada está íntegra com base no estado da célula fornecido (Healthy = true ou false).
4. Capacidade – A distribuição do usuário é baseada no menor número de usuários em uma lógica de célula, portanto, o usuário é atribuído à célula que tem o menor número de usuários.

> **Note**
>
> Esses critérios são apresentados apenas para explicar esse padrão de exemplo. Para uma implementação real de roteador celular, você pode definir critérios mais refinados e baseados em casos de uso.

O `Orchestrator` invoca a função Dispatcher para atribuir usuários às células. Nessa função de demonstração, o valor de mercado é um parâmetro estático definido como`europe`.

A `Dispatcher` função avalia se uma célula já está atribuída ao usuário. Se a célula já estiver atribuída, a `Dispatcher` função retornará os pontos finais da célula. Se nenhuma célula for atribuída ao usuário, a função pesquisará a célula com o menor número de usuários, a atribuirá ao usuário e retornará os endpoints. A eficiência da consulta de pesquisa celular é otimizada usando o índice secundário global.

Função Mapper

A `Mapper` função supervisiona o armazenamento e a manutenção dos user-to-cell mapeamentos no banco de dados. Uma única célula é alocada para cada usuário registrado. Cada célula tem duas células distintas URLs — uma para cada região da AWS. Servindo como endpoints de API hospedados no API Gateway, eles URLs funcionam como pontos de entrada para o aplicativo global.

Quando a `Mapper` função recebe uma solicitação do aplicativo cliente, ela executa uma consulta na `tbl_router` tabela do DynamoDB para recuperar user-to-cell o mapeamento associado ao ID de e-mail fornecido. Se encontrar uma célula atribuída, a `Mapper` função fornecerá imediatamente as duas URLs células. A `Mapper` função também monitora ativamente as alterações na célula URLs e inicia notificações ou atualizações nas configurações do usuário.

Função Scaler

A `Scaler` função gerencia a capacidade residual da célula. Para cada nova solicitação de registro de usuário, a `Scaler` função avalia a capacidade disponível da célula que a `Dispatcher` função atribuiu ao usuário. Se a célula tiver atingido seu limite predeterminado de acordo com os critérios de avaliação especificados, a função iniciará uma solicitação por meio de uma fila do Amazon SQS para a camada Provision and Deploy, solicitando o provisionamento e a implantação de novas células. O dimensionamento das células pode ser executado com base em um conjunto de critérios de avaliação, como os seguintes:

1. Máximo de usuários – Cada célula pode ter um número máximo de 500 usuários.
2. Capacidade do buffer – A capacidade do buffer de cada célula é de 20%, o que significa que cada célula pode ser atribuída a 400 usuários a qualquer momento. Os 20% restantes da capacidade de buffer são reservados para futuros casos de uso e tratamento de cenários inesperados (por exemplo, quando os serviços de criação e provisionamento de células não estão disponíveis).
3. Criação de células – Assim que uma célula existente atinge 70% da capacidade, uma solicitação é acionada para criar uma célula adicional.

> **Note**
>
> Esses critérios são apresentados apenas para explicar esse padrão de exemplo. Para uma implementação real de roteador celular, você pode definir critérios mais refinados e baseados em casos de uso.

O `Scaler` código de demonstração é executado `Orchestrator` após a `Dispatcher` atribuição bem-sucedida de uma célula ao usuário recém-registrado. O`Scaler`, ao receber a ID da célula do`Dispatcher`, avalia se a célula designada tem capacidade adequada para acomodar usuários adicionais, com base em critérios de avaliação predefinidos. Se a capacidade da célula for insuficiente, a `Scaler` função enviará uma mensagem para o serviço Amazon SQS. Essa mensagem é recuperada pelo serviço na camada Provisionar e Implantar, iniciando o provisionamento de uma nova célula.

Função validadora

A `Validator` função identifica e resolve problemas relacionados ao acesso à célula. Quando um usuário faz login no aplicativo global, o aplicativo recupera as células das configurações do perfil URLs do usuário e encaminha as solicitações do usuário para uma das duas regiões atribuídas dentro da célula. Se URLs estiverem inacessíveis, o aplicativo poderá enviar uma solicitação de URL de validação para o roteador celular. O roteador celular `Orchestrator` invoca o. `Validator` Isso `Validator` inicia o processo de validação. A validação pode incluir, entre outras verificações, o seguinte:

- Célula de referência cruzada URLs na solicitação com URLs armazenada no banco de dados para identificar e processar possíveis atualizações
- Executando uma verificação profunda de saúde (por exemplo, uma `HTTP GET` solicitação para o endpoint da célula)

Concluindo, a `Validator` função fornece respostas às solicitações do aplicativo do cliente, fornecendo o status de validação junto com todas as etapas de remediação necessárias.

O foi `Validator` projetado para aprimorar a experiência do usuário. Considere um cenário em que determinados usuários tenham dificuldade em acessar o aplicativo global porque um incidente faz com que as células fiquem temporariamente indisponíveis. Em vez de apresentar erros genéricos, a `Validator` função pode fornecer etapas instrutivas de correção. Essas etapas podem incluir as seguintes ações:

- Informe os usuários sobre o incidente.
- Forneça um tempo de espera aproximado antes da disponibilidade do serviço.
- Forneça um número de contato de suporte para obter informações adicionais.

O código de demonstração da `Validator` função verifica se a célula fornecida pelo usuário URLs na solicitação corresponde aos registros armazenados na `tbl_router` tabela. A `Validator` função também verifica se as células estão saudáveis.

Configure o acesso privado a um bucket do Amazon S3 por meio de um endpoint VPC

Criado por Martin Maritsch (AWS), Gabriel Rodriguez Garcia (AWS), Shukhrat Khodjaev (AWS), Nicolas Jacob Baer (AWS), Mohan Gowda Purushothama (AWS) e Joaquin Rinaudo (AWS)

Resumo

No Amazon Simple Storage Service (Amazon S3), os URLs pré-assinados permitem que você compartilhe arquivos de tamanho arbitrário com os usuários-alvo. Por padrão, os Amazon S3 pré-assinados podem ser URLs acessados pela Internet dentro de um prazo de validade, o que os torna fáceis de usar. No entanto, ambientes corporativos geralmente exigem que o acesso ao Amazon S3 pré-assinado URLs seja limitado apenas a uma rede privada.

Esse padrão apresenta uma solução sem servidor para interagir com segurança com objetos do S3 usando URLs pré-assinados de uma rede privada sem passagem pela Internet. Na arquitetura, os usuários acessam um Application Load Balancer por meio de um nome de domínio interno. O tráfego é roteado internamente por meio do Amazon API Gateway e de um endpoint de nuvem privada virtual (VPC) para o bucket S3. A AWS Lambda função gera arquivos pré-assinados URLs para download por meio do endpoint VPC privado, o que ajuda a aumentar a segurança e a privacidade de dados confidenciais.

Pré-requisitos e limitações

Pré-requisitos

- Uma VPC que inclui uma sub-rede implantada em uma Conta da AWS que está conectada à rede corporativa (por exemplo, por meio de). AWS Direct Connect

Limitações

- O bucket do S3 deve ter o mesmo nome do domínio, por isso recomendamos que você verifique as regras de nomenclatura do bucket do Amazon S3.
- Esse exemplo de arquitetura não inclui recursos de monitoramento para a infraestrutura implantada. Se seu caso de uso exigir monitoramento, considere adicionar serviços AWS de monitoramento.
- Esse exemplo de arquitetura não inclui validação de entrada. Se seu caso de uso exigir validação de entrada e um maior nível de segurança, considere usar AWS WAF para proteger sua API.

- Esse exemplo de arquitetura não inclui o registro de acesso com o Application Load Balancer. Se seu caso de uso exigir registro de acesso, considere habilitar os registros de acesso do balanceador de carga.

Versões

- Python versão 3.11 ou posterior
- Terraform versão 1.6 ou posterior

Arquitetura

Pilha de tecnologias de destino

Os seguintes serviços da AWS são usados na pilha de tecnologia de destino:

- O Amazon S3 é o principal serviço de armazenamento usado para carregar, baixar e armazenar arquivos com segurança.
- O Amazon API Gateway expõe recursos e endpoints para interagir com o bucket do S3. Esse serviço desempenha um papel na geração de dados pré-assinados URLs para download ou upload.
- AWS Lambdagera arquivos pré-assinados URLs para baixar arquivos do Amazon S3. A função Lambda é chamada pelo API Gateway.
- A Amazon VPC implanta recursos dentro de uma VPC para fornecer isolamento de rede. A VPC inclui sub-redes e tabelas de roteamento para controlar o fluxo de tráfego.
- O Application Load Balancer roteia o tráfego de entrada para o API Gateway ou para o VPC endpoint do bucket do S3. Ele permite que os usuários da rede corporativa acessem recursos internamente.
- O VPC endpoint para Amazon S3 permite a comunicação direta e privada entre recursos na VPC e no Amazon S3 sem atravessar a Internet pública.
- AWS Identity and Access Management (IAM) controla o acesso aos AWS recursos. As permissões são configuradas para garantir interações seguras com a API e outros serviços.

Arquitetura de destino

O diagrama ilustra o seguinte:

1. Os usuários da rede corporativa podem acessar o Application Load Balancer por meio de um nome de domínio interno. Supomos que exista uma conexão entre a rede corporativa e a sub-rede da intranet no Conta da AWS (por exemplo, por meio de uma AWS Direct Connect conexão).
2. O Application Load Balancer encaminha o tráfego de entrada para o API Gateway para gerar dados pré-assinados URLs para download ou upload para o Amazon S3 ou para o VPC endpoint do bucket do S3. Em ambos os cenários, as solicitações são roteadas internamente e não precisam atravessar a Internet.
3. O API Gateway expõe recursos e endpoints para interagir com o bucket do S3. Neste exemplo, fornecemos um endpoint para baixar arquivos do bucket do S3, mas isso também pode ser estendido para fornecer a funcionalidade de upload.
4. A função Lambda gera a URL pré-assinada para baixar um arquivo do Amazon S3 usando o nome de domínio do Application Load Balancer em vez do domínio público do Amazon S3.
5. O usuário recebe a URL pré-assinada e a usa para baixar o arquivo do Amazon S3 usando o Application Load Balancer. O balanceador de carga inclui uma rota padrão para enviar tráfego que não é destinado à API para o endpoint VPC do bucket S3.
6. O VPC endpoint encaminha a URL pré-assinada com o nome de domínio personalizado para o bucket do S3. O bucket do S3 deve ter o mesmo nome do domínio.

Automação e escala

Esse padrão usa o Terraform para implantar a infraestrutura do repositório de código em um. Conta da AWS

Ferramentas

Ferramentas

- O Python é uma linguagem de programação de computador de uso geral.
- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir com AWS serviços por meio de comandos em seu shell de linha de comando.

Repositório de código

O código desse padrão está disponível em um GitHub repositório em https://github.com/aws-samples/private-s3-vpce.

Práticas recomendadas

A arquitetura de amostra desse padrão usa permissões do IAM para controlar o acesso à API. Qualquer pessoa que tenha credenciais válidas do IAM pode chamar a API. Se seu caso de uso exigir um modelo de autorização mais complexo, talvez você queira usar um mecanismo de controle de acesso diferente.

Épicos

Implemente a solução em um Conta da AWS

Tarefa	Descrição	Habilidades necessárias
Obtenha AWS credenciais.	Revise suas AWS credencia is e seu acesso à sua conta. Para obter instruções, consulte Configurações e configurações do arquivo de credenciais na AWS CLI documentação.	AWS DevOps, AWS geral
Clonar o repositório.	Clone o GitHub repositório fornecido com esse padrão: `git clone https://g ithub.com/aws-samp les/private-s3-vpce`	AWS DevOps, AWS geral
Configure variáveis.	1. No seu computador, no GitHub repositório, abra a `terraform` pasta: `cd terraform` 2. Abra o `example.tfvars` arquivo e personalize os	AWS DevOps, AWS geral

Tarefa	Descrição	Habilidades necessárias
	parâmetros de acordo com suas necessidades.	
Implemente a solução.	1. Na `terraform` pasta, execute o Terraform e passe as variáveis que você personalizou: `terraform apply -var-file="example.tfvars"` 2. Confirme se os recursos mostrados no diagrama de arquitetura foram implantados com êxito.	AWS DevOps, AWS geral

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Crie um arquivo de teste.	Faça upload de um arquivo para o Amazon S3 para criar um cenário de teste para o download do arquivo. Você pode usar o console do Amazon S3 ou o seguinte comando: AWS CLI `aws s3 cp /path/to/testfile s3://your-bucket-name/testfile`	AWS DevOps, AWS geral
Teste a funcionalidade de URL pré-assinada.	1. Envie uma solicitação ao Application Load Balancer para criar uma URL pré-	AWS DevOps, AWS geral

Tarefa	Descrição	Habilidades necessárias
	assinada para o arquivo de teste usando awscurl: `awscurl https://your-domain-name/api/get_url?key=testfile` Essa etapa cria uma assinatura válida a partir de suas credenciais, que será validada pelo API Gateway. 2. Analise o link da resposta que você recebeu na etapa anterior e abra o URL pré-assinado para baixar o arquivo.	
Limpeza.	Certifique-se de remover os recursos quando eles não forem mais necessários: `terraform destroy`	AWS DevOps, AWS geral

Solução de problemas

Problema	Solução
Os nomes de chave de objeto do S3 com caracteres especiais, como sinais numéricos (#), quebram os parâmetros do URL e causam erros.	Codifique os parâmetros de URL corretame nte e certifique-se de que o nome da chave do objeto S3 siga as diretrizes do Amazon S3.

Recursos relacionados

Amazon S3:

- Compartilhando objetos com presignados URLs
- Controle do acesso a partir de VPC endpoints com políticas de bucket

Amazon API Gateway:

- Use políticas de endpoint VPC para uso privado APIs no API Gateway

Application Load Balancer:

- Hospedagem de sites estáticos HTTPS internos com ALB, S3 e PrivateLink (AWS postagem do blog)

Solucione problemas de estados AWS Step Functions usando o Amazon Bedrock

Criado por Aniket Kurzadkar (AWS) e Sangam Kushwaha (AWS)

Resumo

AWS Step Functions os recursos de tratamento de erros podem ajudar você a ver um erro que ocorre durante um estado em um fluxo de trabalho, mas ainda pode ser um desafio encontrar a causa raiz de um erro e depurá-lo. Esse padrão aborda esse desafio e mostra como o Amazon Bedrock pode ajudá-lo a resolver erros que ocorrem durante estados em Step Functions.

O Step Functions fornece orquestração de fluxo de trabalho, facilitando a automatização dos processos pelos desenvolvedores. O Step Functions também fornece a funcionalidade de tratamento de erros que oferece os seguintes benefícios:

- Os desenvolvedores podem criar aplicativos mais resilientes que não falham completamente quando algo dá errado.
- Os fluxos de trabalho podem incluir lógica condicional para lidar com diferentes tipos de erros de forma diferente.
- O sistema pode repetir automaticamente as operações com falha, talvez com um recuo exponencial.
- Caminhos de execução alternativos podem ser definidos para cenários de erro, permitindo que o fluxo de trabalho se adapte e continue processando.

Quando ocorre um erro em um fluxo de trabalho do Step Functions, esse padrão mostra como a mensagem de erro e o contexto podem ser enviados para um modelo básico (FM) como o Claude 3, que é suportado pelo Step Functions. O FM pode analisar o erro, categorizá-lo e sugerir possíveis etapas de correção.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Compreensão básica AWS Step Functions e fluxos de trabalho
- Conectividade da API Amazon Bedrock

Limitações

- Você pode usar a abordagem desse padrão para vários Serviços da AWS. No entanto, os resultados podem variar de acordo com a solicitação criada por, AWS Lambda que é posteriormente avaliada pelo Amazon Bedrock.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte os serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

O diagrama mostra o fluxo de trabalho automatizado para tratamento e notificação de erros em uma máquina de estado Step Functions:

1. O desenvolvedor inicia a execução de uma máquina de estado.
2. A máquina de estado Step Functions começa a processar seus estados. Há dois resultados possíveis:
   - (a) Se todos os estados forem executados com sucesso, o fluxo de trabalho prosseguirá diretamente para o Amazon SNS para receber uma notificação de sucesso por e-mail.
   - (b) Se algum estado falhar, o fluxo de trabalho será movido para a função Lambda de tratamento de erros.
3. Em caso de erro, ocorre o seguinte:
   - (a) A função Lambda (manipulador de erros) é acionada. A função Lambda extrai a mensagem de erro dos dados do evento que a máquina de estado Step Functions passou para ela. Em seguida, a função Lambda prepara um prompt com base nessa mensagem de erro e envia o prompt para o Amazon Bedrock. O prompt solicita soluções e sugestões relacionadas ao erro específico encontrado.
   - (b) O Amazon Bedrock, que hospeda o modelo generativo de IA, processa o prompt de entrada. (Esse padrão usa o modelo básico Anthropic Claude 3 (FM), que é um dos muitos que o FMs Amazon Bedrock suporta.) O modelo de IA analisa o contexto do erro. Em seguida, o modelo gera uma resposta que pode incluir explicações sobre por que o erro ocorreu, possíveis soluções para resolver o erro e sugestões para evitar cometer os mesmos erros no futuro.

O Amazon Bedrock retorna sua resposta gerada por IA à função Lambda. A função Lambda processa a resposta, potencialmente formatando-a ou extraindo informações importantes. Em seguida, a função Lambda envia a resposta para a saída da máquina de estado.

4. Após o tratamento de erros ou a execução bem-sucedida, o fluxo de trabalho é concluído acionando o Amazon SNS para enviar uma notificação por e-mail.

Ferramentas

Serviços da AWS

- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.

Práticas recomendadas

- Como o Amazon Bedrock é um modelo generativo de IA que aprende com dados treinados, ele também usa esses dados para treinar e gerar contexto. Como prática recomendada, oculte qualquer informação privada que possa causar problemas de vazamento de dados.
- Embora a IA generativa possa fornecer informações valiosas, as decisões críticas de tratamento de erros ainda devem envolver supervisão humana, especialmente em ambientes de produção.

Épicos

Crie uma máquina de estado para seu fluxo de trabalho

Tarefa	Descrição	Habilidades necessárias
Criar uma máquina de estado do .	Para criar uma máquina de estado apropriada para seu fluxo de trabalho, faça o seguinte: 1. Faça login no AWS Management Console e abra o AWS Step Functions console. 2. No painel de navegação esquerdo, escolha State machines. 3. Escolha Criar uma máquina de estado. 4. Escolha um modelo de acordo com seu caso de uso ou escolha Em branco para criar um modelo de acordo com seus requisitos.	AWS DevOps

Criar uma função do Lambda

Tarefa	Descrição	Habilidades necessárias
Crie uma função do Lambda.	Para criar uma função Lambda, faça o seguinte: 1. No AWS Management Console, navegue até o AWS Lambda console.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	2. No painel de navegação à esquerda, selecione Funções e selecione Criar função. 3. Na página Criar função, escolha entre as opções para criar uma função. Em seguida, insira um nome em Nome da função e escolha o idioma apropriado na lista suspensa em Tempo de execução. 4. Escolha a opção Criar função.	

Tarefa	Descrição	Habilidades necessárias

Configure a lógica necessária no código Lambda.	• Para se conectar à API Amazon Bedrock usando o AWS SDK para Python (Boto3), use o código a seguir.
	
	Esse código configura um cliente para o Amazon Bedrock, prepara os parâmetros necessários e, em seguida, envia uma solicitação ao modelo Claude 3 com uma solicitação especificada.
	
	Esse padrão invoca o modelo Claude 3. Para obter mais informações sobre todos os modelos de fundação suportados, incluindo o modelo relacionado IDs, consulte Modelos de fundação suportados no Amazon Bedrock na documentação do Amazon Bedrock.
	
	`client = boto3.client( service_name="bedrock-runtime", region_name="selected-region" )`
	
	`# Invoke Claude 3 with the text prompt`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre> model_id = "your-mod
	el-id" # Select your
	 Model ID, Based on the
	 Model Id, Change the
	 body format
	
	    try:
	        response =
	 client.invoke_model(
	            modelId=m
	odel_id,
	            body=json
	.dumps(
	                {
	
	 "anthropic_version":
	 "bedrock-2023-05-31",
	
	 "max_tokens": 1024,
	
	 "messages": [
	
	 {
	
	    "role": "user",
	
	          "content"
	: [{"type": "text",
	 "text": prompt}],
	
	 }
	                    ],
	                }
	            ),
	        )</pre>
	• (Opcional) Substitua a por uma conta Conta da AWS IDs IDs de espaço reservado. Por motivos de	

Tarefa	Descrição	Habilidades necessárias

	segurança, essa abordagem pode ser útil para limpar registros, mensagens de erro ou outras saídas que possam conter informações confidenciais da conta.
	
	O código a seguir localizar á qualquer ocorrência de um número de 12 dígitos entre dois pontos (que é o formato dos Conta da AWS IDs Amazon Resource Names (ARNs) e de alguns outros AWS identificadores) e a substituirá pelo ID da conta do espaço reservado. `":123456789012:"`
	
	`def replace_account_id(input_string):`
	`  # Use a regular expression to find the AWS account ID pattern`
	`  account_id_pattern = r'(:\d{12}:)'`
	`  # Replace the matched pattern with ":123456789012:"`
	`  modified_string = re.sub(account_id_pattern, ":1234567`	

Tarefa	Descrição	Habilidades necessárias
	89012:", input_str ing) return modified_ string	

Integre Step Functions com o Lambda

Tarefa	Descrição	Habilidades necessárias
Configure o Lambda para lidar com erros em Step Functions.	Para configurar o Step Functions para lidar com erros sem interromper o fluxo de trabalho, faça o seguinte: 1. No console Step Functions , navegue até a máquina de estado que você criou anteriormente. 2. Escolha Editar e, em seguida, escolha o serviço para o qual você deseja configurar o tratamento de erros e escolha Tratamento de erros. 3. Escolha Adicionar novo coletor e, para o estado Fallback, escolha Lambda e, em seguida, escolha a função Lambda que você criou anteriormente. Para obter mais informações, consulte Catch errors na	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	documentação do Step Functions.	

Solução de problemas

Problema	Solução
O Lambda não pode acessar a API Amazon Bedrock (não autorizado a executar)	Esse erro ocorre quando a função Lambda não tem permissão para acessar a API Amazon Bedrock. Para resolver esse problema, adicione a `AmazonBedrockFullAccess` política para a função Lambda. Para obter mais informações, consulte AmazonBedrockFullAccesso Guia de referência de políticas AWS gerenciadas.
Erro de tempo limite do Lambda	Às vezes, pode levar mais de 30 segundos para gerar uma resposta e enviá-la de volta, dependendo da solicitação. Para resolver esse problema, aumente o tempo de configuração. Para obter mais informações, consulte Configurar o tempo limite da função Lambda no Guia do AWS Lambda desenvolvedor.

Recursos relacionados

- Amazon Bedrock
- Acesso à API Amazon Bedrock
- Crie sua primeira função Lambda
- Desenvolvendo fluxos de trabalho com Step Functions
- AWS Step Functions

Reúna os serviços da AWS usando uma abordagem de tecnologia sem servidor

Criado por Aniket Braganza (AWS)

Resumo

Esse padrão demonstra uma abordagem escalável e com tecnologia sem servidor para processar um arquivo enviado por meio do encadeamento do Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) e AWS Lambda. O exemplo do arquivo enviado é para fins de demonstração. Você pode usar uma abordagem com tecnologia sem servidor para concluir outras tarefas encadeando a combinação dos serviços da AWS necessários para atingir suas metas de negócios. A abordagem com tecnologia sem servidor emprega um fluxo de trabalho assíncrono que depende de notificações orientadas por eventos, armazenamento resiliente e computação de função como serviço (FaaS) para processar solicitações. Você pode usar a abordagem de tecnologia sem servidor para escalar para atender à demanda e, ao mesmo tempo, minimizar os custos.

> **Note**
>
> Há várias opções para encadear os serviços da AWS por meio de uma abordagem sem servidor. Por exemplo, você pode usar uma abordagem que combina o Lambda com o Amazon S3 em vez do Amazon SNS e do Amazon SQS. No entanto, esse padrão usa o Amazon SNS e o Amazon SQS porque essa abordagem possibilita adicionar vários pontos de integração ao processo de invocação do Lambda durante uma notificação de evento e estender a implementação para incluir vários receptores em uma orquestração com tecnologia sem servidor, minimizando a quantidade de sobrecarga de processamento.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Acesso programático à conta da AWS. Para obter mais informações, consulte:
  - Pré-requisitos na documentação do AWS Cloud Development Kit (AWS CDK)
  - Pré-requisitos na documentação da AWS Command Line Interface (AWS CLI)

- AWS CDK, instalado
- AWS CLI, instalada e configurada
- Python 3.9

Versões do produto

- AWS CDK 2.x
- Python 3.9

Arquitetura

O diagrama a seguir ilustra como os serviços encadeados da AWS podem permitir que um usuário faça upload de um arquivo em um bucket do S3 para processamento.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário faz upload de um arquivo para seu bucket do S3.
2. O upload inicia um evento do S3 que publica uma mensagem em um tópico do SNS. A mensagem contém os detalhes do evento do S3.
3. A mensagem publicada no tópico do SNS é inserida em uma fila do SQS, que está inscrita e recebe notificações desse tópico.
4. Uma função do Lambda pesquisa a fila do SQS (como fonte de eventos) e espera que as mensagens sejam processadas.
5. Quando a função do Lambda recebe mensagens da fila do SQS, ela as processa e confirma o recebimento dessas mensagens.
6. Se uma mensagem não for processada pelo Lambda, essa mensagem será retornada para a fila do SQS e, consequentemente, transferida para uma fila de mensagens não entregues do SQS.

Pilha de tecnologia

- Amazon S3
- Amazon SNS
- Amazon SQS
- AWS Lambda

Ferramentas

Serviços da AWS

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Outras ferramentas

- O AWS Cloud Development Kit (AWS CDK) é a principal ferramenta para interagir com seu aplicativo do AWS CDK. Ele executa seu aplicativo, interroga o modelo de aplicativo que você definiu e produz e implanta os modelos da AWS gerados pelo CDK da CloudFormation AWS.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- Python é uma linguagem de programação interpretada de alto nível e de uso geral.

Código

O código desse padrão está disponível no repositório GitHub Chaining S3 to SNS to SQS to Lambda.

Épicos

Desenvolva seu ambiente com tecnologia sem servidor

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Clone o repositório e navegue até a pasta `python/s3-sns-sqs-lambda-chain` .	Desenvolvedor de aplicativos
Configurar um ambiente virtual.	1. No AWS CDK, execute o comando `python3 -m venv .venv`. 2. Execute o comando `source .venv/bin/activate` no MacOS/Linux ou `.venv\Scripts\activate.bat` no Windows.	Desenvolvedor de aplicativos
Instale as dependências.	Execute o comando `pip install -r requirements.txt` .	Desenvolvedor de aplicativos

Teste a CloudFormation pilha

Tarefa	Descrição	Habilidades necessárias
Execute testes de unidade.	1. Execute o comando `pip install -r requirements-dev.txt` . 2. **Important** (Opcional) Execute o `cdk synth --no-staging > template.yml`	Desenvolvedor de aplicativos, engenheiro de testes

Tarefa	Descrição	Habilidades necessárias
	comando para gerar a CloudFormation pilha. Você pode inspecionar a pilha, mas evite gerar os recursos e artefatos preparados. 3. Execute o comando `pytest` para executar todos os testes de unidade. 4. (Opcional) Execute o comando `pytest tests/unit/<test_filename>` para executar testes para um arquivo específico.	

Implante a CloudFormation pilha

Tarefa	Descrição	Habilidades necessárias
Configure o ambiente de bootstrap.	Siga as instruções em Bootstrapping na documentação da AWS para inicializar o ambiente para implantação do AWS CDK em cada região da AWS em que a CloudFormation pilha será implantada. **Note** Essa etapa exige que você tenha	Desenvolvedor de aplicativos, DevOps engenheiro, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	credenciais com acesso programático.	
Implante a CloudFormation pilha.	Execute o comando `cdk deploy` para criar e implantar a pilha na conta da AWS.	Desenvolvedor de aplicativos, DevOps engenheiro, AWS DevOps

Limpe os recursos do ambiente

Tarefa	Descrição	Habilidades necessárias
Exclua a CloudFormation pilha e remova os recursos associados.	Para excluir a CloudFormation pilha que foi criada e remover todos os recursos associados, execute o comando `run cdk` destroy.	Desenvolvedor de aplicativos

Mais padrões

- Acesse, consulte e una tabelas do Amazon DynamoDB usando o Athena
- Dados agregados no Amazon DynamoDB para previsão de ML no Athena
- Automatize as CodeGuru avaliações da Amazon para aplicativos AWS CDK Python usando Actions GitHub
- Automatize a avaliação de recursos da AWS
- Automatize a implantação de aplicativos aninhados usando o AWS SAM
- Automatize a replicação de instâncias do Amazon RDS em Contas da AWS
- Arquivar automaticamente itens no Amazon S3 usando o DynamoDB TTL
- Detecte alterações automaticamente e inicie diferentes CodePipeline pipelines para um monorepo em CodeCommit
- Crie uma arquitetura pouco acoplada com microsserviços usando DevOps práticas e o AWS Cloud9
- Crie uma arquitetura sem servidor multilocatário no Amazon Service OpenSearch
- Crie um visualizador avançado de arquivos de mainframe na Nuvem AWS
- Calcule o value at risk (VaR – valor em risco) usando os serviços da AWS
- Copie os produtos do AWS Service Catalog em diferentes contas e regiões da AWS
- Criar pipelines dinâmicos de CI para projetos Java e Python automaticamente
- Decomponha monólitos em microsserviços usando o CQRS e o fornecimento de eventos
- Implante um aplicativo de página única baseado em React no Amazon S3 e CloudFront
- Implante uma API do Amazon API Gateway em um site interno usando endpoints privados e um Application Load Balancer
- Implantar e depure clusters do Amazon EKS
- Implante e gerencie um data lake de tecnologia sem servidor na Nuvem AWS usando a infraestrutura como código
- Implemente um caso de uso do RAG AWS usando o Terraform e o Amazon Bedrock
- Desenvolva um assistente baseado em bate-papo totalmente automatizado usando agentes e bases de conhecimento do Amazon Bedrock
- Desenvolva assistentes avançados baseados em bate-papo com IA generativa usando RAG e prompting ReAct
- Gere dinamicamente uma política do IAM com o IAM Access Analyzer usando Step Functions

- Garanta que o registro do Amazon EMR no Amazon S3 esteja habilitado no lançamento
- Expressa o custo de uma tabela do DynamoDB para capacidade sob demanda
- Gere recomendações personalizadas e reclassificadas usando o Amazon Personalize
- Gerar dados de teste usando um trabalho do AWS Glue e Python
- Implemente SHA1 o hashing para dados de PII ao migrar do SQL Server para o PostgreSQL
- Implementar o padrão de saga com tecnologia sem servidor usando o AWS Step Functions
- Melhore o desempenho operacional habilitando o Amazon DevOps Guru em várias regiões e contas da AWS e OUs com o AWS CDK
- Lance um CodeBuild projeto em várias contas da AWS usando Step Functions e uma função de proxy Lambda
- Migre cargas de trabalho do Apache Cassandra para o Amazon Keyspaces usando o AWS Glue
- Monitore o uso de uma Amazon Machine Image compartilhada em várias Contas da AWS
- Otimize implantações sem servidor de várias contas usando os fluxos de trabalho e Actions AWS CDK GitHub
- Orquestre um pipeline de ETL com validação, transformação e particionamento usando o AWS Step Functions
- Consulte tabelas do Amazon DynamoDB com SQL usando o Amazon Athena
- Executar workloads agendadas e orientadas por eventos em grande escala com o AWS Fargate
- Ofereça conteúdo estático em um bucket do Amazon S3 por meio de uma VPC usando a Amazon CloudFront
- Simplifique o desenvolvimento e a implantação de bots do Amazon Lex usando um fluxo de trabalho automatizado
- Estruture um projeto Python em arquitetura hexagonal usando o AWS Lambda
- Traduza a linguagem natural em consultas DSL para consultas OpenSearch e Elasticsearch
- Desative os controles padrão de segurança em todas as contas de membros do Security Hub em um ambiente com várias contas
- Descarregue dados de um cluster do Amazon Redshift entre contas para o Amazon S3
- Coordene a dependência de recursos e a execução de tarefas usando a AWS Fargate WaitCondition construção de gancho
- Use agentes do Amazon Bedrock para automatizar a criação de controles de entrada de acesso no Amazon EKS por meio de prompts baseados em texto

Redes

Tópicos

- Automatizar a configuração do emparelhamento entre regiões com o AWS Transit Gateway
- Centralize a conectividade de rede usando o AWS Transit Gateway
- Configure a criptografia HTTPS para o Oracle JD Edwards EnterpriseOne no Oracle WebLogic usando um Application Load Balancer
- Conecte-se ao ambiente de gerenciamento e dados do Application Migration Service em uma rede privada
- Crie objetos Infoblox usando recursos CloudFormation personalizados da AWS e Amazon SNS
- Personalize os CloudWatch alertas da Amazon para AWS Network Firewall
- Implante recursos em uma AWS Wavelength zona usando o Terraform
- Migre registros de DNS em massa para uma zona hospedada privada do Amazon Route 53
- Modifique os cabeçalhos HTTP ao migrar de F5 para um Application Load Balancer na AWS
- Acesse de forma privada um endpoint central de serviços da AWS a partir de vários VPCs
- Crie um relatório das descobertas do Network Access Analyzer para acesso de entrada à Internet em vários Contas da AWS
- Configure a resolução de DNS para redes híbridas em um ambiente com várias contas AWS
- Verifique se os balanceadores de carga ELB exigem terminação TLS
- Visualize registros e métricas do AWS Network Firewall usando o Splunk
- Mais padrões

Automatizar a configuração do emparelhamento entre regiões com o AWS Transit Gateway

Criado por Ram Kandaswamy (AWS)

Resumo

O AWS Transit Gateway conecta nuvens privadas virtuais (VPCs) e redes locais por meio de um hub central. O tráfego do Transit Gateway sempre permanece no backbone global da Amazon Web Services (AWS) e não atravessa a Internet pública, o que reduz os vetores de ameaças, como explorações comuns e ataques distribuídos de negação de serviço (S). DDo

Caso precise se comunicar entre duas ou mais regiões da AWS, você poderá usar o emparelhamento entre regiões do Gateway de trânsito para estabelecer conexões de emparelhamento entre gateways de trânsito em diferentes regiões. No entanto, configurar manualmente o emparelhamento entre regiões com o gateway de trânsito pode ser um processo demorado que tem várias etapas. Esse padrão fornece um processo automatizado para remover essas etapas manuais usando código para realizar o emparelhamento. Você pode usar essa abordagem se precisar configurar repetidamente várias regiões e contas da AWS durante a configuração de uma organização multirregional.

Esse padrão usa uma CloudFormation pilha da AWS que inclui o fluxo de trabalho do AWS Step Functions, funções do AWS Lambda, funções do AWS Identity and Access Management (IAM) e grupos de log no Amazon CloudWatch Logs. Em seguida, você pode iniciar a execução do Step Functions e criar a conexão de emparelhamento entre regiões para seus gateways de trânsito. Para configurar manualmente o emparelhamento entre regiões, consulte Emparelhar em VPCs diferentes regiões da AWS usando o AWS Transit Gateway.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket existente do Amazon Simple Storage Service (Amazon S3)
- Gateways de trânsito, criados e configurados na região solicitante e nas regiões aceitantes. A região solicitante é onde uma solicitação de emparelhamento é originada e as regiões aceitantes aceitam a solicitação de emparelhamento. Para obter mais informações, consulte Criar e aceitar uma conexão de emparelhamento da VPC na documentação da VPC da Amazon.

- VPCs, instalado e configurado nas regiões aceitante e solicitante. Para ver as etapas para criar uma VPC, consulte Crie sua VPC em Conceitos básicos da Amazon VPC na documentação da Amazon VPC.
- Eles VPCs devem usar a `addToTransitGateway` tag e o `true` valor.
- Grupos de segurança e listas de controle de acesso à rede (ACLs) para você VPCs, configurados de acordo com seus requisitos. Para obter mais informações sobre isso, consulte Grupos de segurança para sua VPC e rede ACLs na documentação da Amazon VPC.

Regiões e limitações da AWS

- Somente algumas regiões da AWS oferecem suporte para emparelhamento entre regiões. Para obter uma lista completa das regiões que oferecem suporte ao peering entre regiões, consulte o AWS Transit Gateway. FAQs
- No código de exemplo em anexo, presume-se que a região solicitante seja `us-east-2` e a região aceitante seja `us-west-2`. Se quiser configurar regiões diferentes, você deve editar esses valores em todos os arquivos Python. Para implementar uma configuração mais complexa que envolva mais de duas regiões, você pode alterar as Step Functions para passar as regiões como um parâmetro para a função do Lambda e executar a função para cada combinação.

Arquitetura

O diagrama mostra um fluxo de trabalho com as seguintes estapas:

1. O usuário cria uma CloudFormation pilha da AWS.
2. CloudFormation A AWS cria uma máquina de estado Step Functions que usa uma função Lambda. Para obter mais informações, consulte Como criar uma máquina de estado do Step Functions que usa o Lambda na documentação do AWS Step Functions.
3. Step Functions chama uma função do Lambda para emparelhamento.
4. A função do Lambda cria uma conexão de emparelhamento entre os gateways de trânsito.
5. Step Functions chama uma função do Lambda para modificações na tabela de rotas.
6. A função Lambda modifica as tabelas de rotas adicionando o bloco Classless Inter-Domain Routing (CIDR) do. VPCs

Fluxo de trabalho do Step Functions

O diagrama mostra o seguinte fluxo de Step Functions:

1. O fluxo de trabalho Step Functions chama a função do Lambda para o emparelhamento do gateway de trânsito.
2. Há uma chamada no cronômetro para aguardar um minuto.
3. O status de emparelhamento é recuperado e enviado para o bloco de condições. O bloco é responsável pelo loop.
4. Se a condição de sucesso não for atendida, o fluxo de trabalho será codificado para entrar no estágio do cronômetro.
5. Se a condição de sucesso for atendida, uma função do Lambda será chamada para modificar as tabelas de rotas. Após essa chamada, o fluxo de trabalho do Step Functions termina.

Ferramentas

- AWS CloudFormation — CloudFormation A AWS é um serviço que ajuda você a modelar e configurar seus recursos da AWS.
- Amazon CloudWatch Logs — O CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas, aplicativos e serviços da AWS que você usa.
- AWS Identity and Access Management (IAM): o IAM é um serviço web que ajuda você a controlar, com segurança, o acesso a serviços da AWS.
- AWS Lambda: o Lambda executa seu código em uma infraestrutura de computação de alta disponibilidade e executa toda a administração dos recursos computacionais.
- AWS Step Functions: o Step Functions facilita a coordenação de componentes de aplicativos distribuídos como uma série de etapas em um fluxo de trabalho visual.

Épicos

Automatizar o emparelhamento

Tarefa	Descrição	Habilidades necessárias
Faça upload dos arquivos em anexo no bucket do S3.	Faça login no Console de Gerenciamento da AWS, abra o console do Amazon S3 e, em seguida, faça o upload dos arquivos `modify-transit-gateway-routes.zip`, `peer-transit-gateway.zip` e `get-transit-gateway-peering-status.zip` (anexados) em seu bucket do S3.	AWS geral
Crie a CloudFormation pilha da AWS.	Execute o comando a seguir para criar uma CloudFormation pilha da AWS usando o `transit-gateway-peering.json` arquivo (anexado): `aws cloudformation create-stack --stack-name myteststack --template-body file://sampletemplate.json` O AWS CloudFormation stack cria o fluxo de trabalho Step Functions, as funções Lambda, as funções do IAM CloudWatch e os grupos de log.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Certifique-se de que o CloudFormation modelo da AWS se refira ao bucket do S3 que contém os arquivos que você carregou anteriormente. **Note** Você também pode criar uma pilha usando o CloudFormation console da AWS. Para obter mais informaçõ es sobre isso, consulte Criação de uma pilha no CloudFormation console da AWS na CloudFormation documentação da AWS.	

Tarefa	Descrição	Habilidades necessárias
Iniciar uma nova execução em Step Functions.	Abra o console do Step Functions e inicie uma nova execução. O Step Functions chama a função do Lambda e cria a conexão de emparelhamento para os gateways de trânsito. Não é necessário um arquivo JSON de entrada. Verifique se um anexo está disponível e se o tipo de conexão é de emparelhamento. Para obter mais informações, consulte Iniciar uma nova execução em Getting started with AWS Step Functions na documentação do AWS Steps Functions.	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
Verifique as rotas nas tabelas de rotas.	O emparelhamento entre regiões é estabelecido entre os gateways de trânsito. As tabelas de rotas são atualizadas com o intervalo de blocos IPv4 CIDR da VPC da região de mesmo nível. Abra o console do Amazon VPC e escolha a guia Associações na tabela de rotas que corresponde ao anexo do gateway de trânsito. Verifique o intervalo de blocos CIDR da VPC das regiões emparelhadas. Para etapas e instruções detalhadas, consulte Associar uma tabela de rotas do gateway de trânsito na documentação do Amazon VPC.	Administrador de rede

Recursos relacionados

- Executions in Step Functions
- Anexos de emparelhamento do gateway de trânsito
- Faça peering VPCs em diferentes regiões da AWS usando o AWS Transit Gateway
- Interconexão VPCs entre regiões da AWS usando o AWS Transit Gateway — Demonstração (vídeo)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Centralize a conectividade de rede usando o AWS Transit Gateway

Criado por Mydhili Palagummi (AWS) e Nikhil Marrapu (AWS)

Resumo

Esse padrão descreve a configuração mais simples na qual o AWS Transit Gateway pode ser usado para conectar uma rede local a nuvens privadas virtuais (VPCs) em várias contas da AWS em uma região da AWS. Usando essa configuração, você pode estabelecer uma rede híbrida que conecta várias redes VPC em uma região e uma rede on-premises. Para tanto, use um gateway de trânsito e uma conexão de rede privada virtual (VPN) com a rede on-premises.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta para hospedagem de serviços de rede, gerenciada como uma conta membro de uma organização em AWS Organizations
- VPCs em várias contas da AWS, sem sobreposição de blocos de roteamento entre domínios sem classe (CIDR)

Limitações

Esse padrão não suporta o isolamento do tráfego entre determinada rede VPCs ou a rede local. Todas as redes conectadas ao gateway de trânsito poderão se conectar umas às outras. Para isolar o tráfego, você precisa usar tabelas de rotas personalizadas no gateway de trânsito. Esse padrão conecta somente a VPCs rede local usando uma única tabela de rotas padrão do Transit Gateway, que é a configuração mais simples.

Arquitetura

Pilha de tecnologias de destino

- AWS Transit Gateway
- Site-to-SiteVPN AWS
- VPC
- AWS Resource Access Manager (AWS RAM)

Arquitetura de destino

Ferramentas

Serviços da AWS

- O AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar com segurança seus recursos entre suas contas da AWS, unidades organizacionais ou toda a sua organização a partir do AWS Organizations.
- O AWS Transit Gateway é um hub central que conecta nuvens privadas virtuais (VPCs) e redes locais.

Épicos

Crie um gateway de trânsito na conta de serviços de rede

Tarefa	Descrição	Habilidades necessárias
Criar um gateway de trânsito	Na conta da AWS em que você deseja hospedar serviços de rede, crie um gateway de trânsito na região da AWS de destino. Para obter instruções, consulte Criar um gateway de trânsito. Observe o seguinte: • Selecione Associação de tabela de rotas padrão. • Selecione Propagação da tabela de rotas padrão.	Administrador de rede

Conecte o gateway de trânsito à rede on-premises

Tarefa	Descrição	Habilidades necessárias
Configurar o dispositivo de gateway do cliente para uma conexão VPN.	O dispositivo de gateway do cliente está conectado no lado local da conexão Site-to-Site VPN entre o gateway de trânsito e sua rede local. Para obter mais informaçõ es, consulte Seu dispositi vo de gateway do cliente na documentação do AWS Site-to-Site VPN. Identifique ou inicie um dispositivo de cliente on-premises compatíve l e anote seu endereço IP público. A configuração da VPN será concluída posterior mente neste épico.	Administrador de rede
Na conta de serviços de rede, crie um anexo VPN ao gateway de trânsito.	Para configurar uma conexão, crie um anexo VPN para o gateway de trânsito. Para obter instruções, consulte Anexos VPN do Transit Gateway.	Administrador de rede
Configure a VPN no dispositi vo de gateway do cliente na rede on-premises.	Faça o download do arquivo de configuração da conexão Site-to-Site VPN associada ao gateway de trânsito e defina as configurações de VPN no dispositivo de gateway do cliente. Para obter as instruções, consulte Fazer	Administrador de rede

Tarefa	Descrição	Habilidades necessárias
	o download de arquivo de configuração.	

Compartilhe na conta de serviços de rede o gateway de trânsito com outras contas da AWS ou com sua organização

Tarefa	Descrição	Habilidades necessárias
Na conta de gerenciamento do AWS Organizations, ative o compartilhamento.	Para compartilhar o gateway de trânsito com sua organização ou com determinadas unidades organizacionais, ative o compartilhamento no AWS Organizations. Caso contrário, você precisaria compartilhar o gateway de trânsito para cada conta individualmente. Para obter instruções, consulte Habilitar o compartilhamento de recursos no AWS Organizations.	Administrador de sistemas AWS
Crie o compartilhamento de recursos do gateway de trânsito na conta de serviços de rede.	Para permitir que VPCs outras contas da AWS dentro da sua organização se conectem ao gateway de trânsito, na conta de serviços de rede, use o console de RAM da AWS para compartilhar o recurso do gateway de trânsito. Para obter instruções, consulte Criar um compartilhamento de recursos.	Administrador de sistemas AWS

Conecte-se VPCs ao gateway de trânsito

Tarefa	Descrição	Habilidades necessárias
Crie anexos de VPC em contas individuais.	Nas contas nas quais o gateway de trânsito foi compartilhado, crie anexos VPC do gateway de trânsito. Para obter instruções, consulte Criar um anexo do gateway de trânsito para uma VPC.	Administrador de rede
Aceite as solicitações de anexos VPC.	Na conta de serviços de rede, aceite as solicitações de anexo VPC do Transit Gateway. Para obter instruções, consulte Aceitar um anexo compartilhado.	Administrador de rede

Configurar o roteamento

Tarefa	Descrição	Habilidades necessárias
Configure rotas em uma conta individual VPCs.	Em cada conta VPC individual, adicione rotas para a rede on-premises e outras redes VPC usando o gateway de trânsito como destino. Para obter instruções, consulte Adicionar e remover rotas de uma tabela de rotas.	Administrador de rede
Configure rotas em uma tabela de rotas do gateway de trânsito.	As rotas de VPCs e a conexão VPN devem ser propagadas e devem aparecer na tabela de rotas padrão do Transit	Administrador de rede

Tarefa	Descrição	Habilidades necessárias
	Gateway. Se necessário, crie qualquer rota estática (um exemplo são rotas estáticas para a conexão VPN estática) na tabela de rotas padrão do Transit Gateway. Para obter instruções, consulte Criar uma rota estática.	
Adicionar grupos de segurança e listas de controle de acesso (ACLs)	Para as EC2 instâncias e outros recursos na VPC, certifique-se de que as regras do grupo de segurança e as regras da ACL da rede permitam o tráfego entre VPCs a rede local e a rede local. Para obter instruções, consulte Controlar o tráfego para recursos usando grupos de segurança e Adicionar e excluir regras de uma ACL.	Administrador de rede

Teste de conectividade

Tarefa	Descrição	Habilidades necessárias
Teste a conectividade entre VPCs.	Certifique-se que a ACL de rede e os grupos de segurança permitam o tráfego do ICMP (Protocolo de Mensagem de Controle da Internet) e, em seguida, faça ping de instâncias em uma VPC para outra VPC que	Administrador de rede

Tarefa	Descrição	Habilidades necessárias
	também esteja conectada ao gateway de trânsito.	
Teste a conectividade entre VPCs e a rede local.	Certifique-se de que as regras de ACL de rede, as regras de grupos de segurança e quaisquer firewalls permitam tráfego ICMP e, em seguida, faça ping entre a rede local e as instâncias no EC2 . VPCs A comunicação de rede deve ser iniciada primeiro a partir da rede on-premises para que a conexão VPN volte ao status UP.	Administrador de rede

Recursos relacionados

- Criar uma infraestrutura de rede AWS dimensionável e segura de várias VPCs (AWS whitepaper)
- Trabalhando com recursos compartilhados (documentação da AWS RAM)
- Trabalho com gateways de trânsito (documentação do AWS Transit Gateway)

Configure a criptografia HTTPS para o Oracle JD Edwards EnterpriseOne no Oracle WebLogic usando um Application Load Balancer

Criado por Thanigaivel Thirumalai (AWS)

Resumo

Esse padrão explica como configurar a criptografia HTTPS para descarregamento de SSL no Oracle JD Edwards EnterpriseOne em cargas de trabalho Oracle. WebLogic Essa abordagem criptografa o tráfego entre o navegador do usuário e um balanceador de carga para remover a carga de criptografia dos EnterpriseOne servidores.

Muitos usuários escalam horizontalmente a máquina virtual EnterpriseOne JAVA (JVM) usando um AWS Application Load Balancer.O balanceador de carga serve como o único ponto de contato para os clientes e distribui o tráfego de entrada entre vários. JVMs Opcionalmente, o balanceador de carga pode distribuir o tráfego em várias zonas de disponibilidade e aumentar a disponibilidade de. EnterpriseOne

O processo descrito nesse padrão configura a criptografia entre o navegador e o balanceador de carga em vez de criptografar o tráfego entre o balanceador de carga e o. EnterpriseOne JVMs Essa abordagem é conhecida como descarregamento de SSL. Transferir o processo de descriptografia SSL da EnterpriseOne web ou do servidor de aplicativos para o Application Load Balancer reduz a carga do lado do aplicativo. Após o terminal do SSL no balanceador de carga, o tráfego não criptografado é roteado para o aplicativo na AWS.

O Oracle JD Edwards EnterpriseOne é uma solução de planejamento de recursos corporativos (ERP) para organizações que fabricam, constroem, distribuem, atendem ou gerenciam produtos ou ativos físicos. O JD Edwards EnterpriseOne oferece suporte a vários hardwares, sistemas operacionais e plataformas de banco de dados.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma função do AWS Identity and Access Management (IAM) que tem permissões para fazer chamadas de serviço da AWS e gerenciar recursos da AWS
- Um certificado SSL

Versões do produto

- Esse padrão foi testado com o Oracle WebLogic 12c, mas você também pode usar outras versões.

Arquitetura

Existem várias abordagens para realizar o descarregamento de SSL. Esse padrão usa um Application Load Balancer e o Oracle HTTP Server (OHS), conforme ilustrado no diagrama a seguir.

O diagrama a seguir mostra o layout de JD Edwards EnterpriseOne, Application Load Balancer e Java Application Server (JAS) JVM.

Ferramentas

Serviços da AWS

- Os Application Load Balancers distribuem o tráfego de entrada do aplicativo em vários destinos, como o Amazon Elastic Compute Cloud (EC2 instâncias da Amazon), em várias zonas de disponibilidade.
- O AWS Certificate Manager (ACM) ajuda você a criar, armazenar e renovar chaves e certificados SSL/TLS X.509 públicos e privados que protegem seus sites e aplicativos da AWS.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.

Práticas recomendadas

- Para conhecer as melhores práticas do ACM, consulte a documentação do ACM.

Épicos

Configuração WebLogic e OHS

Tarefa	Descrição	Habilidades necessárias
Instale e configure os componentes do Oracle.	1. Instale o Fusion Middlewar e Infrastructure seguindo o processo de instalaçã	JDE CNC, administrador WebLogic

Tarefa	Descrição	Habilidades necessárias
	o padrão. Esse programa ajuda você a instalar e configurar um WebLogic domínio. Para obter instruções, consulte a documentação do Oracle. 2. Instale o OHS seguindo o processo de instalaçã o padrão. Para obter instruções, consulte a documentação do Oracle. 3. Quando a instalação estiver concluída, inicie o assistente de configuração (arquivo `config.sh`) para configurar o OHS. • É possível atualizar um domínio existente ou criar um novo. Esse padrão pressupõe que você esteja atualizando um domínio existente. • Para Modelos Disponíve is, escolha Oracle Enterprise Manager-R estricted JRF e Oracle HTTP Server (Restricted JRF). Selecionar essas opções de Java Required Files (JRF) elimina a conexão com um banco de dados externo. • Para servidores gerenciados, clusters,	

Tarefa	Descrição	Habilidades necessárias
	modelos de servidor, clusters de coerência , máquinas, atribuir servidores a máquinas, destinos virtuais e partições, aceite os valores de configura ção padrão e escolha Avançar para passar para a próxima categoria. • Preencha os detalhes da configuração (por exemplo, host e porta do administrador, endereço e porta de escuta, nome do servidor) da instância de OHS (por exemplo, `ohs1`).	

Tarefa	Descrição	Habilidades necessárias
Ative o WebLogic plug-in no nível do domínio.	O WebLogic plug-in é necessário para o balanceamento de carga. Para habilitar o plug-in: 1. Faça login no console de WebLogic administração usando o link: `http://<WeblogicServer>:<Adminport>/console` 2. Escolha Bloquear e editar e, em seguida, escolha Configuração, Aplicativos Web. 3. Escolha o WebLogic plug-in ativado (caixa de seleção ou opção suspensa). 4. Escolha Salvar e ativar alterações.	JDE CNC, administrador WebLogic

Tarefa	Descrição	Habilidades necessárias

Edite o arquivo de configuração.	O `mod_wl_ohs.conf` arquivo configura solicitações de proxy do OHS para. WebLogic
	
	1. Edite esse arquivo. Ele está localizado em:
	
	`$ORACLE_HOME/user_projects/domains/`
	
	Por exemplo:
	
	`/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1`
	2. Adicione os valores WebLogic host (`WebLogicHost`) e port (`WebLogicPort`) (esse padrão pressupõe localhost e porta 8000.)
	3. Adicione `WLProxySSL` valores `WLProxySSLPassThrough` e valores da seguinte forma:
	
	`<VirtualHost *:8000>`
	`<Location /jde>`
	`WLSRequest On`
		JDE CNC, administrador WebLogic

Tarefa	Descrição	Habilidades necessárias
	SetHandler weblogic-handler WebLogicHost localhost WebLogicPort 8000 WLProxySSL On WLProxySSLPassThrough On </Location> </VirtualHost>	

Tarefa	Descrição	Habilidades necessárias
Inicie o OHS usando o Enterprise Manager.	1. Faça login no Enterprise Manager Fusion Middlewar e usando o link: `http://<WeblogicSe rver>:<Adminport>/ em/` 2. Em Target Navigation, no Servidor HTTP, selecione a instância OHS (por exemplo, `ohs1`). 3. Escolha Desligar and Iniciar para reiniciar a instância OHS. 4. Quando a configuração do OHS estiver concluída , você poderá se conectar ao cliente EnterpriseOne HTML usando o nome do host do servidor HTTP com a porta 8000 em vez do nome do host do Enterpris eOne servidor. • Link antigo: `http://<W ebserver>:80/jde/ owhtml` • Novo link: `http:// <HTTP server or web server>:8000/jde/o whtml` Se você usar uma porta diferente da porta HTTP padrão do Oracle, edite o	JDE CNC, administrador WebLogic

Tarefa	Descrição	Habilidades necessárias

	arquivo `httpd.conf` para adicionar um receptor para essa porta em dois lugares:
	`#[Listen] OHS_LISTEN_PORT`
	`Listen 8000`
	e:
	`#`
	`ServerName <Weblogic Server1>:8000`	

Configure o Application Load Balancer

Tarefa	Descrição	Habilidades necessárias
configure um grupo de destino.	1. Crie um grupo-destino para a porta 8000 do servidor HTTP. 2. Registre os destinos no grupo destino com a mesma porta. 3. Verifique o status dos alvos para confirmar se eles estão íntegros. 4. configure a verificação de integridade conforme necessário. Para obter instruções detalhadas, consulte a	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	documentação do Elastic Load Balancing.	
Configure o balanceador de carga.	1. Crie um Application Load Balancer com atributos padrão e a nuvem privada virtual (VPC), grupos de segurança e sub-redes necessários. Para obter instruções detalhadas, consulte a documentação do Elastic Load Balancing. 2. Adicione uma entrada de receptor para HTTPS 443 e a encaminhe para o grupo de destino que você criou na etapa anterior. (Para obter instruções detalhadas, consulte a documentação do Elastic Load Balancing). Um receptor HTTPS exige um certificado SSL. Você poderá escolher um certificado do ACM ou fazer upload de um. 3. Para ambos os receptores, ative a aderência seguindo as instruções na documentação do Elastic Load Balancing.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Adicionar um registro no Route 53 (DNS).	(Opcional) Você poderá adicionar um registro DNS do Amazon Route 53 para o subdomínio. Esse registro apontaria para seu Application Load Balancer. Para obter instruções, consulte a Documentação do Route 53.	Administrador da AWS

Solução de problemas

Problema	Solução
O servidor HTTP não aparece.	Se o Servidor HTTP não aparecer na lista de Navegação de Destino no console do Enterprise Manager, siga estas etapas: 1. Em WebLogic Domínio, Administração, escolha Instâncias de OHS. 2. Escolha Criar para criar uma nova instância de OHS. 3. Forneça um nome de instância e escolha OK para criar a instância. Quando a instância for criada e as alterações forem ativadas, você poderá ver o servidor HTTP no painel Target Navigation.

Recursos relacionados

Documentação da AWS

- Application Load Balancers

- Trabalhar com zonas hospedadas públicas
- Trabalhar com zonas hospedadas privadas

Documentação da Oracle:

- Visão geral do plug-in Oracle WebLogic Server Proxy
- Instalando WebLogic o servidor usando o instalador de infraestrutura
- Instalar e configurar o Oracle HTTP Server

Conecte-se ao ambiente de gerenciamento e dados do Application Migration Service em uma rede privada

Criado por Dipin Jain (AWS) e Mike Kuznetsov (AWS)

Resumo

Esse padrão explica como você pode se conectar a um plano de AWS Application Migration Service dados e a um plano de controle em uma rede privada e segura usando endpoints VPC de interface.

O Application Migration Service é uma solução altamente automatizada lift-and-shift (rehospedagem) que simplifica, agiliza e reduz o custo da migração de aplicativos para o. AWS Ele permite que as empresas possam redefinir a hospedagem de um grande número de servidores físicos, virtuais ou em nuvem sem problemas de compatibilidade, interrupção no desempenho ou longos períodos de substituição. O Serviço de Migração de Aplicativos está disponível no AWS Management Console. Isso permite uma integração perfeita com outros Serviços da AWS AWS CloudTrail, como Amazon CloudWatch e AWS Identity and Access Management (IAM).

Você pode se conectar de um data center de origem a um plano de dados, ou seja, a uma sub-rede que serve como área de preparação para replicação de dados na VPC de destino, por meio de uma conexão privada usando serviços ou emparelhamento de VPC no Application Migration AWS VPN Service. AWS Direct Connect Você também pode usar endpoints VPC de interface alimentados por AWS PrivateLink para se conectar a um plano de controle do Application Migration Service por meio de uma rede privada.

Pré-requisitos e limitações

Pré-requisitos

- Sub-rede da área de teste — Antes de configurar o Application Migration Service, crie uma sub-rede para ser usada como área de preparação para dados replicados dos seus servidores de origem para AWS (ou seja, um plano de dados). Você deve especificar essa sub-rede no modelo de Configurações de Replicação ao acessar pela primeira vez o console do Application Migration Service. Você pode substituir essa sub-rede para servidores de origem específicos no modelo de Configurações de Replicação. Embora você possa usar uma sub-rede existente na sua Conta da AWS, recomendamos que você crie uma nova sub-rede dedicada para essa finalidade.
- Requisitos de rede — Os servidores de replicação que são iniciados pelo Serviço de Migração de Aplicativos na sub-rede da sua área de armazenamento precisam ser capazes de enviar dados para o endpoint da API do Serviço de Migração de Aplicativos em`https://`

`mgn.<region>.amazonaws.com/`, onde `<region>` está o código para o qual Região da AWS você está replicando (por exemplo,). `https://mgn.us-east-1.amazonaws.com` O serviço Amazon Simple Storage Service (Amazon S3) é necessário para baixar o software Application Migration URLs Service.

- O instalador do AWS Replication Agent deve ter acesso à URL do bucket do Amazon Simple Storage Service (Amazon S3) do bucket que Região da AWS você está usando com o Application Migration Service.
- A sub-rede da área de armazenamento deve ter acesso ao Amazon S3.
- Os servidores de origem nos quais o Agente de AWS Replicação está instalado devem ser capazes de enviar dados para os servidores de replicação na sub-rede da área de armazenamento e para o endpoint da API do Application Migration Service em. `https://mgn.<region>.amazonaws.com/`

A tabela a seguir lista as portas necessárias.

Origem	Destination (Destino)	Porta	Para obter mais informações, consulte
Seu datacenter de origem	Serviço Amazon S3 URLs	443 (TCP)	Comunicação pela porta TCP 443
Seu datacenter de origem	Região da AWS-endereço de console específico para o Application Migration Service	443 (TCP)	Comunicação entre os servidores de origem e o Serviço de Migração de Aplicativos pela porta TCP 443
Seu datacenter de origem	Sub-rede de área de teste	1500 (TCP)	Comunicação entre os servidores de origem e a sub-rede da área de armazenamento pela porta TCP 1500
Sub-rede de área de teste	Região da AWS-endereço de console	443 (TCP)	Comunicação entre a sub-rede da área de

	específico para o Application Migration Service		armazenamento e o Serviço de Migração de Aplicativos pela porta TCP 443
Sub-rede de área de teste	Serviço Amazon S3 URLs	443 (TCP)	Comunicação pela porta TCP 443
Sub-rede de área de teste	Endpoint Amazon Elastic Compute Cloud (Amazon EC2) da sub-rede Região da AWS	443 (TCP)	Comunicação pela porta TCP 443

Limitações

Atualmente, o Application Migration Service não está disponível em todos Regiões da AWS os sistemas operacionais.

- Suportado Regiões da AWS
- Sistemas operacionais com suporte

Arquitetura

O diagrama a seguir ilustra a arquitetura de rede para uma migração típica. Para obter mais informações sobre essa arquitetura, consulte a documentação do Application Migration Service e o vídeo sobre arquitetura do serviço e arquitetura de rede do Application Migration Service.

A visualização detalhada a seguir mostra a configuração dos endpoints da VPC de interface na área de armazenamento VPC para conectar o Amazon S3 e o Application Migration Service.

Ferramentas

- AWS Application Migration Servicesimplifica, agiliza e reduz o custo de rehospedar aplicativos. AWS

- Os endpoints VPC de interface permitem que você se conecte a serviços que são fornecidos AWS PrivateLink sem a necessidade de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias na sua VPC não exigem que endereços IP públicos se comuniquem com recursos no serviço. O tráfego entre a sua VPC e os outros serviços não deixa a rede da Amazon.

Épicos

Crie endpoints para o Application Migration Service EC2, Amazon e Amazon S3

Tarefa	Descrição	Habilidades necessárias
Configure o endpoint da interface para o Application Migration Service.	O datacenter de origem e a área de armazenamento (VPC) se conectam de forma privada ao ambiente de gerenciamento do Applicati on Migration Service por meio do endpoint de interface que você cria na VPC da área de armazenamento de destino. Para criar o endpoint: 1. Abra o console da Amazon Virtual Private Cloud (Amazon VPC). 2. No painel de navegação, escolha Endpoints, Create Endpoint (Criar endpoint). 3. Em Service category (Categoria de serviço), escolha Serviços da AWS. 4. Em Nome do serviço, digite `com.amazonaws.<reg ion>.mgn` . Em Tipo, escolha Interface.	Líder de migração

Tarefa	Descrição	Habilidades necessárias
	5. Para VPC, selecione a área de armazenamento de destino VPC para criar o endpoint. 6. Em Sub-redes, selecione as sub-redes nas quais criar as interfaces de rede do endpoint. 7. Para ativar o DNS privado para o endpoint da interface , na seção Configurações adicionais, selecione Ativar nome DNS. 8. Selecione um grupo de segurança que permita a entrada da sub-rede VPC da área de armazenamento via TCP 443. 9. Escolha Criar endpoint. Para obter mais informaçõ es, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint na documentação da Amazon VPC.	

Tarefa	Descrição	Habilidades necessárias
Configure o endpoint da interface para a Amazon EC2.	A área de teste (VPC) se conecta de forma privada à API da EC2 Amazon por meio do endpoint de interface que você cria na VPC da área de armazenamento de destino. Para criar o endpoint, siga as instruções fornecidas na história anterior. • Em Nome do serviço, digite `com.amazonaws.<region>.ec2` . Em Tipo, escolha Interface. • O grupo de segurança deve permitir o tráfego HTTPS de entrada da sub-rede VPC da área de armazenamento pela porta 443. • Na seção Configurações adicionais, selecione Ativar nome DNS.	Líder de migração

Tarefa	Descrição	Habilidades necessárias
Configure o endpoint de interface para o Amazon S3.	O datacenter de origem e a área de armazenamento (VPC) se conectam de forma privada à API do Amazon S3 por meio do endpoint de interface que você cria na VPC da área de armazenam ento de destino. Para criar o endpoint, siga as instruções fornecidas na primeira história. • Em Nome do serviço, digite `com.amazonaws.<reg ion>.s3` . Em Tipo, escolha Interface. • O grupo de segurança da VPC deve permitir o tráfego HTTPS de entrada da sub-rede VPC da área de armazenamento pela porta 443. • Na seção Configurações adicionais, desmarque Habilitar nome DNS. O DNS privado não é compatível com endpoints da interface do Amazon S3. **Note** Você usa um endpoint de interface porque as conexões de endpoint de gateway não	Líder de migração

Tarefa	Descrição	Habilidades necessárias
	podem ser estendidas para fora de uma VPC. (Para obter detalhes, consulte a AWS PrivateLink documentação.)	
Configurar o endpoint do gateway do Amazon S3.	Durante a fase de configuração, o servidor de replicação precisa se conectar a um bucket S3 para baixar as atualizações de software do servidor AWS de replicação. No entanto, os endpoints da interface do Amazon S3 não oferecem suporte a nomes DNS privados, e não há como fornecer um nome DNS de endpoint do Amazon S3 a um servidor de replicação. Para mitigar esse problema, você cria um endpoint de gateway Amazon S3 na VPC à qual a sub-rede da área de teste pertence e atualiza as tabelas de rotas da sub-rede de teste com as rotas relevantes. Para obter mais informações, consulte Criar um endpoint de gateway na AWS PrivateLink documentação.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure o DNS on-premises para resolver nomes DNS privados para endpoints.	Os endpoints de interface do Application Migration Service e da Amazon EC2 têm nomes DNS privados que podem ser resolvidos na VPC. No entanto, você também precisa configurar servidores on-premises para resolver nomes DNS privados para esses endpoints de interface. Há várias maneiras de configurar esses servidores. Nesse padrão, testamos essa funcionalidade encaminhando consultas de DNS locais para o endpoint de Amazon Route 53 Resolver entrada na área de teste VPC. Para obter mais informações, consulte Resolvendo consultas de DNS entre VPCs e sua rede na documentação do Route 53.	Engenheiro de migração

Conecte-se ao ambiente de gerenciamento do Application Migration Service por meio de um link privado

Tarefa	Descrição	Habilidades necessárias
Instale o Agente AWS de Replicação usando o. AWS PrivateLink	1. Faça o download do Agente AWS de Replicação em um bucket S3 privado na região de destino.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	2. Faça login nos servidores de origem a serem migrados. O instalador do AWS Replication Agent precisa de acesso de rede ao Application Migration Service e aos endpoints do Amazon S3. Como sua rede local não está aberta ao Application Migration Service e aos endpoints públicos do Amazon S3, você deve instalar o Agente com a ajuda dos endpoints de interface que você criou nas etapas anteriores usando. AWS PrivateLink Veja um exemplo para Linux: 1. Baixe o agente usando o comando: `wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-<aws_region>.bucket.<s3-endpoint-DNS-name>/latest/linux/aws-replication-installer-init.py`	

Tarefa	Descrição	Habilidades necessárias
	Por exemplo, se o nome DNS do endpoint da interface Amazon S3 `vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com` for e `us-west-1` for, você usaria Região da AWS o comando: `wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-us-west-1.bucket.vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com/latest/linux/aws-replication-installer-init.py` **Note** `bucket`é uma palavra-chave estática que você deve adicionar antes do nome DNS do endpoint da interface Amazon S3. Para mais informaçõ	

Tarefa	Descrição	Habilidades necessárias

	es, consulte a documentação do Amazon S3.
	2. Instalar o agente:
	• Se você selecionou Ativar nome DNS ao criar o endpoint da interface para o Serviço de Migração de Aplicativos, execute o comando:
	`sudo python3 aws-replication-installer-init.py \ --region <aws_region> \ --aws-access-key-id <access-key> \ --aws-secret-access-key <secret-key> \ --no-prompt \ --s3-endpoint <s3-endpoint-DNS-name>`
	• Se você não selecionou Ativar nome DNS ao criar o endpoint da interface para o Serviço de Migração de Aplicativos, execute o comando:
	`sudo python3 aws-replication-installer-init.py \`	

Tarefa	Descrição	Habilidades necessárias

	<pre>--region
	<aws_region> \
	--aws-access-
	key-id <access-k
	ey> \
	--aws-secret-
	access-key <secret-
	key> \
	--no-prompt \
	--s3-endpoint
	<s3-endpoint-DNS-n
	ame> \
	--endpoint
	<mgn-endpoint-DNS-
	name></pre> Para obter mais informaçõ es, consulte as instruçõe s de instalação AWS do Replication Agent na documentação do Applicati on Migration Service. Depois de estabelecer sua conexão com o Application Migration Service e instalar o AWS Replication Agent, siga as instruções na documenta ção do Application Migration Service para migrar seus servidores de origem para sua VPC e sub-rede de destino.	

Recursos relacionados

Documentação do serviço de migração de aplicativos

- Conceitos
- fluxo de trabalho de migração
- Guia de início rápido
- PERGUNTAS FREQUENTES
- Solução de problemas

Recursos adicionais

- Hospedando novamente seus aplicativos em uma arquitetura de várias contas usando endpoints de interface VPC (guia de orientação prescritiva) AWS AWS
- AWS Application Migration Service — Uma introdução técnica (passo a passo de AWS treinamento e certificação)
- AWS Application Migration Service arquitetura e arquitetura de rede (vídeo)

Mais informações

Solução de problemas de instalações AWS do Replication Agent em servidores Linux

Se você receber um erro gcc em um servidor Amazon Linux, configure o repositório de pacotes e use o seguinte comando:

```
## sudo yum groupinstall "Development Tools"
```

Crie objetos Infoblox usando recursos CloudFormation personalizados da AWS e Amazon SNS

Criado por Tim Sutton (AWS)

Resumo

Aviso: não AWS Cloud9 está mais disponível para novos clientes. Os clientes existentes do AWS Cloud9 podem continuar usando o serviço normalmente. Saiba mais

O Sistema de Nomes de Domínio (DNS) do Infoblox, o Protocolo de Configuração Dinâmica de Host (DHCP) e o gerenciamento de endereços IP (Infoblox DDI) permitem centralizar e controlar com eficiência um ambiente híbrido complexo. Com o Infoblox DDI, você pode descobrir e registrar todos os ativos de rede em um banco de dados autoritário de gerenciamento de endereços IP (IPAM), além de gerenciar o DNS on-premises e na nuvem da Amazon Web Services (AWS) usando os mesmos dispositivos.

Esse padrão descreve como usar um recurso CloudFormation personalizado da AWS para criar objetos Infoblox (por exemplo, registros DNS ou objetos IPAM) chamando a API Infoblox WAPI. Para obter mais informações sobre a WAPI do Infoblox, consulte a Documentação do WAPI na documentação do Infoblox.

Ao usar essa abordagem padrão, você pode obter uma visão unificada dos registros DNS e das configurações IPAM para seus ambientes on-premises e da AWS, além de remover processos manuais que criam registros e provisionam suas redes. É possível usar a abordagem desse padrão para os seguintes casos de uso:

- Adicionar um registro A após criar uma instância do Amazon Elastic Compute Cloud (Amazon EC2)
- Adicionar um registro CNAME após criar um Application Load Balancer
- Adicionar um objeto de rede após criar uma nuvem privada virtual (VPC)
- Fornecendo o próximo intervalo de rede e usando esse intervalo para criar sub-redes

Você também pode estender esse padrão e usar outros recursos do dispositivo Infoblox, como adicionar diferentes tipos de registro DNS ou configurar o Infoblox vDiscovery.

O padrão usa um hub-and-spoke design no qual o hub exige conectividade com o dispositivo Infoblox na nuvem da AWS ou no local e usa o AWS Lambda para chamar a API da Infoblox.

O spoke está na mesma conta ou em uma conta diferente na mesma organização no AWS Organizations e chama a função Lambda usando um recurso CloudFormation personalizado da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Um dispositivo ou grade existente da Infoblox, instalado na nuvem AWS, on-premises ou em ambos, e configurado com um usuário administrador que pode administrar ações de IPAM e DNS. Para obter mais informações sobre isso, consulte Sobre contas de administrador na documentação do Infoblox.
- Uma zona autoritativa de DNS existente na qual você deseja adicionar registros no dispositivo Infoblox. Para obter mais informações sobre isso, consulte Configurando zonas autoritativas na documentação do Infoblox.
- Duas contas ativas da AWS no AWS Organizations. Uma conta é a conta hub e a outra conta é a conta spoke.
- O hub e as contas spoke devem estar na mesma região da AWS.
- A VPC da conta do hub deve se conectar ao dispositivo Infoblox; por exemplo, usando o AWS Transit Gateway ou emparelhamento da VPC.
- AWS Serverless Application Model (AWS SAM), instalado e configurado localmente com o AWS Cloud9 ou AWS. CloudShell
- Os arquivos `Infoblox-Hub.zip` e `ClientTest.yaml` (anexados), baixados para o ambiente local que contém o AWS SAM.

Limitações

- O token de serviço do recurso CloudFormation personalizado da AWS deve ser da mesma região em que a pilha foi criada. Recomendamos usar uma conta hub em cada região, em vez de criar um tópico do Amazon Simple Notification Service (Amazon SNS) em uma região e chamar a função do Lambda em outra.

Versões do produto

- Infoblox WAPI versão 2.7

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho desse padrão.

O diagrama mostra os seguintes componentes para a solução desse padrão:

1. Os recursos CloudFormation personalizados da AWS permitem que você escreva uma lógica de provisionamento personalizada em modelos que a AWS CloudFormation executa quando você cria, atualiza ou exclui pilhas. Quando você cria uma pilha, a AWS CloudFormation envia uma `create` solicitação para um tópico do SNS que é monitorado por um aplicativo executado em uma EC2 instância.
2. A notificação do Amazon SNS do recurso CloudFormation personalizado da AWS é criptografada por meio de uma chave específica do AWS Key Management Service (AWS KMS) e o acesso é restrito às contas da sua organização em Organizations. O tópico do SNS inicia o recurso Lambda que chama a API WAPI da Infoblox.
3. O Amazon SNS invoca as seguintes funções do Lambda que usam o URL WAPI do Infoblox, o nome de usuário e a senha do AWS Secrets Manager Amazon Resource Names () como variáveis de ambiente: ARNs
   - `dnsapi.lambda_handler`— Recebe os `DNSValue` valores `DNSNameDNSType`,, e do recurso CloudFormation personalizado da AWS e os usa para criar registros DNS A e CNAMES.
   - `ipaddr.lambda_handler`— Recebe os `Network Name` valores `VPCCIDRType`,`SubnetPrefix`, e do recurso CloudFormation personalizado da AWS e os usa para adicionar os dados da rede ao banco de dados IPAM da Infoblox ou fornecer ao recurso personalizado a próxima rede disponível que pode ser usada para criar novas sub-redes.
   - `describeprefixes.lambda_handler`: chama a API da AWS `describe_managed_prefix_lists` usando o filtro `"com.amazonaws."+Region+".s3"` para recuperar a `prefix ID` necessária.

   > **Important**
   >
   > Essas funções do Lambda são escritas em Python e são semelhantes entre si, mas têm chamadas diferentes. APIs
4. Você pode implantar a grade Infoblox como dispositivos de rede físicos, virtuais ou baseados em nuvem. Ele pode ser implantado localmente ou como um dispositivo virtual usando uma variedade de hipervisores, incluindo VMware ESXi Microsoft Hyper-V, Linux KVM e Xen. Você

também pode implantar a grade do Infoblox na nuvem AWS com uma imagem de máquina da Amazon (AMI).

5. O diagrama mostra uma solução híbrida para a grade da Infoblox que fornece DNS e IPAM para recursos na nuvem AWS e on-premises.

Pilha de tecnologia

- AWS CloudFormation
- IAM
- AWS KMS
- AWS Lambda
- AWS SAM
- AWS Secrets Manager
- Amazon SNS
- Amazon VPC

Ferramentas

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Organizations é um serviço de gerenciamento de contas que ajuda a consolidar várias contas da AWS em uma organização que você cria e gerencia de maneira centralizada.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente.

- O AWS Serverless Application Model (AWS SAM) é uma estrutura de código aberto que ajuda na criação de aplicativos sem servidor na Nuvem AWS.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Código

Você pode usar o CloudFormation modelo de `ClientTest.yaml` amostra da AWS (anexado) para testar o hub Infoblox. Você pode personalizar o CloudFormation modelo da AWS para incluir os recursos personalizados da tabela a seguir.

Crie um registro A usando o recurso personalizado Infoblox spoke	Retornar valores:
	`infobloxref` : referências do Infoblox
	Exemplo de recurso:
	`ARECORDCustomResource:`
	`  Type: "Custom::InfobloxAPI"`
	`  Properties:`
	`  ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxDNSFunction`
	`  DNSName: 'arecordtest.company.com'`
	`  DNSType: 'ARecord'`
	`  DNSValue: '10.0.0.1'`

Crie um registro CNAME usando o recurso personalizado Infoblox spoke	Retornar valores: `infobloxref` : referências do Infoblox

Exemplo de recurso:

```
CNAMECustomResource:

  Type: "Custom::InfobloxAPI"

  Properties:

    ServiceToken: !Sub arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfoblox

    DNSFunction

    DNSName: 'cnametest.company.com'

    DNSType: 'cname'

    DNSValue: 'aws.amazon.com'
```

Crie um objeto de rede usando o recurso personalizado Infoblox spoke	Retornar valores:
	`infobloxref` : referências do Infoblox
	`network`: alcance da rede (o mesmo do `VPCCIDR`)
	Exemplo de recurso:
	`VPCCustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  Properties:`
	`    ServiceToken: !Sub  arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`    VPCCIDR: !Ref VpcCIDR`
	`    Type: VPC`
	`    NetworkName: My-VPC`

Recupere a próxima sub-rede disponível usando o recurso personalizado Infoblox spoke	Retornar valores:
	`infobloxref` : referências do Infoblox
	`network` : o alcance da rede da sub-rede
	Exemplo de recurso:
	`Subnet1CustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  DependsOn: VPCCustomResource`
	`  Properties:`
	`  ServiceToken: !Sub  arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`  VPCCIDR: !Ref VpcCIDR`
	`  Type: Subnet`
	`  SubnetPrefix: !Ref SubnetPrefix`
	`NetworkName: My-Subnet`

Épicos

Crie e configure a VPC da conta do hub

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC com uma conexão com o dispositivo Infoblox.	Faça login no Console de Gerenciamento da AWS da sua conta do hub e crie uma VPC seguindo as etapas na Amazon VPC na implantação de referência de Início Rápido	Administrador de rede, administrador de sistema

Tarefa	Descrição	Habilidades necessárias
	da Nuvem AWS a partir do AWS Quick Starts. **Important** A VPC deve ter conectividade HTTPS com o dispositivo Infoblox e recomendamos que você use uma sub-rede privada para essa conexão.	

Tarefa	Descrição	Habilidades necessárias
(Opcional) Crie os endpoints da VPC para sub-redes privadas.	Os endpoints da VPC fornecem conectividade a serviços públicos para suas sub-redes privadas. Os seguintes endpoints são exigidos: • Um endpoint de gateway para o Amazon Simple Storage Service (Amazon S3) para permitir que o Lambda se comunique com a AWS CloudFormation • Um endpoint de interface para o Secrets Manager para permitir a conectividade com o Secrets Manager • Um endpoint de interface para o AWS KMS para permitir a criptografia do tópico do SNS e do segredo do Secrets Manager Para obter mais informações sobre como criar endpoints para sub-redes privadas, consulte Endpoints da VPC na documentação da Amazon VPC.	Administrador de rede, Administrador de sistemas

Implemente o hub Infoblox

Tarefa	Descrição	Habilidades necessárias
Crie o modelo do AWS SAM.	1. Execute o comando `unzip Infoblox-Hub.zip` no ambiente que contém o AWS SAM. 2. Execute o comando `cd Hub/` para alterar seu diretório para o diretório `Hub`. 3. Execute o comando `sam build` para processar o arquivo de modelo do AWS SAM, o código do aplicativo e quaisquer arquivos e dependências específicos da linguagem. O comando `sam build` também copia artefatos de construção no formato e no local esperados para a história a seguir.	Desenvolvedor, Administrador de sistemas
Implante o modelo do SAM da AWS.	O `sam deploy` comando pega os parâmetros necessários e os salva no `samconfig.toml` arquivo, armazena o CloudFormation modelo da AWS e as funções do Lambda em um bucket do S3 e, em seguida, implanta o modelo da CloudFormation AWS em sua conta do hub.	Desenvolvedor, Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias

	O código de exemplo a seguir mostra como implantar o modelo do SAM da AWS:
	
	`$ sam deploy --guided`
	
	`Configuring SAM deploy`
	`==========`
	`==`
	`Looking for config file [samconfig.toml] : Found`
	`Reading default arguments : Success`
	`Setting default arguments for 'sam deploy'`
	`==========`
	`==========`
	`==========`
	`Stack Name [Infoblox-Hub]:`
	`AWS Region [eu-west-1]:`
	`Parameter InfobloxUsername:`
	`Parameter InfobloxPassword:`
	`Parameter InfobloxIPAddress [xxx.xxx.xx.xxx]:`
	`Parameter AWSOrganisationID [o-xxxxxxxxx]:`
	`Parameter VPCID [vpc-xxxxxxxxx]:`
	`Parameter VPCCIDR [xxx.xxx.xxx.xxx/16]:`	

Tarefa	Descrição	Habilidades necessárias
	Parameter VPCSubnetID1 [subnet-xxx]: Parameter VPCSubnetID2 [subnet-xxx]: Parameter VPCSubnetID3 [subnet-xxx]: Parameter VPCSubnetID4 []: #Shows you resources changes to be deployed and require a 'Y' to initiate deploy Confirm changes before deploy [Y/n]: y #SAM needs permission to be able to create roles to connect to the resources in your template Allow SAM CLI IAM role creation [Y/n]: n Capabilities [['CAPABILITY_NAMED_IAM']]: Save arguments to configuration file [Y/n]: y SAM configuration file [samconfig.toml]: SAM configuration environment [default]: **Important** Você deve usar a `--guided` opção todas	

Tarefa	Descrição	Habilidades necessárias
	as vezes porque as credenciais de login do Infoblox não são armazenadas no arquivo. `samconfig.toml`	

Recursos relacionados

- Começando a WAPIs usar o Postman (Infoblox Blog)
- Provisionamento de vNIOS para AWS usando o modelo BYOL (documentação do Infoblox)
- quickstart-aws-vpc(GitHub recompra)
- describe_managed_prefix_lists (documentação do AWS SDK para Python)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Personalize os CloudWatch alertas da Amazon para AWS Network Firewall

Criado por Jason Owens (AWS)

Resumo

O padrão ajuda você a personalizar os CloudWatch alertas da Amazon que são gerados por AWS Network Firewall. Você poderá usar regras predefinidas ou criar regras personalizadas que determinam a mensagem, os metadados e a gravidade dos alertas. Você pode então agir de acordo com esses alertas ou automatizar as respostas de outros serviços da Amazon, como a Amazon EventBridge.

Nesse padrão, você gera regras de firewall compatíveis com o Suricata. O Suricata é um mecanismo de detecção de ameaças de código aberto. Primeiro, você cria regras simples e depois as testa para confirmar se os CloudWatch alertas foram gerados e registrados. Depois de testar as regras com sucesso, você as modifica para definir mensagens, metadados e severidades personalizados e, em seguida, testa mais uma vez para confirmar as atualizações.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Command Line Interface (AWS CLI) instalado e configurado em sua estação de trabalho Linux, macOS ou Windows. Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI.
- AWS Network Firewall instalado e configurado para usar o CloudWatch Logs. Para obter mais informações, consulte Registrar tráfego de rede de AWS Network Firewall.
- Uma instância do Amazon Elastic Compute Cloud (Amazon EC2) em uma sub-rede privada de uma nuvem privada virtual (VPC) protegida pelo Firewall de Rede.

Versões do produto

- Para a versão 1 do AWS CLI, use 1.18.180 ou posterior. Para a versão 2 do AWS CLI, use 2.1.2 ou posterior.
- O arquivo classification.config do Suricata versão 5.0.2. Para obter uma cópia desse arquivo de configuração, consulte a seção Informações adicionais.

Arquitetura

O diagrama da arquitetura mostra o seguinte fluxo de trabalho:

1. Uma EC2 instância da Amazon em uma sub-rede privada faz uma solicitação usando curl ou Wget.
2. O Network Firewall processa o tráfego e gera um alerta.
3. O Network Firewall envia os alertas registrados para o CloudWatch Logs.

Ferramentas

Serviços da AWS

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas e aplicativos, Serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS Network Firewallé um serviço gerenciado e estável de firewall de rede e detecção e prevenção de intrusões para nuvens privadas virtuais (VPCs) no. Nuvem AWS

Outras ferramentas

- curl é uma ferramenta e biblioteca de linha de comando de código aberto.
- GNU Wget é uma ferramenta de linha de comando gratuita.

Épicos

Crie as regras de firewall e o grupo de regras

Tarefa	Descrição	Habilidades necessárias
Criar regras.	1. Em um editor de texto, crie uma lista de regras	Administrador de sistemas da AWS, administrador de rede

Tarefa	Descrição	Habilidades necessárias

	que você deseja adicionar ao firewall. Cada regra deverá estar em uma linha separada. O valor no parâmetro `classtype` é do arquivo de configuração padrão da classificação Suricata. Para ver o conteúdo completo do arquivo de configuração, consulte a seção Informações adicionais. Veja os dois exemplos de regras a seguir.
	`alert http any any -> any any (content:"badstuff"; classtype:misc-activity; sid:3; rev:1;)`
	`alert http any any -> any any (content:"morebadstuff"; classtype:bad-unknown; sid:4; rev:1;)`
	2. Salve as regras em um arquivo chamado `custom.rules` .	

Tarefa	Descrição	Habilidades necessárias

Criar o grupo de regras.	No AWS CLI, insira o seguinte comando. Isso cria o grupo de regras.
	
	`# aws network-firewall create-rule-group \ --rule-group-name custom --type STATEFUL \ --capacity 10 --rules file://custom.rules \ --tags Key=environment,Value=development`
	
	Veja a seguir um exemplo de saída. Anote o `RuleGroup Arn` , que você vai precisar em uma etapa posterior.
	
	`{ "UpdateToken": "4f998d72-973c-490a-bed2-fc3460547e23", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b", "Type": "STATEFUL",`
		Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>"Capacity": 10,
	"RuleGrou
	pStatus": "ACTIVE",
	"Tags": [
	{
	"Key":
	"environment",
	"Value":
	"development"
	}
	]
	}</pre>	

Atualizar a política de firewall

Tarefa	Descrição	Habilidades necessárias

Obtenha o ARN da política de firewall.	No AWS CLI, insira o seguinte comando. Isto retorna o nome do recurso da Amazon (ARN) da política de firewall. Registre o ARN para uso mais tarde nesse padrão.
	<pre># aws network-firewall
	describe-firewall \
	--firewall-name
	aws-network-firewall-
	anfw \
	--query 'Firewall
	.FirewallPolicyArn'</pre>
	Veja o seguinte exemplo de ARN retornado por esse comando.
		Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	`"arn:aws:network-firewall:us-east-2:1234567890:firewall-policy/firewall-policy-anfw"`	

Tarefa	Descrição	Habilidades necessárias
Atualizar a política de firewall.	No editor de texto, copie e cole o código a seguir. Substitua `<RuleGroupArn>` pelo valor que você registrou no épico anterior. Salve o arquivo como `firewall-policy-anfw.json` . `{ "StatelessDefaultActions": [ "aws:forward_to_sfe" ], "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ], "StatefulRuleGroupReferences": [ { "ResourceArn": "<RuleGroupArn>" } ] }` Digite o seguinte comando no AWS CLI. Esse comando requer um token de atualização para adicionar as novas regras. O token é usado para confirmar que a política não foi alterada desde a última vez que você a recuperou.	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	`UPDATETOKEN=(`aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --output text --query UpdateToken`)`
	
	`aws network-firewall update-firewall-policy \ --update-token $UPDATETOKEN \ --firewall-policy-name firewall-policy-anfw \ --firewall-policy file://firewall-policy-anfw.json`	

Tarefa	Descrição	Habilidades necessárias

Confirme as atualizações da política.	(Opcional) Se você quiser confirmar que as regras foram adicionadas e visualizar o formato da política, digite o seguinte comando no AWS CLI.
	
	`# aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --query FirewallPolicy`
	
	Veja a seguir um exemplo de saída.
	
	`{ "StatelessDefaultActions": [ "aws:forward_to_sfe" ], "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ], "StatefulRuleGroupReferences": [ { "ResourceArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom"`
		Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	<pre> }] }</pre>	

Testar a funcionalidade do alerta

Tarefa	Descrição	Habilidades necessárias

Gere alertas para testes.	1. Faça login em uma estação de trabalho de teste na sub-rede do firewall.
	2. Insira os comandos que devem gerar alertas. Por exemplo, você poderá usar o `wget` ou o `curl`.
	<pre>wget -U "badstuff"
	 http://www.amazon.
	com -o /dev/null</pre>
	<pre>curl -A "morebads
	tuff" http://ww
	w.amazon.com -o /
	dev/null</pre>
		Administrador de sistemas AWS

Valide se os alertas estão registrados.	1. Abra o console de CloudWatch . 2. Navegue até o grupo de logs e o stream corretos. Para obter mais informaçõ es, consulte Exibir dados de registro enviados para o CloudWatch	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	Logs (documentação de CloudWatch registros).
	3. Confirme se os eventos de logs são semelhantes aos exemplos a seguir. Os exemplos mostram somente a parte relevante do alerta.
	
	Exemplo 1
	
	`"alert": { "action": "allowed", "signature_id": 3, "rev": 1, "signature": "", "category": "Misc activity", "severity": 3 }`
	
	Exemplo 2
	
	`"alert": { "action": "allowed", "signature_id": 4, "rev": 1, "signature": "", "category": "Potentially Bad Traffic",`	

Tarefa	Descrição	Habilidades necessárias
	<pre>"severity ": 2 }</pre>	

Atualize as regras de firewall e o grupo de regras

Tarefa	Descrição	Habilidades necessárias
Atualize as regras do firewall.	1. Em um editor de texto, abra o arquivo `custom.rules` . 2. Altere a primeira regra para ser semelhante à regra a seguir. Essa regra deverá ser inserida em uma única linha no arquivo. <pre>alert http any any -> any any (msg:"Watch out - Bad Stuff!!"; content:"badstuff" ; classtype:misc-activity; priority: 2; sid:3; rev:2; metadata:custom-field-2 Danger!, custom-field More Info;)</pre> Isso realiza as seguintes alterações na regra: • Adiciona uma string msg (site da Suricata) que fornece informações de texto sobre a assinatura ou o alerta. No alerta	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	gerado, isso é mapeado para a assinatura. • Ajusta a prioridade padrão (site da Suricata) de `misc-activity` , de 3 para 2. Para obter os valores padrão dos vários `classtypes` , consulte a seção Informações adicionais. • Adiciona metadados personalizados (site da Suricata) ao alerta. Essas são informaçõ es adicionais que são adicionadas à assinatur a. É recomendável usar pares de chave-valor. • Altera o rev (site da Suricata) de 1 para 2. Isso representa a versão da assinatura.	

Tarefa	Descrição	Habilidades necessárias

Atualizar o grupo de regras.	No AWS CLI, execute os seguintes comandos. Use o ARN da sua política de firewall. Esses comandos obtêm um token de atualizaç ão e atualizam o grupo de regras com as alterações da regra.
	`# UPDATETOKEN=(`aws network-firewall \ describe-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:123457890:stateful-rulegroup/custom \ --output text --query UpdateToken`)`
	`# aws network-firewall update-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom \ --rules file://custom.rules \ --update-token $UPDATETOKEN`
	Veja a seguir um exemplo de saída.
	`{`
		Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	"UpdateToken": "7536939f-6a1d-414c-96d1-bb28110996ed", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b", "Type": "STATEFUL", "Capacity": 10, "RuleGroupStatus": "ACTIVE", "Tags": [{ "Key": "environment", "Value": "development" }] } }	

Testar a funcionalidade de alerta atualizada

Tarefa	Descrição	Habilidades necessárias
Gere um alerta para testes.	1. Faça login em uma estação de trabalho de teste na sub-rede do firewall.	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	2. Insira um comando que deveria gerar um alerta. Por exemplo, você poderá usar o `curl`. `curl -A "badstuff" http://www.amazon.com -o /dev/null`	

Tarefa	Descrição	Habilidades necessárias
Valide o alerta alterado.	1. Abra o console de CloudWatch . 2. Navegue até o grupo de logs e o stream corretos. 3. Confirme se o evento de logs é semelhante ao exemplo a seguir. O exemplo mostra somente a parte relevante do alerta. `"alert": { "action": "allowed", "signature_id": 3, "rev": 2, "signature": "Watch out - Bad Stuff!!", "category": "Misc activity", "severity": 2, "metadata": { "custom-field": [ "More Info" ], "custom-field-2": [ "Danger!" ] } }`	Administrador de sistemas AWS

Recursos relacionados

Referências

- Envie alertas AWS Network Firewall para um canal do Slack (orientação AWS prescritiva)
- Aumentando a prevenção de ameaças AWS com Suricata (AWS postagem no blog)
- Modelos de implantação para AWS Network Firewall (postagem AWS no blog)
- Meta-chaves do Suricata(Documentação do Suricata)

Tutoriais e vídeos

- AWS Network Firewall oficina

Mais informações

Veja a seguir o arquivo de configuração de classificação do Suricata 5.0.2. Essas classificações são usadas ao criar as regras de firewall.

```
# config classification:shortname,short description,priority

config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
config classification: successful-admin,Successful Administrator Privilege Gain,1

# NEW CLASSIFICATIONS
config classification: rpc-portmap-decode,Decode of an RPC Query,2
config classification: shellcode-detect,Executable code was detected,1
config classification: string-detect,A suspicious string was detected,3
config classification: suspicious-filename-detect,A suspicious filename was detected,2
```

```
config classification: suspicious-login,An attempted login using a suspicious username
 was detected,2
config classification: system-call-detect,A system call was detected,2
config classification: tcp-connection,A TCP connection was detected,4
config classification: trojan-activity,A Network Trojan was detected, 1
config classification: unusual-client-port-connection,A client was using an unusual
 port,2
config classification: network-scan,Detection of a Network Scan,3
config classification: denial-of-service,Detection of a Denial of Service Attack,2
config classification: non-standard-protocol,Detection of a non-standard protocol or
 event,2
config classification: protocol-command-decode,Generic Protocol Command Decode,3
config classification: web-application-activity,access to a potentially vulnerable web
 application,2
config classification: web-application-attack,Web Application Attack,1
config classification: misc-activity,Misc activity,3
config classification: misc-attack,Misc Attack,2
config classification: icmp-event,Generic ICMP event,3
config classification: inappropriate-content,Inappropriate Content was Detected,1
config classification: policy-violation,Potential Corporate Privacy Violation,1
config classification: default-login-attempt,Attempt to login by a default username and
 password,2

# Update
config classification: targeted-activity,Targeted Malicious Activity was Detected,1
config classification: exploit-kit,Exploit Kit Activity Detected,1
config classification: external-ip-check,Device Retrieving External IP Address
 Detected,2
config classification: domain-c2,Domain Observed Used for C2 Detected,1
config classification: pup-activity,Possibly Unwanted Program Detected,2
config classification: credential-theft,Successful Credential Theft Detected,1
config classification: social-engineering,Possible Social Engineering Attempted,2
config classification: coin-mining,Crypto Currency Mining Activity Detected,2
config classification: command-and-control,Malware Command and Control Activity
 Detected,1
```

Implante recursos em uma AWS Wavelength zona usando o Terraform

Criado por Zahoor Chaudhrey (AWS) e Luca Iannario (AWS)

Resumo

AWS Wavelengthajuda você a criar uma infraestrutura otimizada para aplicativos de Computação de Borda de Acesso Múltiplo (MEC). AWS As zonas de Wavelength são implantações de infraestrutura que AWS incorporam serviços de computação e armazenamento nas redes 5G dos provedores de serviços de comunicação (CSP). O tráfego de aplicativos de dispositivos 5G chega aos servidores de aplicativos em execução nas zonas de Wavelength sem sair da rede de telecomunicações. O seguinte facilita a conectividade de rede por meio do Wavelength:

- Nuvens privadas virtuais (VPCs) — VPCs em uma Conta da AWS podem se estender para abranger várias zonas de disponibilidade, incluindo zonas de comprimento de onda. As instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e os serviços relacionados aparecem como parte da sua VPC regional. VPCs são criados e gerenciados na Amazon Virtual Private Cloud (Amazon VPC).
- Gateway da operadora — Um gateway da operadora permite a conectividade da sub-rede na Wavelength Zone à rede do CSP, à Internet ou por meio da rede Região da AWS do CSP. O gateway da operadora tem duas finalidades. Ele permite tráfego de entrada de uma rede CSP em um local específico e permite tráfego de saída para a rede de telecomunicações e a Internet.

Esse padrão e o código Terraform associado ajudam você a lançar recursos, como EC2 instâncias da Amazon, volumes do Amazon Elastic Block Store (Amazon EBS), sub-redes e um gateway de operadora VPCs, em uma zona de Wavelength.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um ambiente de desenvolvimento integrado (IDE)
- Opte pela Zona de Wavelength de destino
- AWS Command Line Interface (AWS CLI), instalado e configurado
- Terraform versão 1.8.4 ou posterior, instalado (documentação do Terraform)
- Terraform AWS Provider versão 5.32.1 ou posterior, configurada (documentação do Terraform)

- Git, instalado () GitHub
- Permissões para criar recursos Amazon VPC, Wavelength e Amazon EC2

Limitações

Nem todos são Regiões da AWS compatíveis com zonas de Wavelength. Para obter mais informações, consulte Zonas de comprimento de onda disponíveis na documentação do comprimento de onda.

Arquitetura

O diagrama a seguir mostra como você pode criar uma sub-rede e AWS recursos em uma zona de Wavelength. VPCs que contêm uma sub-rede em uma zona de Wavelength podem se conectar a um gateway de operadora. Um gateway de operadora permite que você se conecte aos seguintes recursos:

- Dispositivos 4G/LTE e 5G na rede da operadora de telecomunicações.
- Acesso sem fio fixo para parceiros selecionados da Wavelength Zone. Para obter mais informações, consulte Acesso AWS Wavelength múltiplo.
- Tráfego de saída para recursos públicos da Internet.

Ferramentas

Serviços da AWS

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.
- AWS Wavelengthestende a Nuvem AWS infraestrutura às redes 5G dos provedores de telecomunicações. Isso ajuda você a criar aplicativos que oferecem latências ultrabaixas para dispositivos móveis e usuários finais.

Outras ferramentas

- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Repositório de código

O código desse padrão está disponível no repositório GitHub Creating AWS Wavelength Infrastructure using Terraform. O código do Terraform implanta a seguinte infraestrutura e recursos:

- Uma VPC
- Uma zona de comprimento de onda
- Uma sub-rede púbica na Wavelength Zone
- Um gateway de operadora na Wavelength Zone
- Uma EC2 instância da Amazon na Wavelength Zone

Práticas recomendadas

- Antes de implantar, confirme se você está usando as versões mais recentes do Terraform e do. AWS CLI
- Use um pipeline de integração contínua e entrega contínua (CI/CD) para implantar o IaC. Para obter mais informações, consulte Práticas recomendadas para gerenciar arquivos de estado do Terraform no AWS CI/CD Pipeline em blogs. AWS

Épicos

Provisionar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Insira o comando a seguir para clonar o repositório Creating AWS Wavelength Infrastructure using Terraform em seu ambiente. `git clone git@github.com:aws-samples/terraform-waveleng th-infrastructure. git`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Atualize as variáveis.	1. Navegue até o repositório clonado. `cd terraform-wavelength-infrastructure` 2. Usando qualquer editor de texto, crie um arquivo chamado terraform.tfvars no diretório raiz. 3. Crie as seguintes variáveis e insira seus valores: • `region = <enter Region name>` • `vpc_cidr = <enter CIDR block used by VPC>` • `wavelength_subnet_cidr = <enter CIDR block for the subnet in the Wavelength Zone>` • `availabilityzone_wavelength = <enter Wavelength Zone name>` 4. Salve o arquivo terraform.tfvars.	DevOps engenheiro, Terraform

Tarefa	Descrição	Habilidades necessárias
Inicialize a configuração.	Digite o comando a seguir para inicializar o diretório de trabalho. `terraform init`	DevOps engenheiro, Terraform
Visualize o plano do Terraform .	Digite o comando a seguir para comparar o estado de destino com o estado atual do seu AWS ambiente. Esse comando gera uma visualização prévia dos recursos que serão configurados. `terraform plan`	DevOps engenheiro, Terraform

Tarefa	Descrição	Habilidades necessárias
Verifique e implante.	1. Revise as alterações de configuração no plano do Terraform e confirme que você deseja implementar essas alterações. 2. Insira o comando a seguir para aplicar o plano e criar a infraestrutura. `terraform apply` 3. Entre `yes` para continuar. O Terraform cria a arquitetura que é declarada nos arquivos de configuração. Para obter mais informações sobre a arquitetura, consulte a seção Arquitetura do Target desse padrão.	DevOps engenheiro, Terraform

Validar e limpar

Tarefa	Descrição	Habilidades necessárias
Verifique a implantação da infraestrutura.	1. Se você ainda não tem uma EC2 instância da Amazon em uma sub-rede pública na sua Região da AWS, crie uma. Para obter instruções, consulte Iniciar sua instância do Linux ou Iniciar sua instância do Windows. Você usará essa instância para testar	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	a conectividade entre a Wavelength Zone e Região da AWS a Wavelength Zone. 2. Teste a conectividade da instância na Região da AWS para a instância na Wavelength Zone. Para obter instruções, consulte Testar a conectividade na documentação do Wavelength.	
(Opcional) Limpe a infraestrutura.	Se você precisar excluir todos os recursos que foram provisionados pelo Terraform, faça o seguinte: 1. Insira o comando da a seguir. `terraform destroy` 2. Digite `yes` para confirmar.	DevOps engenheiro, Terraform

Solução de problemas

Problema	Solução
Conectividade com EC2 instâncias da Amazon no Região da AWS.	Consulte Solucionar problemas de conexão com sua instância Linux ou Solucionar problemas de conexão com sua instância do Windows.

Problema	Solução
Conectividade com EC2 instâncias da Amazon na Wavelength Zone.	Consulte Solucionar problemas de conectividade SSH ou RDP com minhas EC2 instâncias lançadas em uma zona de Wavelength.
Capacidade na zona de comprimento de onda.	Consulte Cotas e considerações para zonas de comprimento de onda.
Conectividade móvel ou operadora da rede da operadora para Região da AWS o.	1. Verifique se o gateway da operadora está operacional. Faça o seguinte: a. Abra o console da Amazon VPC. b. No painel de navegação, escolha Seu VPCs. c. Selecione o VPC que contém a Wavelength Zone. d. No painel Detalhes, para Carrier gateway, confirme se o valor está anexado. 2. Verifique se todos os endereços IP elásticos anexados às instâncias na Wavelength Zone estão operacionais. Faça o seguinte: a. Abra o EC2 console da Amazon. b. No painel de navegação, escolha Instâncias. c. Selecione a instância na Wavelength Zone. d. Escolha a guia Redes. e. Confirme se a interface de rede elástica tem um endereço IP elástico anexado. 3. Entre em contato com a equipe de suporte da rede da operadora.

Recursos relacionados

- O que AWS Wavelengthé
- Como AWS Wavelength funciona
- Resiliência em AWS Wavelength

Migre registros de DNS em massa para uma zona hospedada privada do Amazon Route 53

Criado por Ram Kandaswamy (AWS)

Resumo

Engenheiros de rede e administradores de nuvem precisam de uma maneira eficiente e simples de adicionar registros do Sistema de Nomes de Domínio (DNS) às zonas hospedadas privadas no Amazon Route 53. Usar uma abordagem manual para copiar entradas de uma planilha do Microsoft Excel para locais apropriados no console do Route 53 é entediante e propenso a erros. Esse padrão descreve uma abordagem automatizada que reduz o tempo e o esforço necessários para adicionar vários registros. Ele também fornece um conjunto repetível de etapas para a criação de várias zonas hospedadas.

Esse padrão usa o Amazon Simple Storage Service (Amazon S3) para armazenar registros. Para trabalhar com dados de forma eficiente, o padrão usa o formato JSON devido à sua simplicidade e à capacidade de oferecer suporte a um dicionário Python (tipo de dados `dict`).

> **Note**
>
> Se você puder gerar um arquivo de zona do seu sistema, considere usar o recurso de importação do Route 53 em vez disso.

Pré-requisitos e limitações

Pré-requisitos

- Uma planilha do Excel que contém registros de zona hospedada privada
- Familiaridade com diferentes tipos de registros DNS, como registro A, registro Ponteiro de autoridade de nome (NAPTR - Name Authority Pointer record) e registro SRV (consulte Tipos de registro DNS suportados)
- Familiaridade com a linguagem Python e suas bibliotecas

Limitações

- O padrão não oferece cobertura abrangente para todos os cenários de casos de uso. Por exemplo, a chamada change_resource_record_sets não usa todas as propriedades disponíveis da API.
- Na planilha do Excel, o valor em cada linha é considerado exclusivo. Espera-se que vários valores para cada nome de domínio totalmente qualificado (FQDN - fully qualified domain name) apareçam na mesma linha. Se isso não for verdade, você deve modificar o código fornecido nesse padrão para realizar a concatenação necessária.
- O padrão usa o AWS SDK para Python (Boto3) para chamar diretamente o serviço Route 53. Você pode aprimorar o código para usar um CloudFormation wrapper da AWS para os `update_stack` comandos `create_stack` and e usar os valores JSON para preencher os recursos do modelo.

Arquitetura

Pilha de tecnologia

- Zonas hospedadas privadas do Route 53 para roteamento de tráfego
- Amazon S3 para armazenar o arquivo JSON de saída

O fluxo de trabalho consiste nessas etapas, conforme ilustrado no diagrama anterior e discutido na seção Épicos:

1. Faça upload de uma planilha do Excel que tenha as informações do conjunto de registros em um bucket do S3.
2. Crie e execute um script Python que converta os dados do Excel para o formato JSON.
3. Leia os registros do bucket do S3 e limpe os dados.
4. Crie conjuntos de registros em sua zona hospedada privada.

Ferramentas

- Route 53: o Amazon Route 53 é um serviço web de DNS altamente disponível e escalável que gerencia registro de domínios, roteamento de DNS e verificação de integridade.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.

Épicos

Prepare dados para automação

Tarefa	Descrição	Habilidades necessárias
Crie um arquivo Excel para seus registros.	Use os registros que você exportou do seu sistema atual para criar uma planilha do Excel que tenha as colunas necessárias para um registro, como nome de domínio totalmente qualificado (FQDN), tipo de registro, tempo de vida (TTL) e valor. Para registros NAPTR e SRV, o valor é uma combinação de várias propriedades, então use o método `concat` do Excel para combinar essas propriedades. FqdnN Recor Valor TTL e somet A 1.1.1.1 900 .exam org	Engenheiro de dados, habilidades em Excel
Verifique o ambiente de trabalho.	No seu IDE, crie um arquivo Python para converter a planilha de entrada do Excel para o formato JSON. (Em vez de um IDE, você também pode usar um SageMaker notebook da Amazon para trabalhar com código Python.)	AWS geral

Tarefa	Descrição	Habilidades necessárias

	Verifique se a versão do Python que você está usando é a versão 3.7 ou superior.
	`python3 --version`
	Instale o pacote do pandas.
	`pip3 install pandas --user`	

Converta os dados da planilha do Excel em JSON.	Crie um arquivo Python que contenha o código a seguir para converter do Excel para JSON.
	`import pandas as pd`
	`data=pd.read_excel('./Book1.xls')`
	`data.to_json(path_or_buf='my.json', orient='records')`
	onde `Book1` é o nome da planilha do Excel e `my.json` é o nome do arquivo JSON de saída.
		Engenheiro de dados, habilidades em Python

Faça upload do arquivo JSON em um bucket do S3.	Faça upload do arquivo `my.json` em um bucket do S3. Para obter mais informações, consulte Criar um bucket na documentação do Amazon S3.	Desenvolvedor de aplicativos

Inserir registros

Tarefa	Descrição	Habilidades necessárias

Crie uma zona hospedada privada.	Use a API create_hosted_zone e o código de exemplo do Python a seguir para criar uma zona hospedada privada. Substitua os valores dos parâmetros `hostedZoneName`, `vpcRegion`, e `vpcId` pelos seus próprios valores.
	`import boto3`
	`import random`
	`hostedZoneName ="xxx"`
	`vpcRegion = "us-east-1"`
	`vpcId="vpc-xxxx"`
	`route53_client = boto3.client('route53')`
	`response = route53_client.create_hosted_zone(`
	`Name= hostedZoneName,`
	`VPC={`
	`'VPCRegion: vpcRegion,`
	`'VPCId': vpcId`
	`},`
	`CallerReference=str(random.random()*100000),`
	`HostedZoneConfig={`
	`'Comment': "private hosted zone`
		Arquiteto de nuvem, administrador de rede, habilidades em Python

Tarefa	Descrição	Habilidades necessárias

	<pre>created by automatio
	n",
	'PrivateZ
	one': True
	}
	)
	print(response)</pre>
	Você também pode usar uma ferramenta de infraestrutura como código (IaC), como CloudFormation a AWS, para substituir essas etapas por um modelo que cria uma pilha com os recursos e proprieda des apropriados.	

Tarefa	Descrição	Habilidades necessárias
Recupere detalhes como um dicionário do Amazon S3.	Use o código a seguir para ler do bucket do S3 e obter os valores JSON como um dicionário Python. `fileobj = s3_client .get_object( Bucket=bu cket_name, Key='my.json' ) filedata = fileobj[' Body'].read() contents = filedata. decode('utf-8') json_content=json. loads(contents) print(json_content )` onde `json_content` contém o dicionário Python.	Desenvolvedor de aplicativos, habilidades em Python

Tarefa	Descrição	Habilidades necessárias

Limpe os valores de dados para espaços e caracteres Unicode.	Como medida de segurança para garantir a exatidão dos dados, use o código a seguir para realizar uma operação de separação dos valores em `json_content` . Esse código remove os caracteres de espaço na frente e no final de cada string. Ele também usa o método `replace` para remover espaços rígidos (não quebráveis) (os caracteres `\xa0`).
	`for item in json_cont ent:`
	`fqn_name = unicodeda ta.normalize("NFKD ",item["FqdnName"] .replace("u'", "'").replace('\xa0', '').strip())`
	`rec_type = item["Rec ordType"].replace( '\xa0', '').strip()`
	`res_rec = {`
	`'Value': item["Val ue"].replace('\xa0', '').strip()`
	`}`
		Desenvolvedor de aplicativos, habilidades em Python

Tarefa	Descrição	Habilidades necessárias
Inserir registros.	Use o código a seguir como parte do loop `for` anterior. `change_response = route53_client.change_resource_record_sets( HostedZoneId="xxxxxxxx", ChangeBatch={ 'Comment': 'Created by automation', 'Changes': [ { 'Action': 'UPSERT', 'ResourceRecordSet': { 'Name': fqn_name, 'Type': rec_type, 'TTL': item["TTL"], 'ResourceRecords': res_rec } } ] } )`	Desenvolvedor de aplicativos, habilidades em Python

Tarefa	Descrição	Habilidades necessárias
	Onde xxxxxxx está o ID da zona hospedada desde a primeira etapa desse épico.	

Recursos relacionados

Referências

- Criação de registros importando um arquivo de zona (documentação do Amazon Route 53)
- método create_hosted_zone (documentação do Boto3)
- método change_resource_record_sets (documentação do Boto3)

Tutoriais e vídeos

- Tutorial do Python (documentação do Python)
- Design de DNS usando o Amazon Route 53 (YouTube vídeo, AWS Online Tech Talks)

Modifique os cabeçalhos HTTP ao migrar de F5 para um Application Load Balancer na AWS

Criado por Sachin Trivedi (AWS)

Resumo

Quando você migra um aplicativo que usa um balanceador de carga F5 para a Amazon Web Services (AWS) e deseja usar um Application Load Balancer na AWS, migrar regras F5 para modificações de cabeçalho é um problema comum. Um Application Load Balancer não suporta modificações de cabeçalhos, mas você pode usar a Amazon CloudFront como uma rede de distribuição de conteúdo (CDN) e o Lambda @Edge para modificar cabeçalhos.

Esse padrão descreve as integrações necessárias e fornece um exemplo de código para modificação do cabeçalho usando a AWS CloudFront e o Lambda @Edge.

Pré-requisitos e limitações

Pré-requisitos

- Um aplicativo on-premises que usa um balanceador de carga F5 com uma configuração que substitui o valor do cabeçalho HTTP usando `if, else`. Para obter mais informações sobre essa configuração, consulte HTTP::header na documentação do produto F5.

Limitações

- Esse padrão se aplica à personalização do cabeçalho do balanceador de carga F5. Para outros balanceadores de carga de terceiros, confira a documentação do balanceador de carga para obter informações de suporte.
- As funções do Lambda que você usa no Lambda@Edge devem estar na região Leste dos EUA (Norte da Virgínia).

Arquitetura

O diagrama a seguir mostra a arquitetura na AWS, incluindo o fluxo de integração entre a CDN e outros componentes da AWS.

Ferramentas

Serviços da AWS

- Application Load Balancer – Um Application Load Balancer é um serviço de balanceamento de carga totalmente gerenciado pela AWS que funciona na sétima camada do modelo Open Systems Interconnection (OSI). Ele equilibra o tráfego em vários destinos e oferece suporte a solicitações de roteamento avançado com base em cabeçalhos e métodos HTTP, strings de consulta e roteamento baseado em host ou em caminho.
- Amazon CloudFront — CloudFront A Amazon é um serviço web que acelera a distribuição de seu conteúdo web estático e dinâmico, como .html, .css, .js e arquivos de imagem, para seus usuários. CloudFront entrega seu conteúdo por meio de uma rede mundial de data centers chamados de pontos de presença para menor latência e melhor desempenho.
- O Lambda @Edge – Lambda @Edge é uma extensão do AWS Lambda que permite executar funções para personalizar o conteúdo que é entregue. CloudFront Você pode criar funções na região Leste dos EUA (Norte da Virgínia) e depois associar a função a uma CloudFront distribuição para replicar automaticamente seu código em todo o mundo, sem provisionar ou gerenciar servidores. Isso reduz a latência e melhora a experiência do usuário.

Código

O código de exemplo a seguir fornece um plano para modificar os cabeçalhos de CloudFront resposta. Siga as instruções na seção Épicos para implantar o código.

```
exports.handler = async (event, context) => {
    const response = event.Records[0].cf.response;
    const headers = response.headers;


    const headerNameSrc = 'content-security-policy';
    const headerNameValue = '*.xyz.com';


    if (headers[headerNameSrc.toLowerCase()]) {
        headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
        }];
        console.log(`Response header "${headerNameSrc}" was set to ` +
                    `"${headers[headerNameSrc.toLowerCase()][0].value}"`);
```

```
    }
    else {
            headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
            }];
    }
    return response;
};
```

Épicos

Criar uma distribuição CDN

Tarefa	Descrição	Habilidades necessárias
Crie uma distribuição CloudFront na web.	Nesta etapa, você cria uma CloudFront distribuição para informar de CloudFront onde deseja que o conteúdo seja entregue e os detalhes sobre como rastrear e gerenciar a entrega de conteúdo. Para criar uma distribui ção usando o console, faça login no AWS Management Console, abra o CloudFront console e siga as etapas na CloudFront documentação.	Administrador de nuvem

Criar e implantar as funções do Lambda@Edge

Tarefa	Descrição	Habilidades necessárias
Crie e implante uma função do Lambda@Edge.	Você pode criar uma função Lambda @Edge usando um esquema para modificar	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	CloudFront cabeçalhos de resposta. (Outros BluePrints estão disponíveis para diferentes casos de uso; para obter mais informações, consulte exemplos de funções do Lambda @Edge CloudFront na documentação.) Para criar uma função Lambda@Edge: 1. Faça login no AWS Management Console e abra o console do AWS Lambda em. https://console.aws.amazon.com/lambda/ 2. Verifique se você está na região Leste dos EUA (Norte da Virgínia). CloudFront As plantas estão disponíveis somente nesta região. 3. Escolha a opção Criar função. 4. Escolha Usar um esquema e, em seguida, insira cloudfront no campo de pesquisa Esquemas. 5. Escolha o cloudfront-modify-response-headerblueprint e, em seguida, escolha Configurar.	

Tarefa	Descrição	Habilidades necessárias
	6. Na página Informaçõ es básicas, forneça as seguintes informações: a. Insira um nome de função. b. Em Função de execução, selecione Criar uma nova função de modelos de política da AWS. c. Associe o nome do perfil do AWS Identity and Access Management (IAM). 7. Escolha a opção Criar função. 8. Na seção Designer da página, escolha o nome da sua função. 9. Na seção Código da função, substitua o código do modelo pelo código de amostra fornecido anteriorm ente nesse padrão, na seção Código. 10. No código de exemplo, substitua `xyz.com` pelo nome de seu domínio. 11. Escolha Salvar.	

Tarefa	Descrição	Habilidades necessárias
Implante a função do Lambda@Edge.	Siga as instruções na etapa 4 do tutorial: Criação de uma função simples do Lambda @Edge na CloudFront documentação da Amazon para configurar o CloudFront gatilho e implantar a função.	Administrador da AWS

Recursos relacionados

CloudFront documentação

- Comportamento de solicitações e respostas para origens personalizadas
- Trabalhar com distribuições
- Funções de exemplo do Lambda@Edge
- Personalizar o conteúdo na borda com o Lambda@Edge
- Tutorial: criação de uma função do Lambda@Edge simples

Acesse de forma privada um endpoint central de serviços da AWS a partir de vários VPCs

Criado por Martin Guenthner (AWS) e Samuel Gordon (AWS)

Resumo

Os requisitos de segurança e conformidade do seu ambiente podem especificar que o tráfego para os serviços ou endpoints da Amazon Web Services (AWS) não deve atravessar a Internet pública. Esse padrão é uma solução projetada para uma hub-and-spoketopologia, em que um hub central VPC é conectado a vários raios distribuídos. VPCs Nessa solução, você usa PrivateLink a AWS para criar uma interface VPC endpoint para o serviço da AWS na conta do hub. Em seguida, você usa gateways de trânsito e uma regra distribuída de Sistema de Nomes de Domínio (DNS) para resolver solicitações para o endereço IP privado do endpoint, entre os conectados. VPCs

Esse padrão descreve como usar o AWS Transit Gateway, um endpoint de entrada do Amazon Route 53 Resolver e uma regra de encaminhamento compartilhada do Route 53 para resolver as consultas de DNS dos recursos conectados. VPCs Você cria o endpoint, o gateway de trânsito, o resolvedor e a regra de encaminhamento na conta do hub. Em seguida, você usa o AWS Resource Access Manager (AWS RAM) para compartilhar o gateway de trânsito e a regra de encaminhamento com o spoke VPCs. Os CloudFormation modelos da AWS fornecidos ajudam você a implantar e configurar os recursos no hub VPC e spoke. VPCs

Pré-requisitos e limitações

Pré-requisitos

- Uma conta do hub e uma ou mais contas spoke, gerenciadas na mesma organização no AWS Organizations. Para obter mais informações, consulte Criação e gerenciamento de uma organização .
- O AWS Resource Access Manager (AWS RAM) é configurado como um serviço confiável no AWS Organizations. Para obter mais informações, consulte Usando o AWS Organizations com outros serviços da AWS.
- A resolução de DNS deve estar habilitada no hub and spoke VPCs. Para ter mais informações, consulte Atributos de DNS para sua VPC (documentação da Amazon Virtual Private Cloud).

Limitações

- Esse padrão conecta contas hub e spoke na mesma região da AWS. Para implantações em várias regiões, você deve repetir esse padrão para cada região.
- O serviço da AWS deve ser integrado PrivateLink como uma interface de VPC endpoint. Para obter uma lista completa, consulte os serviços da AWS que se integram à AWS PrivateLink (PrivateLink documentação).
- A afinidade com a zona de disponibilidade não é garantida. Por exemplo, consultas da Zona de Disponibilidade A podem responder com um endereço IP da Zona de Disponibilidade B.
- A interface de rede elástica associada ao VPC endpoint tem um limite de 10.000 consultas por segundo.

Arquitetura

Pilha de tecnologias de destino

- Um hub VPC na conta hub da AWS
- Um ou mais falaram VPCs em uma conta da AWS
- Um ou mais endpoints VPC de interface na conta do hub
- Resolvedores Route 53 de entrada e saída na conta do hub
- Uma regra de encaminhamento do Route 53 Resolver implantada na conta do hub e compartilhada com a conta spoke
- Um gateway de trânsito implantado na conta do hub e compartilhado com a conta spoke
- AWS Transit Gateway conectando o hub e o spoke VPCs

Arquitetura de destino

A imagem a seguir mostra um exemplo de arquitetura para essa solução. Nessa arquitetura, a regra de encaminhamento do Route 53 Resolver na conta do hub tem a seguinte relação com os outros componentes da arquitetura:

1. A regra de encaminhamento é compartilhada com a VPC spoke usando a AWS RAM.
2. A regra de encaminhamento está associada ao resolvedor de saída na VPC do hub.
3. A regra de encaminhamento tem como destino o resolvedor de entrada na VPC do hub.

A imagem a seguir mostra o fluxo de tráfego por meio da arquitetura de exemplo:

1. Um recurso, como uma instância do Amazon Elastic Compute Cloud (Amazon EC2), no spoke VPC, faz uma solicitação de DNS para. `<service>.<region>.amazonaws.com` A solicitação é recebida pelo Amazon DNS Resolver.
2. A regra de encaminhamento do Route 53, que é compartilhada da conta do hub e associada à VPC spoke, intercepta a solicitação.
3. Na VPC do hub, o resolvedor de saída usa a regra de encaminhamento para encaminhar a solicitação para o resolvedor de entrada.
4. O Resolvedor de entrada usa o hub VPC Amazon DNS Resolver para resolver o endereço IP `<service>.<region>.amazonaws.com` para o endereço IP privado de um endpoint da VPC. Se nenhum endpoint da VPC estiver presente, ele será resolvido para o endereço IP público.

Ferramentas

Ferramentas e serviços da AWS

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Resource Access Manager (AWS RAM) ajuda a compartilhar com segurança seus recursos entre contas da para reduzir a sobrecarga operacional e fornecer visibilidade e auditabilidade.
- O Amazon Route 53 é um serviço da web do Sistema de Nomes de Domínio (DNS) altamente disponível e dimensionável.
- O AWS Systems Manager ajuda você a gerenciar seus aplicativos e infraestrutura em execução na nuvem AWS. Isso simplifica o gerenciamento de aplicações e recursos, diminui o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus recursos da AWS de modo seguro e em grande escala.
- O AWS Transit Gateway é um hub central que conecta VPCs redes locais.

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas e serviços

- nslookup é uma ferramenta de linha de comando usada para consultar registros DNS. Nesse padrão, você usa essa ferramenta para testar a solução.

Repositório de código

O código desse padrão está disponível em GitHub, no vpc-endpoint-sharingrepositório. Esse padrão fornece dois CloudFormation modelos da AWS:

- Um modelo para implantar os seguintes recursos na conta do hub:
  - `rSecurityGroupEndpoints`: o grupo de segurança que controla o acesso ao endpoint da VPC.
  - `rSecurityGroupResolvers`: o grupo de segurança que controla o acesso ao Resolver do Route 53.
  - `rKMSEndpoint`, `rSSMMessagesEndpoint`, `rSSMEndpoint`, e `rEC2MessagesEndpoint` – Exemplo de endpoints VPC de interface na conta do hub. Personalize esses endpoints para o seu caso de uso.
  - `rInboundResolver`: um Route 53 Resolver que resolve consultas de DNS no hub Amazon DNS Resolver.
  - `rOutboundResolver`: um resolvedor de saída do Route 53 que encaminha as consultas para o Resolvedor de entrada.
  - `rAWSApiResolverRule`— A regra de encaminhamento do Route 53 Resolver que é compartilhada com todos os VPCs falados.
  - `rRamShareAWSResolverRule`— O compartilhamento de RAM da AWS que permite que o spoke use VPCs a regra `rAWSApiResolverRule` de encaminhamento.
  - * `rVPC`: o hub VPC, usado para modelar os serviços compartilhados.
  - * `rSubnet1`: uma sub-rede privada usada para hospedar os recursos do hub.
  - * `rRouteTable1`: a tabela de rotas para o hub VPC.
  - * `rRouteTableAssociation1`: para a tabela de rotas `rRouteTable1` no hub VPC, a associação para a sub-rede privada.

  - * `rRouteSpoke`: a rota do hub VPC para a VPC spoke.
  - * `rTgw` — O gateway de trânsito que é compartilhado com todos os falantes VPCs.
  - * `rTgwAttach`: o anexo que permite ao hub VPC rotear o tráfego para o gateway de trânsito `rTgw`.
  - * `rTgwShare`: o compartilhamento de RAM da AWS que permite que as contas spoke usem o gateway de trânsito `rTgw`.
- Um modelo para implantar os seguintes recursos nas contas spoke:
  - `rAWSApiResolverRuleAssociation`: uma associação que permite que a VPC spoke use a regra de encaminhamento compartilhado na conta do hub.
  - * `rVPC`: o VPC spoke.
  - * `rSubnet1, rSubnet2, rSubnet3`: uma sub-rede para cada zona de disponibilidade, usada para abrigar os recursos privados do spoke.
  - * `rTgwAttach`: o anexo que permite que a VPC spoke roteie o tráfego para o gateway de trânsito `rTgw`.
  - * `rRouteTable1`: a tabela de rotas para a VPC spoke.
  - * `rRouteEndpoints`: a rota dos recursos na VPC spoke até o gateway de trânsito.
  - * `rRouteTableAssociation1/2/3`: para a tabela de rotas `rRouteTable1` na VPC spoke, as associações para as sub-redes privadas.
  - * `rInstanceRole`: o perfil do IAM usada para testar a solução.
  - * `rInstancePolicy`: a política do IAM usada para testar a solução.
  - * `rInstanceSg`: o grupo de segurança usado para testar a solução.
  - * `rInstanceProfile`: o perfil de instância do IAM usado para testar a solução.
  - * `rInstance` — Uma EC2 instância pré-configurada para acesso por meio do AWS Systems Manager. Use essa instância para testar a solução.

* Esses recursos oferecem suporte à arquitetura de amostra e podem não ser necessários ao implementar esse padrão em uma zona de pouso existente.

Épicos

Prepare os CloudFormation modelos

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de códigos.	1. Em uma interface da linha de comando, altere seu diretório de trabalho para o local em que você deseja armazenar os arquivos de amostra. 2. Digite o comando: `git clone https://github.com/aws-samples/vpc-endpoint-sharing.git`	Administrador de rede, arquiteto de nuvem
Modifique os modelos.	1. No repositório clonado, abra os arquivos hub.yml e spoke.yml. 2. Analise os recursos criados por esses modelos e ajuste-os conforme necessário para seu ambiente. Para obter uma lista completa, consulte a seção Repositório de códigos em Ferramentas. Se suas contas já tiverem alguns desses recursos, remova-os do CloudFormation modelo. Para obter mais informações, consulte Trabalhando com modelos (CloudFormation documentação).	Administrador de rede, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	3. Salve e feche os arquivos hub.yml e spoke.yml.	

Implante os recursos nas contas de destino

Tarefa	Descrição	Habilidades necessárias
Implante os recursos do hub.	Usando o modelo hub.yml, crie uma pilha. CloudFormation Quando solicitado, apresente os valores para os parâmetros do modelo. Para obter mais informações, consulte Criação de uma pilha (CloudFormation documentação).	Arquiteto de nuvem, administrador de rede
Implante os recursos do spoke.	Usando o modelo spoke.yml, crie uma pilha. CloudFormation Quando solicitado, apresente os valores para os parâmetros do modelo. Para obter mais informações, consulte Criação de uma pilha (CloudFormation documentação).	Arquiteto de nuvem, administrador de rede

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Teste consultas privadas de DNS para o serviço da AWS.	1. Conecte-se à `rInstance` EC2 instância usando o Session Manager, um	Administrador de rede

Tarefa	Descrição	Habilidades necessárias
	recurso do AWS Systems Manager. Para obter mais informações, consulte Conecte-se à sua instância Linux usando o Session Manager (EC2 documentação da Amazon). 2. Para um serviço da AWS que tenha um endpoint da VPC na conta do hub, use `nslookup` para confirmar se os endereços IP privados do Resolvedor do Route 53 de entrada foram retornados. A seguir temos um exemplo de uso `nslookup` para alcançar um endpoint do Amazon Systems Manager. `nslookup ssm.<region>.amazonaws.com` 3. Na AWS Command Line Interface (AWS CLI), insira um comando que pode ajudar você a confirmar que as alterações não afetaram a funcionalidade do serviço. Para obter uma lista de comandos, consulte Referência de comandos da AWS CLI.	

Tarefa	Descrição	Habilidades necessárias
	Por exemplo, o comando a seguir deve retornar uma lista de documentos do Amazon Systems Manager. `aws ssm list-documents`	

Tarefa	Descrição	Habilidades necessárias

Teste consultas públicas de DNS em um serviço da AWS.	1. Para um serviço da AWS que não tenha um endpoint da VPC na conta do hub, use `nslookup` para confirmar se os endereços IP públicos foram retornados. A seguir temos um exemplo de uso `nslookup` para acessar um endpoint do Amazon Simple Notification Service (Amazon SNS).
	`nslookup sns.<region>.amazonaws.com`
	2. Na AWS CLI, insira um comando que pode ajudá-lo a confirmar que as alterações não afetaram a funcionalidade do serviço. Para obter uma lista de comandos, consulte Referência de comandos da AWS CLI.
	Por exemplo, se algum tópico do Amazon SNS estiver presente na conta do hub, o comando a seguir deverá retornar uma lista de tópicos.
	`aws sns list-topics`
		Administrador de rede

Recursos relacionados

- Criar uma infraestrutura de rede AWS dimensionável e segura de várias VPCs (AWS whitepaper)
- Trabalhando com recursos compartilhados (documentação da AWS RAM)
- Trabalho com gateways de trânsito (documentação do AWS Transit Gateway)

Crie um relatório das descobertas do Network Access Analyzer para acesso de entrada à Internet em vários Contas da AWS

Criado por Mike Virgilio (AWS)

Resumo

O acesso não intencional de entrada aos AWS recursos pela Internet pode representar riscos para o perímetro de dados de uma organização. O Network Access Analyzer é um recurso da Amazon Virtual Private Cloud (Amazon VPC) que ajuda você a identificar o acesso não intencional à rede aos seus recursos na Amazon Web Services ().AWS Você pode usar o Analisador de Acesso à Rede para especificar seus requisitos de acesso à rede e identificar possíveis caminhos de rede que não atendam aos requisitos especificados. Você pode usar o Analisador de Acesso à Rede para fazer o seguinte:

1. Identifique AWS recursos acessíveis à Internet por meio de gateways da Internet.
2. Valide se suas nuvens privadas virtuais (VPCs) estão segmentadas adequadamente, como isolar ambientes de produção e desenvolvimento e separar cargas de trabalho transacionais.

O Network Access Analyzer analisa as condições de acessibilidade end-to-end da rede e não apenas um único componente. Para determinar se um recurso é acessível pela Internet, o Network Access Analyzer avalia o gateway da Internet, as tabelas de rotas da VPC, as listas de controle de acesso à rede (ACLs), os endereços IP públicos em interfaces de rede elásticas e os grupos de segurança. Se algum desses componentes impedir o acesso à Internet, o Analisador de Acesso à Rede não gerará uma descoberta. Por exemplo, se uma instância do Amazon Elastic Compute Cloud (Amazon EC2) tiver um grupo de segurança aberto que permite o tráfego, `0/0` mas a instância está em uma sub-rede privada que não é roteável de nenhum gateway da Internet, o Network Access Analyzer não geraria uma descoberta. Isso fornece resultados de alta fidelidade para que você possa identificar recursos que são realmente acessíveis pela Internet.

Ao executar o Analisador de Acesso à Rede, você usa os Network Access Scopes para especificar seus requisitos de acesso à rede. Essa solução identifica caminhos de rede entre um gateway da Internet e uma interface de rede elástica. Nesse padrão, você implanta a solução de forma centralizada Conta da AWS em sua organização, gerenciada por AWS Organizations, e ela analisa todas as contas, em qualquer uma Região da AWS, na organização.

Essa solução foi projetada com o seguinte em mente:

- Os AWS CloudFormation modelos reduzem o esforço necessário para implantar os AWS recursos nesse padrão.
- Você pode ajustar os parâmetros nos CloudFormation modelos e no script naa-script.sh no momento da implantação para personalizá-los para seu ambiente.
- O script Bash provisiona e analisa automaticamente os escopos de acesso à rede para várias contas, em paralelo.
- Um script Python processa as descobertas, extrai os dados e consolida os resultados. Você pode optar por revisar o relatório consolidado das descobertas do Network Access Analyzer no formato CSV ou em. AWS Security Hub Um exemplo do relatório CSV está disponível na seção Informações adicionais desse padrão.
- Você pode corrigir as descobertas ou excluí-las de futuras análises adicionando-as ao arquivo naa-exclusions.csv.

Pré-requisitos e limitações

Pré-requisitos

- E Conta da AWS para hospedar serviços e ferramentas de segurança, gerenciados como uma conta membro de uma organização em AWS Organizations. Nesse padrão, essa conta é chamada de conta de segurança.
- Na conta de segurança, você deve ter uma sub-rede privada com acesso de saída à Internet. Para obter instruções, consulte Criar uma sub-rede na documentação da Amazon VPC. Você pode estabelecer acesso à Internet usando um gateway NAT ou um endpoint da VPC de interface.
- Acesso à conta AWS Organizations de gerenciamento ou a uma conta que tenha delegado permissões de administrador para CloudFormation. Para obter instruções, consulte Registrar um administrador delegado na CloudFormation documentação.
- Habilite o acesso confiável entre AWS Organizations CloudFormation e. Para obter instruções, consulte Habilitar acesso confiável AWS Organizations na CloudFormation documentação.
- Se você estiver fazendo o upload das descobertas para o Security Hub, o Security Hub deve estar habilitado na conta e Região da AWS onde a EC2 instância da Amazon está provisionada. Para obter mais informações, consulte Configurar AWS Security Hub.

Limitações

- Atualmente, os caminhos de rede entre contas não são analisados devido às limitações do atributo Analisador de Acesso à Rede.
- O alvo Contas da AWS deve ser gerenciado como uma organização em AWS Organizations. Se você não estiver usando AWS Organizations, você pode atualizar o CloudFormation modelo naa-execrole.yaml e o script naa-script.sh para seu ambiente. Em vez disso, você fornece uma lista Conta da AWS IDs e regiões nas quais deseja executar o script.
- O CloudFormation modelo foi projetado para implantar a EC2 instância da Amazon em uma sub-rede privada com acesso de saída à Internet. O AWS Systems Manager Agente (Agente SSM) requer acesso de saída para alcançar o endpoint do serviço Systems Manager, e você precisa de acesso de saída para clonar o repositório de código e instalar dependências. Se quiser usar uma sub-rede pública, você deve modificar o modelo naa-resources.yaml para associar um endereço IP elástico à instância da Amazon. EC2

Arquitetura

Arquitetura de destino

Opção 1: acessar as descobertas em um bucket do Amazon S3

O diagrama mostra o seguinte processo:

1. Se você estiver executando manualmente a solução, o usuário se autentica na EC2 instância da Amazon usando o Gerenciador de Sessões e, em seguida, executa o script naa-script.sh. Esse script de shell executa as etapas de 2 a 7.

   Se você estiver executando a solução automaticamente, o script naa-script.sh será iniciado automaticamente na programação que você definiu na expressão cron. Esse script de shell executa as etapas de 2 a 7. Para obter mais informações, consulte Automação e escala no fim desta seção.
2. A EC2 instância da Amazon baixa o arquivo naa-exception.csv mais recente do bucket do Amazon S3. Esse arquivo é usado posteriormente no processo, quando o script Python processa as exclusões.
3. A EC2 instância da Amazon assume a função `NAAEC2Role` AWS Identity and Access Management (IAM), que concede permissões para acessar o bucket do Amazon S3 e assumir `NAAExecRole` as funções do IAM nas outras contas da organização.

4. A EC2 instância da Amazon assume a função `NAAExecRole` do IAM na conta de gerenciamento da organização e gera uma lista das contas na organização.
5. A EC2 instância da Amazon assume a função do `NAAExecRole` IAM nas contas dos membros da organização (chamadas de contas de carga de trabalho no diagrama de arquitetura) e realiza uma avaliação de segurança em cada conta. As descobertas são armazenadas como arquivos JSON na EC2 instância da Amazon.
6. A EC2 instância da Amazon usa um script Python para processar os arquivos JSON, extrair os campos de dados e criar um relatório CSV.
7. A EC2 instância da Amazon carrega o arquivo CSV no bucket do Amazon S3.
8. Uma EventBridge regra da Amazon detecta o upload do arquivo e usa um tópico do Amazon SNS para enviar um e-mail notificando o usuário de que o relatório foi concluído.
9. O usuário baixa o arquivo CSV do bucket do Amazon S3. O usuário importa os resultados para o modelo do Excel e revisa os resultados.

Opção 2: Acesse os resultados em AWS Security Hub

O diagrama mostra o seguinte processo:

1. Se você estiver executando manualmente a solução, o usuário se autentica na EC2 instância da Amazon usando o Gerenciador de Sessões e, em seguida, executa o script naa-script.sh. Esse script de shell executa as etapas de 2 a 7.

   Se você estiver executando a solução automaticamente, o script naa-script.sh será iniciado automaticamente na programação que você definiu na expressão cron. Esse script de shell executa as etapas de 2 a 7. Para obter mais informações, consulte Automação e escala no fim desta seção.
2. A EC2 instância da Amazon baixa o arquivo naa-exception.csv mais recente do bucket do Amazon S3. Esse arquivo é usado posteriormente no processo, quando o script Python processa as exclusões.
3. A EC2 instância da Amazon assume a função `NAAEC2Role` do IAM, que concede permissões para acessar o bucket do Amazon S3 e assumir `NAAExecRole` as funções do IAM nas outras contas da organização.
4. A EC2 instância da Amazon assume a função `NAAExecRole` do IAM na conta de gerenciamento da organização e gera uma lista das contas na organização.

5. A EC2 instância da Amazon assume a função do `NAAExecRole` IAM nas contas dos membros da organização (chamadas de contas de carga de trabalho no diagrama de arquitetura) e realiza uma avaliação de segurança em cada conta. As descobertas são armazenadas como arquivos JSON na EC2 instância da Amazon.
6. A EC2 instância da Amazon usa um script Python para processar os arquivos JSON e extrair os campos de dados para importação no Security Hub.
7. A EC2 instância da Amazon importa as descobertas do Network Access Analyzer para o Security Hub.
8. Uma EventBridge regra da Amazon detecta a importação e usa um tópico do Amazon SNS para enviar um e-mail notificando o usuário de que o processo foi concluído.
9. O usuário visualiza as descobertas no Security Hub.

Automação e escala

Você pode programar essa solução para executar o script naa-script.sh automaticamente em um agendamento personalizado. Para definir um agendamento personalizado, no modelo naa-resources.yaml CloudFormation , modifique o parâmetro. `CronScheduleExpression` Por exemplo, o valor padrão de `0 0 * * 0` executa a solução à meia-noite de todos os domingos. Um valor de `0 0 * 1-12 0` executaria a solução à meia-noite do primeiro domingo de cada mês. Para obter mais informações sobre o uso de expressões cron, consulte Cron e expressões rate na documentação do Systems Manager.

Se quiser ajustar a programação após a implantação da pilha `NAA-Resources`, você pode editar manualmente a programação cron em `/etc/cron.d/naa-schedule`.

Ferramentas

Serviços da AWS

- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS

- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS. Também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala. Esse padrão usa o Session Manager, um atributo do Systems Manager.

Repositório de código

O código desse padrão está disponível no repositório de análise de várias contas do GitHub Network Access Analyzer. O repositório de código contém os seguintes arquivos:

- naa-script.sh — Esse script bash é usado para iniciar uma análise de vários dados do Network Access Analyzer Contas da AWS, em paralelo. Conforme definido no CloudFormation modelo naa-resources.yaml, esse script é implantado automaticamente na pasta na instância da Amazon. `/usr/local/naa` EC2
- naa-resources.yaml — Você usa esse CloudFormation modelo para criar uma pilha na conta de segurança na organização. Esse modelo implanta todos os recursos necessários para essa conta a fim de oferecer suporte à solução. Essa pilha deve ser implantada antes do modelo naa-execrole.yaml.

> **Note**
>
> Se essa pilha for excluída e reimplantada, você deverá reconstruir o conjunto de `NAAExecRole` pilhas para reconstruir as dependências entre contas entre as funções do IAM.

- naa-execrole.yaml — Você usa esse CloudFormation modelo para criar um conjunto de pilhas que implanta a função `NAAExecRole` do IAM em todas as contas da organização, incluindo a conta de gerenciamento.
- naa-processfindings.py: o script naa-script.sh chama automaticamente esse script Python para processar as saídas JSON do Analisador de Acesso à Rede, excluir quaisquer recursos em boas condições no arquivo naa-exclusions.csv e, em seguida, gerar um arquivo CSV dos resultados consolidados ou importar os resultados para o Security Hub.

Épicos

Preparar-se para implantação

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de códigos.	1. Em uma interface da linha de comando, altere seu diretório de trabalho para o local em que você deseja armazenar os arquivos de amostra. 2. Digite o comando: `git clone https://github.com/aws-samples/network-access-analyzer-multi-account-analysis.git`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Consulte os modelos.	1. No repositório clonado, abra os arquivos naa-resources.yaml e naa-execrole.yaml. 2. Analise os recursos criados por esses modelos e ajuste-os conforme necessário para seu ambiente. Para obter mais informações, consulte Trabalhando com modelos na CloudFormation documentação. 3. Salve e feche os arquivos naa-resources.yaml e naa-execrole.yaml.	AWS DevOps

Crie as CloudFormation pilhas

Tarefa	Descrição	Habilidades necessárias
Provisione recursos na conta de segurança.	Usando o modelo naa-resources.yaml, você cria uma CloudFormation pilha que implanta todos os recursos necessários na conta de segurança. Para obter instruções, consulte Criação de uma pilha na CloudFormation documentação. Observe o seguinte ao implantar esse modelo: 1. Na página Especificar modelo, escolha O modelo	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	está pronto e, em seguida, carregue o arquivo naa-resources.yaml. 2. Na página Specify stack details (Especificar detalhes da pilha), na caixa Stack name (Nome da pilha), insira `NAA-Resources` . 3. Na seção Parameters (Parâmetros), insira o seguinte: • `VPCId`: selecione uma VPC na conta. • `SubnetId`: selecione uma sub-rede privada que tenha acesso à Internet. **Note** Se você selecionar uma sub-rede pública, talvez a EC2 instância da Amazon não receba um endereço IP público porque o CloudFormation modelo, por padrão, não provisiona e anexa um	

Tarefa	Descrição	Habilidades necessárias
	endereço IP elástico. • `InstanceType` : deixe o tipo de instância padrão. • `InstanceImageId` : mantenha o padrão. • `KeyPairName` : se você estiver usando SSH para acessar, especifique o nome de um par de chaves existente. • `PermittedSSHInbound` : se você estiver usando SSH para acesso, especifique um bloco CIDR permitido. Se você não estiver usando SSH, mantenha o valor padrão de `127.0.0.1` . • `BucketName` : o valor padrão é `naa-<accountID>-<region>` . Você pode modificar isso conforme necessário. Se você especificar um valor personalizado, a ID da conta e a região serão automaticamente anexados ao valor especificado. • `EmailAddress` : especifique um endereço	

Tarefa	Descrição	Habilidades necessárias
	de e-mail para uma notificação do Amazon SNS quando a análise for concluída. **Note** A configuração da assinatura do Amazon SNS deve ser confirmada antes da conclusão da análise, ou uma notificação não será enviada. • `NAAEC2Role` : mantenha o padrão, a menos que suas convenções de nomenclatura exijam um nome diferente para esse perfil do IAM. • `NAAExecRole` : mantenha o padrão, a menos que outro nome seja usado ao implantar o naa-execrole.yaml • `Parallelism` : especifique o número de avaliações paralelas a serem realizadas.	

Tarefa	Descrição	Habilidades necessárias
	• `Regions`— Especifique o que Regiões da AWS você deseja analisar. • `ScopeNameValue` : especifique a tag que será atribuída ao escopo. Essa tag é usada para determinar o escopo de acesso à rede. • `ExclusionFile` : especifique o nome do arquivo de exclusão. As entradas nesse arquivo serão excluídas das descobertas. • `FindingsToCSV` : especifique se as descobertas devem ser enviadas para CSV. Os valores aceitos são `true` e `false`. • `FindingsToSecurityHub` : especifique se as descobertas devem ser importadas para o Security Hub. Os valores aceitos são `true` e `false`. • `EmailNotificationsForSecurityHub` : especifique se a importação de descobertas para o Security Hub	

Tarefa	Descrição	Habilidades necessárias
	deve gerar notificações por e-mail. Os valores aceitos são `true` e `false`. • `ScheduledAnalysis` : se você quiser que a solução seja executada automaticamente em um agendamento, insira `true` e personalize o agendamento no parâmetro `CronSchedule Expression` . Se você não deseja executar a solução automatic amente, insira `false`. • `CronScheduleExpression` : se você estiver executando a solução automaticamente, insira uma expressão cron para definir o cronograma. Para obter mais informações, consulte Automação e escala na seção Arquitetura desse padrão. 1. Na página Revisar, selecione Os seguintes recursos exigem recursos: [AWS::IAM::Role] e escolha Criar pilha.	

Tarefa	Descrição	Habilidades necessárias
	2. Depois que a pilha for criada com sucesso, no CloudFormation console, na guia Saídas, copie o `NAAEC2Role` Amazon Resource Name (ARN). Você usa esse ARN posteriormente ao implantar o arquivo naa-execr ole.yaml.	

Tarefa	Descrição	Habilidades necessárias
Provisione o perfil do IAM nas contas dos membros.	Na conta AWS Organizations de gerenciamento ou em uma conta com permissões de administrador delegado para CloudFormation, use o modelo naa-execrole.yaml para criar um conjunto de pilhas. CloudFormation O conjunto de pilhas implanta o perfil `NAAExecRole` do IAM para todas as contas-membro da organização. Para obter instruções, consulte Criar um conjunto de pilhas com permissões gerenciadas pelo serviço na documentação. CloudFormation Observe o seguinte ao implantar esse modelo: 1. Em Preparar modelo, escolha O modelo está pronto e, em seguida, carregue o arquivo naa-execrole.yaml. 2. Na página Especificar StackSet detalhes, nomeie o conjunto `NAA-ExecRole` de pilhas. 3. Na seção Parameters (Parâmetros), insira o seguinte: • `AuthorizedARN` : insira o ARN `NAAEC2Rol`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	e , que você copiou ao criar a pilha NAA-Resources . • NAARoleName : mantenha o valor padrão de NAAExecRole , a menos que outro nome tenha sido usado ao implantar o arquivo naa-resources.yaml. 4. Em Permissions (Permissões), escolha Service-managed permissions (Permissões gerenciadas pelo serviço). 5. Na página Set deployment options (Definir opções de implantação) em Deployment targets (Destinos da implantação), escolha Deploy to organization (Implantar na organização) e aceite todos os padrões. **Note** Se você quiser que as pilhas sejam implantadas em todas as contas dos membros simultaneamente, defina Máximo de contas simultâneas e	

Tarefa	Descrição	Habilidades necessárias
	Tolerância a falhas como um valor alto, como. `100` 6. Em Regiões de implantação, escolha a região em que a EC2 instância da Amazon para o Network Access Analyzer está implantada. Como os recursos do IAM são globais e não regionais, isso implanta o perfil do IAM em todas as regiões ativas. 7. Na página de revisão, selecione Eu reconheço que AWS CloudFormation posso criar recursos do IAM com nomes personalizados e, em seguida, escolha Criar StackSet. 8. Monitore a guia Instâncias de pilha (para o status da conta individual) e a guia Operações (para o status geral) para determinar quando a implantação será concluída.	

Tarefa	Descrição	Habilidades necessárias
Provisione o perfil do IAM na conta de gerenciamento.	Usando o modelo naa-execrole.yaml, você cria uma CloudFormation pilha que implanta a função do `NAAExecRole` IAM na conta de gerenciamento da organização. O conjunto de pilhas que você criou anteriormente não implanta o perfil do IAM na conta de gerenciamento. Para obter instruções, consulte Criação de uma pilha na CloudFormation documentação. Observe o seguinte ao implantar esse modelo: 1. Na página Especificar modelo, escolha O modelo está pronto e, em seguida, carregue o arquivo naa-execrole.yaml. 2. Na página Specify stack details (Especificar detalhes da pilha), na caixa Stack name (Nome da pilha), insira `NAA-ExecRole` . 3. Na seção Parameters (Parâmetros), insira o seguinte: • `AuthorizedARN` : insira o ARN `NAAEC2Role` , que você copiou ao	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	criar a pilha `NAA-Resources` . • `NAARoleName` : mantenha o valor padrão de `NAAExecRole` , a menos que outro nome tenha sido usado ao implantar o arquivo naa-resources.yaml. 4. Na página Revisar, selecione Os seguintes recursos exigem recursos: [AWS::IAM::Role] e escolha Criar pilha.	

Realizar a análise

Tarefa	Descrição	Habilidades necessárias
Personalize o script de shell.	1. Faça login na conta de segurança na organização. 2. Usando o Session Manager, conecte-se à EC2 instância da Amazon para o Network Access Analyzer que você provision ou anteriormente. Para obter instruções, consulte Conectar-se à instância do Linux usando o Session Manager. Se você não conseguir se conectar, consulte a seção Solução	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	de problemas desse padrão.
	3. Digite os seguintes comandos para abrir o arquivo naa-script.sh para edição:
	`sudo -i`
	`cd /usr/local/naa`
	`vi naa-script.sh`
	4. Revise e modifique os parâmetros e variáveis ajustáveis neste script conforme necessário para seu ambiente. Para obter mais informações sobre as opções de personalização, consulte os comentários no início do script.
	Por exemplo, em vez de obter uma lista de todas as contas dos membros da organização a partir da conta de gerenciamento, você pode modificar o script para especificar Conta da AWS IDs ou Regiões da AWS que deseja verificar , ou pode referenciar um arquivo externo que contenha esses parâmetro s.	

Tarefa	Descrição	Habilidades necessárias
	5. Salve e feche o arquivo naa-script.sh.	

Tarefa	Descrição	Habilidades necessárias

Analise as contas de destino.	1. Insira os comandos a seguir: Isso executa o script naa-script.sh:
	`sudo -i`
	`cd /usr/local/naa`
	`screen`
	`./naa-script.sh`
	Observe o seguinte:
	• O comando `screen` permite que o script continue em execução caso a conexão expire ou você perca o acesso ao console.
	• Após o início da digitaliz ação, você pode forçar a separação da tela pressionando Ctrl+A D. A tela se separa e você pode fechar a conexão da instância enquanto a análise prossegue.
	• Para retomar uma sessão desanexada, conecte-se à instância, insira `sudo -i` e depois `screen -r`.
	2. Monitore a saída em busca de erros para garantir que o script esteja funcionan do corretamente. Para obter um exemplo de saída,
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	consulte a seção Informações adicionais desse padrão. 3. Aguarde a conclusão da análise. Se você configurou notificações por e-mail, receberá um e-mail quando os resultados forem carregados no bucket do Amazon S3 ou importados para o Security Hub.	
Opção 1 — Recupere os resultados do bucket do Amazon S3.	1. Faça download do arquivo CSV do bucket `naa-<accountID>-<region>` . Para obter instruções, consulte Baixar um objeto na documentação do Amazon S3. 2. Exclua o arquivo CSV do bucket do Amazon S3. Essa é a melhor prática para otimização de custos. Para obter instruções, consulte Excluir objetos na documentação do Amazon S3.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Opção 2 – Analise os resultados no Security Hub.	1. Abra o console do Security Hub. 2. No painel de navegação, selecione Descobertas. 3. Analise as descobertas do Analisador de Acesso à Rede. Para obter instruções, consulte Visualização de listas de descobertas e detalhes na documentação do Security Hub. **Note** Você pode pesquisar descobertas adicionando um título que começa com o filtro e inserindo `Network Access Analyzer`.	AWS DevOps

Corrija e exclua as descobertas

Tarefa	Descrição	Habilidades necessárias
Corrija as descobertas.	Corrija as descobertas que você deseja abordar. Para obter mais informações e melhores práticas sobre como criar um perímetro em torno de suas AWS identidades,	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	recursos e redes, consulte Construindo um perímetro de dados em AWS (AWS Whitepaper).	

Tarefa	Descrição	Habilidades necessárias
Exclua recursos com caminhos de rede em boas condições.	Se o Analisador de Acesso à Rede gerar descobertas para recursos que devem ser acessíveis pela Internet, você poderá adicionar esses recursos a uma lista de exclusão. Na próxima vez que o Analisador de Acesso à Rede for executado, ele não gerará uma descoberta para esse recurso. 1. Navegue até `/usr/local/naa` e então abra o script naa-script.sh. Anote o valor da variável `S3_EXCLUSION_FILE` . 2. Se o valor da variável `S3_EXCLUSION_FILE` for `true`, baixe o arquivo naa-exclusions.csv do bucket `naa-<accountID>-<region>` . Para obter instruções, consulte Baixar um objeto na documentação do Amazon S3. Se o valor da variável `S3_EXCLUSION_FILE` for `false`, navegue até `/usr/local/naa` e abra o arquivo naa-exclusions.csv.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Note Se o valor da `S3_EXCLUSION_FILE` variável for `false`, o script usará uma versão local do arquivo de exclusões. Se você alterar posteriormente o valor para `true`, o script substituirá a versão local pelo arquivo no bucket do Amazon S3. 3. No arquivo naa-exclusions.csv, insira os recursos que você deseja excluir. Insira um recurso em cada linha e use o formato a seguir. `<resource_id>,<secgroup_id>,<sgrule_cidr>,<sgrule_portrange>,<sgrule_protocol>` A seguir, uma exemplo de recurso.	

Tarefa	Descrição	Habilidades necessárias
	`eni-1111aaaaa2222bbbb,sg-3333ccccc4444dddd,0.0.0.0/0,80 to 80,tcp` 4. Salve e feche o arquivo naa-exclusions.csv. 5. Se você baixou o arquivo naa-exclusions.csv do bucket do Amazon S3, faça o upload da nova versão. Para obter instruções, consulte Fazer uploads de objetos na documentação do Amazon S3.	

(Opcional) Atualize o script naa-script.sh

Tarefa	Descrição	Habilidades necessárias
Atualize o script naa-script.sh.	Se você quiser atualizar o script naa-script.sh para a versão mais recente no repositório, faça o seguinte: 1. Conecte-se à EC2 instância da Amazon usando o Gerenciador de Sessões. Para obter instruções, consulte Conectar-se à instância do Linux usando o Session Manager 2. Digite o comando:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`sudo -i`
	3. Navegue até o diretório do script naa-script.sh:
	`cd /usr/local/naa`
	4. Digite o comando a seguir para armazenar o script local para que você possa mesclar as alterações personalizadas na versão mais recente:
	`git stash`
	5. Digite o comando a seguir para obter a versão mais recente do script:
	`git pull`
	6. Digite o comando a seguir para mesclar o script personalizado com a versão mais recente do script:
	`git stash pop`	

Limpar (opcional)

Tarefa	Descrição	Habilidades necessárias
Exclua todos os recursos implantados.	Você pode deixar os recursos implantados nas contas.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Para desprovisionar todos os recursos, faça o seguinte: 1. Exclua a pilha `NAA-ExecRole` provisionada na conta de gerenciamento. Para obter instruções, consulte Como excluir uma pilha na CloudFormation documentação. 2. Exclua o conjunto de pilhas `NAA-ExecRole` provisionado na conta de gerenciamento da organização ou na conta de administrador delegada. Para obter instruções, consulte Excluir um conjunto de pilhas na CloudFormation documentação. 3. Exclua todos os objetos no bucket do `naa-<accountID>-<region>` Amazon S3. Para obter instruções, consulte Excluir objetos na documentação do Amazon S3. 4. Exclua a pilha `NAA-Resources` provisionada na conta de segurança. Para obter instruções, consulte Como excluir uma pilha na CloudFormation documentação.	

Solução de problemas

Problema	Solução
Não é possível se conectar à EC2 instância da Amazon usando o Gerenciador de Sessões.	O SSM Agent deve conseguir se comunicar com o endpoint do Session Manager. Faça o seguinte: 1. Valide que a sub-rede em que a EC2 instância da Amazon está implantada tem acesso à Internet. 2. Reinicie a EC2 instância da Amazon.
Ao implantar o conjunto de pilhas, o CloudFormation console solicita que você faça isso. `Enable trusted access with AWS Organizations to use service-managed permissions`	Isso indica que o acesso confiável não foi habilitado entre AWS Organizations CloudFormation e. É necessário o acesso confiável para implantar o conjunto de pilhas gerenciadas pelo serviço. Escolha o botão para habilitar o acesso confiável. Para obter mais informações, consulte Habilitar acesso confiável na CloudFormation documentação.

Recursos relacionados

- Novo — Analisador de acesso à rede Amazon VPC (AWS publicação no blog)
- AWS Re:inforce 2022 - Valide controles efetivos de acesso à rede em AWS (NIS202) (vídeo)
- Demonstração - Análise do caminho de dados de entrada na Internet em toda a organização usando o Analisador de Acesso à Rede (vídeo)

Mais informações

Exemplo de saída de console

O exemplo a seguir mostra o resultado da geração da lista de contas de destino e da análise das contas de destino.

```
[root@ip-10-10-43-82 naa]# ./naa-script.sh
```

```
download: s3://naa-<account ID>-us-east-1/naa-exclusions.csv to ./naa-exclusions.csv

AWS Management Account: <Management account ID>

AWS Accounts being processed...
<Account ID 1> <Account ID 2> <Account ID 3>

Assessing AWS Account: <Account ID 1>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 2>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 3>, using Role: NAAExecRole
Processing account: <Account ID 1> / Region: us-east-1
Account: <Account ID 1> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 2> / Region: us-east-1
Account: <Account ID 2> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 3> / Region: us-east-1
Account: <Account ID 3> / Region: us-east-1 - Detecting Network Analyzer scope...
Account: <Account ID 1> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 1> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 2> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 2> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 3> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 3> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
```

Exemplos de relatórios CSV

As imagens a seguir são exemplos da saída CSV.

Configure a resolução de DNS para redes híbridas em um ambiente com várias contas AWS

Criado por Anvesh Koganti (AWS)

Resumo

Esse padrão fornece uma solução abrangente para configurar a resolução de DNS em ambientes de rede híbrida que incluem várias contas da Amazon Web Services (AWS). Ele permite a resolução bidirecional de DNS entre redes locais e o ambiente por meio de endpoints. AWS Amazon Route 53 Resolver O padrão apresenta duas soluções para permitir a resolução de DNS em uma arquitetura centralizada com várias contas:

- A configuração básica não usa perfis do Route 53. Ele ajuda a otimizar os custos para implantações pequenas e médias de menor complexidade.
- A configuração aprimorada usa perfis do Route 53 para simplificar as operações. É melhor para implantações de DNS maiores ou mais complexas.

> **Note**
>
> Consulte a seção Limitações para ver as limitações e cotas do serviço antes da implementação. Considere fatores como despesas gerais de gerenciamento, custos, complexidade operacional e experiência da equipe ao tomar sua decisão.

Pré-requisitos e limitações

Pré-requisitos

- Um ambiente de AWS várias contas com Amazon Virtual Private Cloud (Amazon VPC) implantado em serviços compartilhados e contas de carga de trabalho (de preferência configurado por meio do AWS Control Tower AWS seguindo as melhores práticas de estrutura de contas).
- Conectividade híbrida existente (AWS Direct Connect ou AWS Site-to-Site VPN) entre sua rede local e o AWS ambiente.
- Amazon VPC peering ou Nuvem AWS WAN para AWS Transit Gateway conectividade de rede de camada 3 entre. VPCs (Essa conectividade é necessária para o tráfego do aplicativo. Não é

necessário que a resolução de DNS funcione. A resolução de DNS opera independentemente da conectividade de rede entre VPCs o.)

- Servidores DNS em execução no ambiente local.

Limitações

- Os endpoints, regras e perfis do Route 53 Resolver são construções regionais e podem exigir replicação em vários Regiões da AWS para organizações globais.
- Para obter uma lista abrangente de cotas de serviço para o Resolvedor do Route 53, zonas hospedadas privadas e perfis, consulte Cotas na documentação do Route 53.

Arquitetura

Pilha de tecnologias de destino

- Endpoints de saída e entrada do Route 53
- Regras do Route 53 Resolver para encaminhamento condicional
- AWS Resource Access Manager (AWS RAM)
- Zona hospedada privada do Route 53

Arquitetura de destino

Endpoints de saída e entrada

O diagrama a seguir mostra o fluxo de resolução de DNS de AWS para o local. Essa é a configuração de conectividade para resoluções de saída em que o domínio está hospedado localmente. Aqui está uma visão geral de alto nível do processo envolvido na configuração. Consulte a seção Épicos para obter detalhes.

1. Implante endpoints de saída do Route 53 Resolver na VPC do Shared Services.
2. Crie regras do Route 53 Resolver (regras de encaminhamento) na conta do Shared Services para domínios hospedados no local.
3. Compartilhe e associe as regras a outras contas que hospedam recursos que precisam resolver domínios hospedados no local. VPCs Isso pode ser feito de maneiras diferentes, dependendo do seu caso de uso, conforme descrito posteriormente nesta seção.

Depois de configurar a conectividade, as etapas envolvidas na resolução de saída são as seguintes:

1. A instância Amazon Elastic Compute Cloud (Amazon EC2) envia uma solicitação de resolução de DNS `db.onprem.example.com` para o Resolvedor Route 53 da VPC no endereço VPC+2.
2. O Resolvedor do Route 53 verifica as regras do Resolver e encaminha a solicitação para o servidor DNS local IPs usando o endpoint de saída.
3. O endpoint de saída encaminha a solicitação para o DNS local. IPs O tráfego passa pela conectividade de rede híbrida estabelecida entre a VPC do Shared Services e o data center local.
4. O servidor DNS local responde de volta ao endpoint de saída, que então encaminha a resposta de volta para o Resolvedor Route 53 da VPC. O Resolver retorna a resposta para a EC2 instância.

O diagrama a seguir mostra o fluxo de resolução de DNS do ambiente local para o. AWS Essa é a configuração de conectividade para resoluções de entrada em que o domínio está hospedado. AWS Aqui está uma visão geral de alto nível do processo envolvido na configuração. Consulte a seção Épicos para obter detalhes.

1. Implante endpoints de entrada do Resolver na VPC do Shared Services.
2. Crie zonas hospedadas privadas na conta do Shared Services (abordagem centralizada).
3. Associe as zonas hospedadas privadas à VPC do Shared Services. Compartilhe e associe essas zonas a várias contas VPCs para resolução de VPC-to-VPC DNS. Isso pode ser feito de maneiras diferentes, dependendo do seu caso de uso, conforme descrito posteriormente nesta seção.

Depois de configurar a conectividade, as etapas envolvidas na resolução de entrada são as seguintes:

1. O recurso local envia uma solicitação de resolução de DNS `ec2.prod.aws.example.com` para o servidor DNS local.
2. O servidor DNS local encaminha a solicitação para o endpoint Resolver de entrada na VPC do Shared Services pela conexão de rede híbrida.
3. O endpoint de entrada do Resolver pesquisa a solicitação na zona hospedada privada associada com a ajuda do VPC Route 53 Resolver e obtém o endereço IP apropriado.

4. Esses endereços IP são enviados de volta ao servidor DNS local, que retorna a resposta ao recurso local.

Essa configuração permite que os recursos locais resolvam nomes de domínio AWS privados roteando consultas pelos endpoints de entrada para a zona hospedada privada apropriada. Nessa arquitetura, as zonas hospedadas privadas são centralizadas em uma VPC de Serviços Compartilhados, o que permite o gerenciamento central do DNS por uma única equipe. Essas zonas podem ser associadas a várias VPCs para abordar o caso de uso da resolução de VPC-to-VPC DNS. Como alternativa, talvez você queira delegar a propriedade e o gerenciamento do domínio DNS a cada um. Conta da AWS Nesse caso, cada conta gerencia suas próprias zonas hospedadas privadas e associa cada zona à VPC central do Shared Services para uma resolução unificada com o ambiente local. Essa abordagem descentralizada está fora do escopo desse padrão. Para obter mais informações, consulte Como escalar o gerenciamento de DNS em várias contas e VPCs no whitepaper Opções de DNS de nuvem híbrida para Amazon VPC.

Ao estabelecer os fluxos fundamentais de resolução de DNS usando os endpoints do Resolver, você precisa determinar como gerenciar o compartilhamento e a associação das regras do Resolver e das zonas hospedadas privadas em todo o seu. Contas da AWS Você pode abordar isso de duas maneiras: por meio do compartilhamento autogerenciado usando AWS RAM para compartilhar regras do Resolver e associações diretas de zonas hospedadas privadas, conforme detalhado na seção Configuração básica, ou por meio dos Perfis do Route 53, conforme discutido na seção Configuração aprimorada. A escolha depende das preferências de gerenciamento de DNS e dos requisitos operacionais da sua organização. Os diagramas de arquitetura a seguir ilustram um ambiente escalável que inclui várias contas VPCs diferentes, o que representa uma implantação corporativa típica.

Configuração básica

Na configuração básica, a implementação da resolução de DNS híbrida em um AWS ambiente de várias contas é usada AWS RAM para compartilhar regras de encaminhamento do Resolver e associações de zonas hospedadas privadas para gerenciar consultas de DNS entre locais e recursos. AWS Esse método usa endpoints centralizados do Route 53 Resolver em uma VPC do Shared Services conectada à sua rede local para lidar com a resolução de DNS de entrada e saída com eficiência.

- Para resolução de saída, as regras de encaminhamento do Resolver são criadas na conta do Shared Services e depois compartilhadas com outras pessoas Contas da AWS usando. AWS RAM Esse compartilhamento é limitado a contas dentro da mesma região. As contas de destino podem

então associar essas regras às suas VPCs e habilitar os recursos nelas VPCs para resolver nomes de domínio locais.

- Para resolução de entrada, zonas hospedadas privadas são criadas na conta do Shared Services e associadas à VPC do Shared Services. Essas zonas podem então ser associadas VPCs a outras contas usando a API do Route 53 ou a AWS Command Line Interface (AWS CLI). AWS SDKs Os recursos associados VPCs podem então resolver os registros DNS definidos nas zonas hospedadas privadas, o que cria uma visão unificada do DNS em todo o seu AWS ambiente.

O diagrama a seguir mostra os fluxos de resolução de DNS nessa configuração básica.

Essa configuração funciona bem quando você trabalha com a infraestrutura de DNS em uma escala limitada. No entanto, pode ser difícil gerenciá-lo à medida que seu ambiente cresce. A sobrecarga operacional de gerenciar como a zona hospedada privada e as regras do Resolver são compartilhadas e associadas VPCs individualmente aumenta significativamente com a escala. Além disso, cotas de serviço, como o limite de associação de 300 VPC por zona hospedada privada, podem se tornar fatores restritivos em implantações em grande escala. A configuração aprimorada aborda esses desafios.

Configuração aprimorada

Os perfis do Route 53 oferecem uma solução simplificada para gerenciar a resolução de DNS em redes híbridas em várias. Contas da AWS Em vez de gerenciar zonas hospedadas privadas e regras do Resolver individualmente, você pode agrupar as configurações de DNS em um único contêiner que pode ser facilmente compartilhado e aplicado em várias VPCs contas em uma região. Essa configuração mantém a arquitetura centralizada do endpoint Resolver em uma VPC de Serviços Compartilhados e, ao mesmo tempo, simplifica significativamente o gerenciamento das configurações de DNS.

O diagrama a seguir mostra os fluxos de resolução de DNS em uma configuração aprimorada.

Os perfis do Route 53 permitem agrupar associações de zonas hospedadas privadas, regras de encaminhamento de resolvedores e regras de firewall DNS em uma única unidade compartilhável. Você pode criar perfis na conta do Shared Services e compartilhá-los com contas de membros usando AWS RAM. Quando um perfil é compartilhado e aplicado ao alvo VPCs, todas as associações e configurações necessárias são gerenciadas automaticamente pelo serviço. Isso

reduz significativamente a sobrecarga operacional do gerenciamento de DNS e fornece excelente escalabilidade para ambientes em crescimento.

Automação e escala

Use ferramentas de infraestrutura como código (IaC), como AWS CloudFormation o Terraform, para provisionar e gerenciar automaticamente endpoints, regras, zonas hospedadas privadas e perfis do Route 53 Resolver. Integre a configuração de DNS com pipelines de integração contínua e entrega contínua (CI/CD) para obter consistência, repetibilidade e atualizações rápidas.

Ferramentas

Serviços da AWS

- AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar seus recursos com segurança Contas da AWS para reduzir a sobrecarga operacional e fornecer visibilidade e auditabilidade.
- Amazon Route 53 Resolverresponde recursivamente às consultas de DNS dos AWS recursos e está disponível por padrão em todos. VPCs Você pode criar endpoints do Resolver e regras de encaminhamento condicional para resolver namespaces DNS entre seu data center local e seu. VPCs
- A zona hospedada privada do Amazon Route 53 é um contêiner que contém informações sobre como você deseja que o Route 53 responda às consultas de DNS para um domínio e seus subdomínios.
- Os perfis do Amazon Route 53 permitem que você aplique e gerencie configurações do Route 53 relacionadas ao DNS em várias VPCs e diferentes configurações de forma Contas da AWS simplificada.

Práticas recomendadas

Esta seção fornece algumas das melhores práticas para otimizar o Route 53 Resolver. Elas representam um subconjunto das melhores práticas do Route 53. Para obter uma lista abrangente, consulte Melhores práticas para o Amazon Route 53.

Evite configurações de loop com endpoints Resolver

- Projete sua arquitetura de DNS para evitar o roteamento recursivo planejando cuidadosamente as associações de VPC. Quando uma VPC hospeda um endpoint de entrada, evite associá-lo às regras do Resolver que poderiam criar referências circulares.

- Use AWS RAM estrategicamente ao compartilhar recursos de DNS entre contas para manter caminhos de roteamento limpos.

Para obter mais informações, consulte Evite configurações de loop com endpoints do Resolver na documentação do Route 53.

Pontos finais do Scale Resolver

- Para ambientes que exigem um alto número de consultas por segundo (QPS), esteja ciente de que há um limite de 10.000 QPS por ENI em um endpoint. Mais ENIs podem ser adicionados a um endpoint para escalar o DNS QPS.
- CloudWatch Fornecedores `InboundQueryVolume` e `OutboundQueryVolume` métricas da Amazon (consulte a CloudWatch documentação). Recomendamos que você configure regras de monitoramento que alertem você se o limite exceder um determinado valor (por exemplo, 80% de 10.000 QPS).
- Configure regras de grupo de segurança com estado para endpoints do Resolver para evitar que limites de rastreamento de conexão causem limitação de consultas de DNS durante tráfego de alto volume. Para saber mais sobre como o rastreamento de conexão funciona em grupos de segurança, consulte Rastreamento de conexão de grupos de EC2 segurança da Amazon na EC2 documentação da Amazon.

Para obter mais informações, consulte Escalabilidade de endpoint do Resolver na documentação do Route 53.

Forneça alta disponibilidade para endpoints do Resolver

- Crie endpoints de entrada com endereços IP em, pelo menos, duas zonas de disponibilidade para garantir redundância.
- Provisione interfaces de rede adicionais para garantir a disponibilidade durante a manutenção ou picos de tráfego.

Para obter mais informações, consulte Alta disponibilidade para endpoints do Resolver na documentação do Route 53.

Épicos

Implante endpoints do Route 53 Resolver

Tarefa	Descrição	Habilidades necessárias
Implante um endpoint de entrada.	O Route 53 Resolver usa o endpoint de entrada para receber consultas ao DNS de solucionadores DNS on-premises. Para obter instruções, consulte Encaminhando consultas de DNS de entrada para você VPCs na documentação do Route 53. Anote o endereço IP do endpoint de entrada.	Administrador da AWS, administrador de nuvem
Implante um endpoint de saída.	O Route 53 Resolver usa o endpoint de saída para enviar consultas ao DNS para solucionadores DNS on-premises. Para obter instruções, consulte Como encaminhar consultas ao DNS de saída para sua rede na documentação do Route 53. Anote o ID do endpoint de saída.	Administrador da AWS, administrador de nuvem

Configurar e compartilhar zonas hospedadas privadas do Route 53

Tarefa	Descrição	Habilidades necessárias
Crie uma zona hospedada privada para um domínio hospedado em AWS.	Essa zona contém os registros DNS dos recursos em um domínio AWS hospedado (por exemplo,`prod.aws.`	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	`example.com`) que devem ser resolvidos a partir do ambiente local. Para obter instruções, consulte Como criar uma zona hospedada privada na documentação do Route 53. Ao criar uma zona hospedada privada, você deve associar uma VPC à zona hospedada de propriedade da mesma conta. Selecione a VPC do Shared Services para essa finalidade.	
Configuração básica: associe a zona hospedada privada VPCs a outras contas.	Se você estiver usando a configuração básica (consulte a seção Arquitetura): Para permitir que recursos na conta do membro VPCs resolvam registros DNS nessa zona hospedada privada, você deve associar o seu VPCs à zona hospedada. Você deve autorizar a associação e, em seguida, fazer a associaçã o programaticamente. Para obter instruções, consulte Associando uma Amazon VPC e uma zona hospedada privada que você criou com Contas da AWS diferentes na documentação do Route 53.	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Configuração aprimorada: configure e compartilhe perfis do Route 53.	Se você estiver usando a configuração aprimorada (consulte a seção Arquitetura): 1. Crie um perfil do Route 53 e associe as zonas hospedadas privadas relevantes a ele. Para obter instruções, consulte Criação de perfis do Route 53 na documentação do Route 53. 2. Use AWS RAM para compartilhar o perfil com contas de membros e, em seguida, associar o perfil compartilhado ao alvo VPCs. Para obter instruções, consulte Compartilhando um perfil do Route 53 e Associar um perfil do Route 53 VPCs na documentação do Route 53. **Note** Dependendo da estrutura da sua organização e dos requisitos de DNS, talvez seja necessário criar e gerenciar vários perfis para diferentes	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	contas ou cargas de trabalho.	

Configurar e compartilhar regras de encaminhamento do Route 53 Resolver

Tarefa	Descrição	Habilidades necessárias
Crie uma regra de encaminhamento para um domínio hospedado no local.	Essa regra instruirá o Resolvedor do Route 53 a encaminhar quaisquer consultas de DNS para domínios locais (como `onprem.example.com`) para resolvedores de DNS locais. Para criar essa regra, você precisa dos endereços IP dos resolvedores de DNS locais e da ID do endpoint de saída. Para obter instruções, consulte Criação de regras de encaminhamento na documentação do Route 53.	Administrador da AWS, administrador de nuvem
Configuração básica: compartilhe e associe a regra de encaminhamento à sua VPCs em outras contas.	Se você estiver usando a configuração básica: Para que a regra de encaminhamento entre em vigor, você deve compartilhar e associar a regra às suas VPCs em outras contas. O Route 53 Resolver então leva a regra em consideração ao	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	resolver um domínio. Para obter instruções, consulte Compartilhamento de regras do Resolvedor com outras pessoas Contas da AWS e uso de regras compartilhadas e Associação de regras de encaminhamento a uma VPC na documentação do Route 53.	

Tarefa	Descrição	Habilidades necessárias
Configuração aprimorada: configure e compartilhe perfis do Route 53.	Se você estiver usando a configuração aprimorada: 1. Se você já criou um perfil do Route 53 nas etapas anteriores, você pode usar o mesmo perfil. Caso contrário, crie um perfil do Route 53 e associe as regras de encaminhamento relevantes do Resolver a ele. Para obter instruções, consulte Criação de perfis do Route 53 na documentação do Route 53. 2. Use AWS RAM para compartilhar o perfil com contas de membros e, em seguida, associar o perfil compartilhado ao alvo VPCs. Para obter instruções, consulte Compartilhando um perfil do Route 53 e Associar um perfil do Route 53 VPCs na documentação do Route 53. **Note** Dependendo da estrutura da sua organização e dos requisitos de DNS, talvez seja necessário	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	criar e gerenciar vários perfis para diferentes contas ou cargas de trabalho.	

Configurar resolvedores de DNS locais para integração AWS

Tarefa	Descrição	Habilidades necessárias
Configure o encaminhamento condicional nos resolvedores de DNS locais.	Para que as consultas DNS sejam enviadas AWS do ambiente local para resolução , você deve configurar o encaminhamento condicional nos resolvedores de DNS locais para apontar para o endereço IP do endpoint de entrada. Isso instrui os resolvedores de DNS a encaminhar todas as consultas de DNS do domínio AWS hospedado (por exemplo, for`prod.aws.example.com`) para o endereço IP do endpoint de entrada para resolução pelo Route 53 Resolver.	Administrador de rede

Verifique a resolução end-to-end do DNS em um ambiente híbrido

Tarefa	Descrição	Habilidades necessárias
Teste a resolução de DNS AWS até o ambiente local.	Em uma instância em uma VPC que tenha a regra de encaminhamento associada a ela, execute uma consulta de DNS para um domínio hospedado no local (por exemplo, for). `db.onprem.example.com`	Administrador de rede
Teste a resolução de DNS do ambiente local para. AWS	Em um servidor local, execute a resolução de DNS para um domínio AWS hospedado (por exemplo, para). `ec2.prod.aws.example.com`	Administrador de rede

Recursos relacionados

- Opções de DNS de nuvem híbrida para Amazon VPCAWS (whitepaper)
- Trabalhando com zonas hospedadas privadas (documentação do Route 53)
- Introdução ao Route 53 Resolver (documentação do Route 53)
- Simplifique o gerenciamento de DNS em um ambiente de várias contas com o Route 53 Resolver (AWS postagem no blog)
- Unifique o gerenciamento de DNS usando perfis do Amazon Route 53 com vários VPCs e Contas da AWS (AWS postagem no blog)
- Migrando seu ambiente DNS de várias contas para os perfis do Amazon Route 53 (AWS postagem no blog)
- Usando perfis do Amazon Route 53 para AWS ambientes escaláveis de várias contas (AWS postagem no blog)

Verifique se os balanceadores de carga ELB exigem terminação TLS

Criado por Priyanka Chaudhary (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), o Elastic Load Balancing (ELB) distribui automaticamente o tráfego de entrada do aplicativo em vários destinos, como instâncias do Amazon Elastic Compute Cloud (Amazon EC2), contêineres, endereços IP e funções do AWS Lambda. Os balanceadores de carga usam receptores para definir as portas e os protocolos que o balanceador de carga usa para aceitar o tráfego dos usuários. Os balanceadores de carga de aplicativos tomam decisões de roteamento na camada do aplicativo e usam o. HTTP/HTTPS protocols. Classic Load Balancers make routing decisions at either the transport layer, by using TCP or Secure Sockets Layer (SSL) protocols, or at the application layer, by using HTTP/HTTPS

Esse padrão fornece um controle de segurança que examina vários tipos de eventos para Application Load Balancers e Classic Load Balancers. Quando a função é invocada, o AWS Lambda inspeciona o evento e garante que o balanceador de carga esteja em conformidade.

A função inicia um evento Amazon CloudWatch Events nas seguintes chamadas de API: CreateLoadBalancerCreateLoadBalancerListeners, DeleteLoadBalancerListeners, CreateLoadBalancerPolicy, SetLoadBalancerPoliciesOfListener, CreateListener, DeleteListener, e. ModifyListener Quando o evento detecta um deles APIs, ele chama o AWS Lambda, que executa um script Python. O script Python avalia se o receptor contém um certificado SSL e se a política aplicada está usando Transport Layer Security (TLS). Se a política SSL for determinada como diferente de TLS, a função enviará uma notificação do Amazon Simple Notification Service (Amazon SNS) ao usuário com as informações relevantes.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa

Limitações

- Esse controle de segurança não verifica os balanceadores de carga existentes, a menos que seja feita uma atualização nos receptores do balanceador de carga.

- Esse controle de segurança é regional. Você deve implantá-lo em cada região da AWS que você deseja monitorar.

Arquitetura

Arquitetura de destino

Automação e escala

- Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

Serviços da AWS

- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

Esse padrão inclui os seguintes anexos:

- `ELBRequirestlstermination.zip`: o código Lambda para o controle de segurança.
- `ELBRequirestlstermination.yml`— O CloudFormation modelo que configura o evento e a função Lambda.

Épicos

Configurar o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	No console do Amazon S3, escolha ou crie um bucket do S3 para hospedar o arquivo .zip do código do Lambda. Esse bucket do S3 deve estar na mesma região da AWS que o balanceador de carga que você deseja avaliar. Um nome de bucket do S3 é globalmente exclusivo, e o namespace é compartilhado por todas as contas da AWS. O nome do bucket do S3 não pode incluir barras iniciais.	Arquiteto de nuvem
Faça o upload do código do Lambda.	Faça upload do código do Lambda (arquivo `ELBRequirestlstermination.zip`) fornecido na seção Anexos para o bucket do S3.	Arquiteto de nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo da AWS.	Abra o CloudFormation console da AWS na mesma região da AWS do seu bucket do S3 e implante o modelo `ELBRequirestlstermination.yml` anexado. Para obter mais informações sobre a implantação de CloudFormation modelos da AWS, consulte Como criar uma pilha no CloudFormation console da AWS na CloudFormation documentação.	Arquiteto de nuvem
Preencher os parâmetros no modelo.	Ao iniciar o modelo, você será solicitado a fornecer as seguintes informações: • Bucket do S3: especifique o bucket que você criou ou selecionou no primeiro épico. É aqui que você fez o upload do código do Lambda anexado (arquivo `ELBRequirestlstermination.zip`). • Chave do S3: especifique a localização do arquivo .zip do Lambda em seu bucket do S3 (por exemplo, `ELBRequirestlstermination.zip` ou	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`controls/ELBRequirestlstermination.zip`). Não inclua barras iniciais. • E-mail de notificação: forneça um endereço de e-mail ativo para receber notificações do Amazon SNS. • Nível de registro do Lambda: especifique o nível de registro em log e a frequência da função do Lambda. Use Informaçõ es para registrar em log mensagens informati vas detalhadas sobre o progresso, Erro para eventos de erro que ainda permitiriam a continuidade da implantação e Aviso sobre situações potencial mente prejudiciais.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o CloudFormation modelo é implantado com sucesso, ele envia um e-mail de assinatura para o endereço de e-mail que você forneceu. Você deve confirmar essa	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	assinatura de e-mail para começar a receber notificaç ões de violação.	

Recursos relacionados

- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- O que é o AWS Lambda? (Documentação do AWS Lambda)
- O que é um Classic Load Balancer? (Documentação do ELB)
- O que é um Application Load Balancer? (Documentação do ELB)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Visualize registros e métricas do AWS Network Firewall usando o Splunk

Criado por Ivo Pinto

Resumo

Muitas organizações usam o Splunk Enterprise como uma ferramenta centralizada de agregação e visualização para registros e métricas de diferentes fontes. Esse padrão ajuda você a configurar o Splunk para buscar registros e métricas do AWS Network Firewall do Amazon CloudWatch Logs usando o complemento Splunk para AWS.

Para conseguir isso, você cria uma função somente para leitura do AWS Identity and Access Management (IAM). O complemento Splunk para AWS usa essa função para acessar. CloudWatch Você configura o complemento Splunk para AWS para buscar métricas e registros do. CloudWatch Por fim, você cria visualizações no Splunk a partir dos dados e métricas de log recuperados.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta Splunk
- Uma instância do Splunk Enterprise, versão 8.2.2 ou posterior
- Uma conta AWS ativa
- Firewall de rede, configurado e configurado para enviar registros para o CloudWatch Logs

Limitações

- O Splunk Enterprise deve ser implantado como um cluster de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) na Nuvem AWS.
- A coleta de dados usando uma função do IAM descoberta automaticamente para a Amazon não EC2 é suportada nas regiões da AWS na China.

Arquitetura

O diagrama ilustra o seguinte:

1. O Network Firewall publica registros em CloudWatch Logs.

2. O Splunk Enterprise recupera métricas e registros de. CloudWatch

Para preencher exemplos de métricas e registros nessa arquitetura, uma carga de trabalho gera tráfego que passa pelo endpoint do Network Firewall para acessar a Internet. Isso é obtido pelo uso de tabelas de rotas. Embora esse padrão use uma única EC2 instância da Amazon como carga de trabalho, esse padrão pode ser aplicado a qualquer arquitetura, desde que o Network Firewall esteja configurado para enviar CloudWatch registros para Logs.

Essa arquitetura também usa uma instância do Splunk Enterprise em outra nuvem privada virtual (VPC). No entanto, a instância do Splunk pode estar em outro local, como na mesma VPC da carga de trabalho, desde que possa alcançar o. CloudWatch APIs

Ferramentas

Serviços da AWS

- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas, aplicativos e serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Network Firewall é um firewall de rede gerenciado e monitorado, além de um serviço de detecção e prevenção de intrusões VPCs na nuvem da AWS.

Outras ferramentas

- O Splunk ajuda você a monitorar, visualizar e analisar dados de log.

Épicos

Criar um perfil do IAM

Tarefa	Descrição	Habilidades necessárias
Crie a política do IAM.	Siga as instruções em Como criar políticas usando o editor JSON para criar a	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	política do IAM que concede acesso somente para leitura aos dados e métricas do CloudWatch Logs. CloudWatch Cole a política a seguir no editor de JSON. `{ "Statement": [ { "Action": [ "cloudwatch:List*", "cloudwatch:Get*", "network-firewall:List*", "logs:Describe*", "logs:Get*", "logs:List*", "logs:StartQuery", "logs:StopQuery", "logs:TestMetricFilter", "logs:FilterLogEvents", "network-firewall:Describe*" ], "Effect": "Allow",`	

Tarefa	Descrição	Habilidades necessárias
	<pre>"Resource": "*" }], "Version": "2012-10-17" }</pre>	
Crie uma nova função do IAM.	Siga as instruções em Criação de uma função para delegar permissões a um serviço da AWS para criar a função do IAM que o complemento Splunk para AWS usa para acessar. CloudWatch Em Políticas de permissões, escolha a política que você criou anteriormente.	Administrador da AWS
Atribua a função do IAM às EC2 instâncias no cluster Splunk.	1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/. 2. No painel de navegação, escolha Instâncias. 3. Selecione as EC2 instâncias no cluster Splunk. 4. Escolha Ações, Segurança e, em seguida, Modificar a função do IAM. 5. Selecione a função do IAM que você criou anteriormente e escolha Salvar.	Administrador da AWS

Instale o complemento Splunk para AWS

Tarefa	Descrição	Habilidades necessárias
Instale o complemento .	1. No painel do Splunk, navegue até Splunk Apps. 2. Pesquise o complemento Splunk para Amazon Web Services. 3. Escolha Instalar. 4. Forneça suas credenciais do Splunk.	Administrador do Splunk
Configure as credenciais da AWS.	1. No painel do Splunk, navegue até o complemen to Splunk para AWS. 2. Escolher configuração. 3. Na coluna Função do IAM descoberta automática, selecione a função do IAM que você criou anteriorm ente. Para obter mais informações, consulte Encontre uma função do IAM em sua instância da plataforma Splunk na documentação do Splunk.	Administrador do Splunk

Configure o acesso do Splunk ao CloudWatch

Tarefa	Descrição	Habilidades necessárias
Configure a recuperação dos registros do Firewall de Rede a partir dos CloudWatch Registros.	1. No painel do Splunk, navegue até o complemento Splunk para AWS. 2. Escolha Entrada. 3. Escolha Criar nova entrada. 4. Na lista, escolha Tipo de dados personalizado e, em seguida, escolha CloudWatch Registros. 5. Forneça o nome, a conta da AWS, a região da AWS e o grupo de registros para seus registros do Network Firewall. 6. Escolha Salvar. Por padrão, o Splunk busca os dados de log a cada 10 minutos. Esse é um parâmetro configurável em Configurações avançadas. Para obter mais informações, consulte Configurar uma entrada de CloudWatch registros usando o Splunk Web na documentação do Splunk.	Administrador do Splunk
Configure a recuperação das métricas do Network Firewall de CloudWatch.	1. No painel do Splunk, navegue até o complemento Splunk para AWS. 2. Escolha Entrada.	Administrador do Splunk

Tarefa	Descrição	Habilidades necessárias
	3. Escolha Criar nova entrada. 4. Na lista, escolha CloudWatch. 5. Forneça o nome, a conta da AWS e a região da AWS para suas métricas do Network Firewall. 6. Ao lado de Configuração métrica, escolha Editar no modo avançado. 7. (Opcional) Exclua todos os namespaces pré-configurados. 8. Escolha Adicionar namespace e, em seguida, nomeie-o como AWS/NetworkFirewall 9. Em Valor da Dimensão, adicione o seguinte. `[{"AvailabilityZone":[".*"],"Engine":[".*"],"FirewallName":[".*"]}]` 10. Em Métricas, escolha Tudo. 11. Para Estatísticas métricas, escolha Soma. 12. Escolha OK. 13. Escolha Salvar. Por padrão, o Splunk busca os dados métricos a cada 5 minutos. Esse é um parâmetro	

Tarefa	Descrição	Habilidades necessárias
	configurável em Configura ções avançadas. Para obter mais informações, consulte Configurar uma CloudWatch entrada usando o Splunk Web na documentação do Splunk.	

Crie visualizações do Splunk usando consultas

Tarefa	Descrição	Habilidades necessárias
Veja os principais endereços IP de origem.	1. No painel do Splunk, navegue até Pesquisa e relatórios. 2. Na caixa digitar pesquisar aqui, digite o seguinte. `sourcetype="aws:cloudwatchlogs" | top event.src_ip` Essa consulta exibe uma tabela dos endereços IP de origem com mais tráfego, em ordem decrescente. 3. Para uma representação gráfica, escolha Visualização.	Administrador do Splunk
Exibir estatísticas de pacotes.	1. No painel do Splunk, navegue até Pesquisa e relatórios. 2. Na caixa digitar pesquisar aqui, digite o seguinte.	Administrador do Splunk

Tarefa	Descrição	Habilidades necessárias
	`sourcetype="aws:cloudwatch"| timechart sum(Sum) by metric_name` Essa consulta exibe uma tabela das métricas `DroppedPackets` `PassedPackets`, e `ReceivedPackets` por minuto. 3. Para uma representação gráfica, escolha Visualização.	
Veja as portas de origem mais usadas.	1. No painel do Splunk, navegue até Pesquisa e relatórios. 2. Na caixa digitar pesquisar aqui, digite o seguinte. `sourcetype="aws:cloudwatchlogs" | top event.dest_port` Essa consulta exibe uma tabela das portas de origem com mais tráfego, em ordem decrescente. 3. Para uma representação gráfica, escolha Visualização.	Administrador do Splunk

Recursos relacionados

Documentação da AWS

- Criação de uma função para delegar permissões a um serviço da AWS (documentação do IAM)
- Criação de políticas do IAM (Documentação do IAM)
- Registro e monitoramento no Firewall de Rede da AWS (documentação do Firewall de Rede)
- Configurações da tabela de rotas para o Firewall de Rede da AWS (documentação do Firewall de Rede)

Publicações do blog da AWS

- Modelos de implantação do AWS Network Firewall

AWS Marketplace

- Imagem de máquina da Amazon (AMI) da Splunk Enterprise

Mais padrões

- Acesse um bastion host usando o Session Manager e o Amazon EC2 Instance Connect
- Acesse aplicativos de contêineres de forma privada no Amazon ECS usando o AWS Fargate, a PrivateLink AWS e um Network Load Balancer
- Acesse aplicativos de contêineres de forma privada no Amazon ECS usando a AWS PrivateLink e um Network Load Balancer
- Centralize a resolução de DNS usando o Microsoft AWS Managed Microsoft AD Active Directory local
- Verifique as entradas de rede de host único nas regras de entrada do grupo de segurança para e IPv4 IPv6
- Crie um portal para microfrontends usando Angular e AWS Amplify Module Federation
- Implante um firewall usando o AWS Network Firewall e o AWS Transit Gateway
- Implante uma API do Amazon API Gateway em um site interno usando endpoints privados e um Application Load Balancer
- Implemente controles de acesso baseados em atributos de detetive para sub-redes públicas usando AWS Config
- Implemente controles de acesso preventivos baseados em atributos para sub-redes públicas
- Habilite conexões criptografadas para instâncias de banco de dados PostgreSQL no Amazon RDS
- Estenda VRFs para a AWS usando o AWS Transit Gateway Connect
- Migre uma workload do F5 BIG-IP para o F5 BIG-IP VE na Nuvem AWS
- Migre os controladores de entrada NGINX ao ativar o modo automático do Amazon EKS
- Preserve o espaço IP roteável em projetos de VPC com várias contas para sub-redes sem workload
- Impeça o acesso à Internet no nível da conta usando uma política de controle de serviços
- Envie alertas do AWS Network Firewall para um canal do Slack
- Ofereça conteúdo estático em um bucket do Amazon S3 por meio de uma VPC usando a Amazon CloudFront
- Configure a recuperação de desastres para o Oracle JD Edwards com o EnterpriseOne AWS Elastic Disaster Recovery
- Use as consultas do BMC Discovery para extrair dados de migração para o planejamento da migração

- Use o Network Firewall para capturar os nomes de domínio DNS da Indicação de Nome do Servidor para tráfego de saída

Entrega de conteúdo

Tópicos

- Envie AWS WAF registros para o Splunk usando o AWS Firewall Manager Amazon Data Firehose
- Ofereça conteúdo estático em um bucket do Amazon S3 por meio de uma VPC usando a Amazon CloudFront
- Mais padrões

Envie AWS WAF registros para o Splunk usando o AWS Firewall Manager Amazon Data Firehose

Criado por Michael Friedenthal (AWS), Aman Kaur Gandhi (AWS) e JJ Johnson (AWS)

Resumo

Historicamente, havia duas maneiras de mover dados para o Splunk: uma arquitetura push ou pull. Uma arquitetura pull oferece garantias de entrega de dados por meio de novas tentativas, mas requer recursos dedicados no Splunk para pesquisar dados. As arquiteturas Pull geralmente não são em tempo real por causa da pesquisa. Uma arquitetura push normalmente tem menor latência, é mais escalável e reduz a complexidade operacional e os custos. No entanto, isso não garante a entrega e normalmente requer agentes.

A integração do Splunk com o Amazon Data Firehose fornece dados de streaming em tempo real para o Splunk por meio de um coletor de eventos HTTP (HEC). Essa integração oferece as vantagens das arquiteturas push e pull – ela garante a entrega de dados por meio de novas tentativas, é quase em tempo real e tem baixa latência e baixa complexidade. O HEC envia dados de forma rápida e eficiente por HTTP ou HTTPS diretamente para o Splunk. HECs são baseados em tokens, o que elimina a necessidade de codificar credenciais em um aplicativo ou em arquivos de suporte.

Em uma AWS Firewall Manager política, você pode configurar o registro para todo o tráfego de ACL AWS WAF da web em todas as suas contas e, em seguida, usar um stream de entrega do Firehose para enviar esses dados de registro ao Splunk para monitoramento, visualização e análise. Essa solução oferece os seguintes benefícios:

- Gerenciamento central e registro do tráfego de ACL AWS WAF da web em todas as suas contas
- Integração do Splunk com um único Conta da AWS
- Escalabilidade
- Entrega quase em tempo real dos dados de log
- Otimização de custos por meio do uso de uma solução de tecnologia sem servidor, para que você não precise pagar por recursos não utilizados.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS que faz parte de uma organização em AWS Organizations.
- Você deve ter as seguintes permissões para ativar o registro com o Firehose:
  - `iam:CreateServiceLinkedRole`
  - `firehose:ListDeliveryStreams`
  - `wafv2:PutLoggingConfiguration`
- AWS WAF e sua web ACLs deve ser configurada. Para obter instruções, consulte Introdução ao AWS WAF.
- AWS Firewall Manager deve ser configurado. Para obter instruções, consulte os AWS Firewall Manager pré-requisitos.
- As políticas de segurança do Firewall Manager AWS WAF devem ser configuradas. Para obter instruções, consulte Introdução às AWS Firewall ManagerAWS WAF políticas.
- O Splunk deve ser configurado com um endpoint HTTP público que possa ser acessado pelo Firehose.

Limitações

- Eles Contas da AWS devem ser gerenciados em uma única organização em AWS Organizations.
- A Web ACL deve estar na mesma região do que o fluxo de entrega. Se você estiver capturando registros para a Amazon CloudFront, crie o stream de entrega do Firehose na região Leste dos EUA (Norte da Virgínia),. `us-east-1`
- O complemento Splunk para Firehose está disponível para implantações pagas do Splunk Cloud, implantações distribuídas do Splunk Enterprise e implantações do Splunk Enterprise de instância única. Esse complemento não é compatível com implantações de teste gratuito do Splunk Cloud.

Arquitetura

Pilha de tecnologias de destino

- Firewall Manager
- Firehose
- Amazon Simple Storage Service (Amazon S3)
- AWS WAF
- Splunk

Arquitetura de destino

A imagem a seguir mostra como você pode usar o Firewall Manager para registrar centralmente todos os AWS WAF dados e enviá-los ao Splunk por meio do Firehose.

1. A AWS WAF web ACLs envia dados de registro do firewall para o Firewall Manager.
2. O Firewall Manager envia os dados de registro para o Firehose.
3. O stream de entrega do Firehose encaminha os dados de log para o Splunk e para um bucket do S3. O bucket do S3 atua como um backup no caso de um erro com o stream de entrega do Firehose.

Automação e escala

Essa solução foi projetada para escalar e acomodar toda a AWS WAF web ALCs dentro da organização. Você pode configurar toda ACLs a web para usar a mesma instância do Firehose. No entanto, se você quiser configurar e usar várias instâncias do Firehose, você pode.

Ferramentas

Serviços da AWS

- AWS Firewall Manageré um serviço de gerenciamento de segurança que ajuda você a configurar e gerenciar centralmente as regras de firewall em suas contas e aplicativos em AWS Organizations.
- O Amazon Data Firehose ajuda você a entregar dados de streaming em tempo real para outros Serviços da AWS endpoints HTTP personalizados e endpoints HTTP de propriedade de provedores de serviços terceirizados compatíveis, como o Splunk.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- AWS WAFé um firewall de aplicativo web que ajuda você a monitorar solicitações HTTP e HTTPS que são encaminhadas para seus recursos protegidos de aplicativos web.

Outras ferramentas

- O Splunk ajuda você a monitorar, visualizar e analisar dados de log.

Épicos

Configurar o Splunk

Tarefa	Descrição	Habilidades necessárias
Instale o aplicativo Splunk para AWS.	1. Faça login no Splunk Heavy Forwarder. O URL padrão é `http://<IP address>:8000` . 2. Na navegação à esquerda, ao lado de Aplicativos, escolha o botão de engrenagem. 3. Escolha Procurar mais aplicativos. 4. Pesquise por AWS. 5. Para o aplicativo Splunk para AWS, escolha Instalar. 6. Insira suas credenciais de login no Splunk.com, aceite os termos e condições e escolha Login e Instalar. 7. Selecione Concluído.	Administrador de segurança, administrador do Splunk
Instale o complemento para AWS WAF.	Repita as instruções anteriores para instalar o complemento AWS Web Application Firewall para Splunk.	Administrador de segurança, administrador do Splunk
Instale e configure o complemento Splunk para Firehose.	1. Instale e configure o complemento Splunk para Firehose. Como parte da instalação e configuração, se necessário para sua plataforma Splunk, você	Administrador de segurança, administrador do Splunk

Tarefa	Descrição	Habilidades necessárias
	configura um coletor de eventos HTTP e prepara a infraestrutura para enviar os dados de log aos seus indexadores. Veja as instruções que correspondem à sua implantação do Splunk: • Implantação do Splunk Cloud (documentação do Splunk) • Implantação distribuída do Splunk Enterprise (documentação do Splunk) • Implantação do Splunk Enterprise em uma única instância (documentação do Splunk) **Important** Pare esse procedimento depois de instalar e configurar o complemento Splunk. Não continue com as instruções para configurar o Firehose para enviar dados para a plataforma Splunk.	

Tarefa	Descrição	Habilidades necessárias
	2. Anote o token do coletor de eventos HTTP e o endpoint HTTP. Você precisará desse valor posteriormente, ao configurar o stream de entrega.	

Crie o stream de entrega do Firehose

Tarefa	Descrição	Habilidades necessárias
Conceda ao Firehose acesso a um destino do Splunk.	Configure a política de acesso que permite que o Firehose acesse um destino do Splunk e faça backup dos dados de log em um bucket do S3. Para obter mais informaçõ es, consulte Conceder ao Firehose acesso a um destino do Splunk.	Administrador de segurança
Crie um stream de entrega do Firehose.	Na mesma conta em que você gerencia a web ACLs AWS WAF, crie um stream de entrega no Firehose. Você precisa ter um perfil do IAM ao criar um fluxo de entrega. O Firehose assume essa função do IAM e obtém acesso ao bucket S3 especificado. Para obter instruções, consulte Criação de um stream de entrega. Observe o seguinte:	Administrador de segurança

Tarefa	Descrição	Habilidades necessárias
	• O nome do fluxo de entrega deve começar com `aws-waf-logs-` . • Para a fonte, escolha Direct PUT. • Para o modo de backup do S3, escolha Backup de todos os eventos e, em seguida, escolha um bucket existente ou crie um novo. • Para o destino, siga as instruções em Escolha o Splunk para seu destino na documentação do Firehose. Para obter informações sobre os valores dos endpoints e tipos de endpoints do Splunk, consulte Configurar o Amazon Data Firehose na documentação do Splunk. Repita esse processo para cada token que você configurou no coletor de eventos HTTP.	
Teste o fluxo de entrega.	Teste o stream de entrega para validar se ele está configurado corretamente. Para obter instruções, consulte Testar usando o Splunk como destino na documentação do Firehose.	Administrador de segurança

Configure o Firewall Manager para registrar dados

Tarefa	Descrição	Habilidades necessárias
Configure as políticas do Firewall Manager.	As políticas do Firewall Manager devem ser configuradas para ativar o registro e encaminhar os registros para o fluxo de entrega correto do Firehose. Para obter mais informações e instruções, consulte Como configurar o registro em log para uma AWS WAF política.	Administrador de segurança

Recursos relacionados

AWS recursos

- Registrando tráfego de ACL da web (AWS WAF documentação)
- Configurando o registro em log para uma AWS WAF política (AWS WAF documentação)
- Tutorial: Enviando registros de fluxo de VPC para o Splunk usando o Amazon Data Firehose (documentação do Firehose)
- Como faço para enviar registros de fluxo de VPC para o Splunk usando o Amazon Data Firehose? (Centro de AWS conhecimento)
- Potencialize a ingestão de dados no Splunk usando o Amazon Data Firehose (postagem no blog)AWS

Documentação do Splunk

- Complemento Splunk para Amazon Data Firehose

Ofereça conteúdo estático em um bucket do Amazon S3 por meio de uma VPC usando a Amazon CloudFront

Criado por Angel Emmanuel Hernandez Cebrian

Resumo

Quando você veicula conteúdo estático hospedado na Amazon Web Services (AWS), a abordagem recomendada é usar um bucket do Amazon Simple Storage Service (S3) como origem e usar a Amazon CloudFront para distribuir o conteúdo. Essa solução tem dois benefícios principais: a conveniência de armazenar em cache conteúdo estático em locais periféricos e a capacidade de definir listas de controle de acesso à web (web ACLs) para a CloudFront distribuição, o que ajuda a proteger as solicitações de conteúdo com o mínimo de configuração e sobrecarga administrativa.

No entanto, há uma limitação arquitetônica comum à abordagem padrão recomendada. Em alguns ambientes, você deseja que dispositivos de firewall virtual sejam implantados em uma nuvem privada virtual (VPC) para inspecionar todo o conteúdo, inclusive conteúdo estático. A abordagem padrão não direciona o tráfego pela VPC para inspeção. Esse padrão fornece uma solução arquitetônica alternativa. Você ainda usa uma CloudFront distribuição para veicular conteúdo estático em um bucket do S3, mas o tráfego é roteado pela VPC usando um Application Load Balancer. Em seguida, uma função do AWS Lambda recupera e retorna o conteúdo do bucket do S3.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Conteúdo estático do site hospedado em um bucket S3.

Limitações

- Os recursos nesse padrão devem estar em uma única região da AWS, mas podem ser provisionados em diferentes contas da AWS.
- Os limites se aplicam ao tamanho máximo de solicitação e resposta que a função do Lambda pode receber e enviar, respectivamente. Para obter mais informações, consulte Limites em Funções do Lambda como destino (documentação do Elastic Load Balancing).
- É importante encontrar um bom equilíbrio entre desempenho, escalabilidade, segurança e economia ao usar essa abordagem. Apesar da alta escalabilidade do Lambda, se o número

de invocações simultâneas do Lambda exceder a cota máxima, algumas solicitações serão limitadas. Para obter mais informações, consulte cotas do Lambda (documentação do Lambda). Você também precisa considerar os preços ao usar o Lambda. Para minimizar as invocações do Lambda, certifique-se de definir adequadamente o cache para a distribuição. CloudFront Para obter mais informações, consulte Otimizando o armazenamento em cache e a disponibilidade (CloudFront documentação).

Arquitetura

Pilha de tecnologias de destino

- CloudFront
- Amazon Virtual Private Cloud (Amazon VPC)
- Application Load Balancer
- Lambda
- Amazon S3

Arquitetura de destino

A imagem a seguir mostra a arquitetura sugerida quando você precisa usá-la CloudFront para servir conteúdo estático de um bucket do S3 por meio de uma VPC.

1. O cliente solicita o URL de CloudFront distribuição para obter um arquivo de site específico no bucket do S3.
2. CloudFront envia a solicitação para o AWS WAF. O AWS WAF filtra a solicitação usando a web ACLs aplicada à CloudFront distribuição. Se a solicitação for determinada como válida, o fluxo continuará. Se a solicitação for determinada como inválida, o cliente receberá um erro 403.
3. CloudFront verifica seu cache interno. Se houver uma chave válida correspondente à solicitação recebida, o valor associado será enviado de volta ao cliente como resposta. Caso contrário, o fluxo continua.
4. CloudFront encaminha a solicitação para a URL do Application Load Balancer especificado.
5. O Application Load Balancer tem um receptor associado a um grupo de destino baseado em uma função do Lambda. O Application Load Balancer invoca a função do Lambda.

6. A função do Lambda se conecta ao bucket do S3, executa uma operação `GetObject` nele e retorna o conteúdo como resposta.

Automação e escala

Para automatizar a implantação de conteúdo estático usando essa abordagem, crie pipelines de CI/CD para atualizar os buckets do Amazon S3 que hospedam sites.

A função do Lambda é escalada automaticamente para lidar com as solicitações simultâneas, dentro das cotas e limitações do serviço. Para obter mais informações, consulte Dimensionamento da função do Lambda e Cotas do Lambda (documentação do Lambda). Para os outros serviços e recursos da AWS, como CloudFront o Application Load Balancer, a AWS os escala automaticamente.

Ferramentas

- A Amazon CloudFront acelera a distribuição do seu conteúdo da web ao entregá-lo por meio de uma rede mundial de data centers, o que reduz a latência e melhora o desempenho.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Nesse padrão, você usa um Application Load Balancer provisionado por meio do Elastic Load Balancing para direcionar o tráfego para a função do Lambda.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Épicos

Use CloudFront para servir conteúdo estático do Amazon S3 por meio de uma VPC

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	Crie uma VPC para hospedar os recursos implantados nesse padrão, como o Application Load Balancer e a função do Lambda. Para obter instruções, consulte Criar uma VPC (document ação da Amazon VPC).	Arquiteto de nuvem
Crie uma ACL web do AWS WAF.	Crie uma ACL web do AWS WAF. Posteriormente nesse padrão, você aplica essa ACL da web à CloudFront distribui ção. Para obter instruções, consulte Criação de uma ACL da web (documentação do AWS WAF).	Arquiteto de nuvem
Criar a função do Lambda.	Crie a função do Lambda que serve o conteúdo estático hospedado no bucket do S3 como um site. Use o código fornecido na seção Informaçõ es adicionais desse padrão. Personalize o código para identificar o bucket do S3 de destino.	AWS geral
Upload a função do Lambda.	Insira o comando a seguir para carregar o código da função do Lambda em um	AWS geral

Tarefa	Descrição	Habilidades necessárias
	arquivo de arquivo .zip no Lambda. `aws lambda update-function-code \ --function-name \ --zip-file fileb://lambda-alb-s3-website.zip`	
Criar um Application Load Balancer.	Crie um Application Load Balancer voltado para a Internet que aponte para a função do Lambda. Para obter instruções, consulte Criar um grupo de destino para a função do Lambda (documentação do Elastic Load Balancing). Para criar uma configuração de alta disponibilidade, crie o Application Load Balancer e conecte-o a sub-redes privadas em diferentes zonas de disponibilidade.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie uma CloudFront distribui ção.	Crie uma CloudFront distribui ção que aponte para o Application Load Balancer que você criou. 1. Faça login no AWS Management Console e abra o CloudFront console em https://console.aws.amazon.com/cloudfront/v3/home. 2. Escolha Criar distribuição. 3. Na primeira página do assistente Criar distribui ção, na seção Web, escolha Começar a usar. 4. Especifique as configura ções para sua distribuição. Para obter mais informaçõ es, consulte Valores especificados ao criar ou atualizar uma distribuição. Observe o seguinte: a. Defina o Application Load Balancer como origem. b. Em Configurações de distribuição, escolha a web existente ACLs que você deseja aplicar por meio do AWS WAF. Para obter mais informações, consulte AWS WAF web ACL.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	5. Salve as alterações. 6. Depois de CloudFront criar sua distribuição, o valor da coluna Status da sua distribuição muda de InProgressImplantado. Se você optar por permitir a distribuição, ela estará pronta para processar solicitações depois que o status mudar para Implantado.	

Recursos relacionados

Documentação da AWS

- Otimizando o armazenamento em cache e a disponibilidade (documentação) CloudFront
- Funções do Lambda como destino (documentação do Elastic Load Balancing)
- Cotas Lambda (documentação Lambda)

Sites de serviços da AWS

- Application Load Balancer
- Lambda
- CloudFront
- Amazon S3
- AWS WAF
- Amazon VPC

Mais informações

Código

O exemplo de função do Lambda a seguir foi escrito em Node.js. Essa função do Lambda atua como um servidor web que executa uma operação `GetObject` em um bucket do S3 que contém os recursos do site.

```
/**

 * This is an AWS Lambda function created for demonstration purposes.

 * It retrieves static assets from a defined Amazon S3 bucket.

 * To make the content available through a URL, use an Application Load Balancer with a
 Lambda integration.
 *
 * Set the S3_BUCKET environment variable in the Lambda function definition.
 */

var AWS = require('aws-sdk');

exports.handler = function(event, context, callback) {

    var bucket = process.env.S3_BUCKET;
    var key = event.path.replace('/', '');

    if (key == '') {
        key = 'index.html';
    }

    // Fetch from S3
    var s3 = new AWS.S3();
    return s3.getObject({Bucket: bucket, Key: key},
       function(err, data) {

            if (err) {
                return err;
            }

            var isBase64Encoded = false;
            var encoding = 'utf8';

            if (data.ContentType.indexOf('image/') > -1) {
                isBase64Encoded = true;
                encoding = 'base64'
            }
```

```
            var resp = {
                statusCode: 200,
                headers: {
                    'Content-Type': data.ContentType,
                },
                body: new Buffer(data.Body).toString(encoding),
                isBase64Encoded: isBase64Encoded
            };

            callback(null, resp);
        }
    );
};
```

Mais padrões

- Verifique a versão de registro de acesso, HTTPS e TLS em uma CloudFront distribuição da Amazon
- Implemente um aplicativo baseado em gRPC em um cluster Amazon EKS e acesse-o com um Application Load Balancer
- Implemente controles de acesso preventivos baseados em atributos para sub-redes públicas
- Implante recursos em uma AWS Wavelength zona usando o Terraform
- Implemente as automações de segurança para a AWS WAF solução usando o Terraform
- Configure um roteador celular sem servidor para uma arquitetura baseada em células
- Use o Amazon Q Developer como assistente de codificação para aumentar sua produtividade
- Visualize registros e métricas do AWS Network Firewall usando o Splunk

Bancos de dados e armazenamento

Tópicos

- Bancos de dados
- Armazenamento e backup

Bancos de dados

Tópicos

- Acesse tabelas locais do Microsoft SQL Server a partir do Microsoft SQL Server na Amazon EC2 usando servidores vinculados
- Adicione HA ao Oracle PeopleSoft no Amazon RDS Custom usando uma réplica de leitura
- Avaliar o desempenho das consultas para migrar bancos de dados do SQL Server para o MongoDB Atlas na AWS
- Automatize implantações azul/verdes dos bancos de dados globais Amazon Aurora usando princípios de IaC
- Automatize tarefas de banco de dados na edição SQL Server Express em execução na Amazon EC2 usando AWS Lambda um Agendador de Tarefas
- Automatize o failover e o failback entre regiões usando o DR Orchestrator Framework
- Automatize a replicação de instâncias do Amazon RDS em Contas da AWS
- Faça backup automático dos bancos de dados SAP HANA usando o Systems Manager e EventBridge
- Gere automaticamente um modelo PyNamoDB e funções CRUD para o Amazon DynamoDB usando um aplicativo Python
- Bloqueie o acesso público ao Amazon RDS usando o Cloud Custodian
- Configurar o acesso entre contas ao Amazon DynamoDB
- Configurar o roteamento somente leitura em um grupo de disponibilidade Always On (Sempre ativo) no SQL Server na AWS
- Conecte-se usando um túnel SSH no pgAdmin
- Converta consultas JSON Oracle em SQL do banco de dados PostgreSQL
- Copie tabelas do Amazon DynamoDB entre contas usando AWS Backup
- Copiar tabelas do Amazon DynamoDB entre contas usando uma implementação personalizada
- Crie relatórios detalhados de custos e uso para o Amazon RDS e o Amazon Aurora
- Implante instâncias de cluster de failover do SQL Server na Amazon EC2 e na Amazon FSx usando o Terraform
- Emule workloads do Oracle RAC usando endpoints personalizados no Aurora PostgreSQL
- Habilite conexões criptografadas para instâncias de banco de dados PostgreSQL no Amazon RDS
- Criptografe uma instância de banco de dados Amazon RDS para PostgreSQL existente

- Aplique a marcação automática dos bancos de dados do Amazon RDS no lançamento
- Expressa o custo de uma tabela do DynamoDB para capacidade sob demanda
- Estime os custos de armazenamento de uma tabela do Amazon DynamoDB
- Estime o tamanho do mecanismo Amazon RDS para um banco de dados Oracle usando relatórios AWR
- Exporter tabelas do Amazon RDS para SQL Server para um bucket do S3 usando o AWS DMS
- Manipule blocos anônimos em instruções de SQL dinâmico no Aurora PostgreSQL
- Lide com funções sobrecarregadas do Oracle no Aurora compatível com PostgreSQL
- Ajude a aplicar a marcação no DynamoDB
- Implemente a recuperação de desastres entre regiões com o AWS DMS e o Amazon Aurora
- Migre funções e procedimentos do Oracle que tenham mais de 100 argumentos para o PostgreSQL
- Migre instâncias do banco de dados Amazon RDS para Oracle para outras contas que usam AMS
- Migrar variáveis de ligação Oracle OUT para um banco de dados PostgreSQL
- Migre o SAP HANA para a AWS usando o SAP HSR com o mesmo nome de host
- Migre o SQL Server para a AWS usando grupos de disponibilidade distribuídos
- Migre do Oracle 8i ou 9i para o Amazon RDS for Oracle usando o AWS DMS SharePlex
- Monitore o Amazon Aurora em busca de instâncias sem criptografia
- Monitore GoldenGate os logs do Oracle usando a Amazon CloudWatch
- Redefinir a plataforma do Oracle Database Enterprise Edition para o Standard Edition 2 no Amazon RDS para Oracle
- Replique bancos de dados de mainframe para AWS usando o Precisely Connect
- Agendar trabalhos para o Amazon RDS para PostgreSQL e Aurora PostgreSQL usando o Lambda e o Secrets Manager
- Envie notificações para uma instância de banco de dados Amazon RDS para SQL Server usando um servidor SMTP on-premises e o Database Mail
- Configure a recuperação de desastres para SAP no IBM Db2 na AWS
- Configure um pipeline de CI/CD para migração de banco de dados usando o Terraform
- Configure uma arquitetura de HA/DR para o Oracle E-Business Suite no Amazon RDS Custom com um banco de dados ativo em espera
- Configure a replicação de dados entre o Amazon RDS for MySQL e o MySQL na Amazon usando o GTID EC2

- Funções de transição para um PeopleSoft aplicativo Oracle no Amazon RDS Custom for Oracle
- Descarregue dados de um cluster do Amazon Redshift entre contas para o Amazon S3
- Padrões de migração de base de dados por workload
- Mais padrões

Acesse tabelas locais do Microsoft SQL Server a partir do Microsoft SQL Server na Amazon EC2 usando servidores vinculados

Criado por Tirumala Dasari (AWS) e Eduardo Valentim (AWS)

Resumo

Esse padrão descreve como acessar tabelas de banco de dados locais do Microsoft SQL Server executadas no Microsoft Windows, a partir de bancos de dados Microsoft SQL Server executados ou hospedados em instâncias Windows ou Linux do Amazon Elastic Compute Cloud EC2 (Amazon) usando servidores vinculados.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Amazon EC2 com Microsoft SQL Server em execução no Amazon Linux AMI (Amazon Machine Image)
- AWS Direct Connect entre o servidor local Microsoft SQL Server (Windows) e a instância Windows ou Linux EC2

Versões do produto

- SQL Server 2016 ou superior

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Microsoft SQL Server on-premises em execução no Windows
- Amazon EC2 com Microsoft SQL Server em execução na AMI do Windows ou AMI do Linux

Pilha de tecnologias de destino

- Amazon EC2 com Microsoft SQL Server em execução no Amazon Linux AMI
- Amazon EC2 com Microsoft SQL Server em execução na AMI do Windows

Arquitetura de banco de dados de origem e destino

Ferramentas

- O Microsoft SQL Server Management Studio (SSMS) é um ambiente integrado para o gerenciamento de uma infraestrutura do SQL Server. Ele fornece uma interface de usuário e um grupo de ferramentas com editores de scripts avançados que interagem com o SQL Server.

Épicos

Alterar o modo de autenticação para Windows para SQL Server no Windows SQL Server

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao Windows SQL Server por meio do SSMS.		DBA
Altere o modo de autentica ção para o Windows no SQL Server no menu de contexto (clique com o botão direito) da instância do Windows SQL Server.		DBA

Reinicie o serviço Windows MSSQL

Tarefa	Descrição	Habilidades necessárias
Reinicie o serviço SQL.	1. No SSMS Object Explorer, escolha a instância do SQL Server. 2. Abra o menu de contexto (clique com o botão direito). 3. Selecione Reiniciar.	DBA

Crie um novo login e escolha bancos de dados para acessar no Windows SQL Server

Tarefa	Descrição	Habilidades necessárias
Na guia Segurança, abra o menu de contexto (clique com o botão direito) de Login e selecione um novo login.		DBA
Na guia Geral, escolha Autenticação do SQL Server, digite um nome de usuário, digite a senha, confirme a senha e desmarque a opção de alterar a senha no próximo login.		DBA
Na guia Perfis do servidor, escolha Público.		DBA
Na guia Mapeamento do usuário, escolha o banco de dados e o esquema que você deseja acessar e, em seguida, destaque o banco de dados para selecionar as funções do banco de dados.	Selecione public e db_datareader para acessar os dados das tabelas do banco de dados.	DBA
Escolha OK para criar um usuário.		DBA

Adicionar IP do Windows SQL Server ao arquivo host Linux SQL Server

Tarefa	Descrição	Habilidades necessárias
Conecte-se à caixa Linux SQL Server por meio da janela do terminal.		DBA
Abra o the /etc/hosts arquivo e adicione o endereço IP da máquina Windows com o SQL Server.		DBA
Salve o arquivo de hosts.		DBA

Crie um servidor vinculado no Linux SQL Server

Tarefa	Descrição	Habilidades necessárias
Crie um servidor vinculado usando os procedimentos armazenados master.sys.sp_addlinkedserver e master.dbo.sp_addlinkedsrvlogin.	Para obter mais informações sobre o uso desses procedimentos armazenados, consulte a seção Informações adicionais.	DBA, Desenvolvedor

Verifique o servidor vinculado e os bancos de dados criados no SSMS

Tarefa	Descrição	Habilidades necessárias
No Linux SQL Server no SSMS, vá para Servidores vinculados e atualize.		DBA

Tarefa	Descrição	Habilidades necessárias
Expanda os servidores e catálogos vinculados criados no painel esquerdo.	Você verá os bancos de dados do SQL Server selecionados com tabelas e exibições.	DBA

Verifique se você pode acessar as tabelas do banco de dados do Windows SQL Server

Tarefa	Descrição	Habilidades necessárias
Na janela de consulta SSMS, execute a consulta: “select top 3 * from [sqllin] .dms_samp le_win.dbo.mlb_data”.	Observe que a cláusula FROM usa uma sintaxe de quatro partes: computer. database.schema.table (por exemplo, SELECT name "databases” FROM [sqllin] .master.sys.databa ses). SQL2 Em nosso exemplo, criamos um alias para SQL2 no arquivo hosts, para que você não precise inserir o nome real do NetBIOS entre colchetes. Se você usar os nomes NetBIOS reais, observe que a AWS usa como padrão nomes NetBIOS, como Win-xxxx, e o SQL Server exige colchetes para nomes com traços.	DBA, Desenvolvedor

Recursos relacionados

- Notas de lançamento do SQL Server no Linux

Mais informações

Usando procedimentos armazenados para criar servidores vinculados

O SSMS não oferece suporte à criação de servidores vinculados para Linux SQL Server, então você precisa usar esses procedimentos armazenados para criá-los:

```
EXEC master.sys.sp_addlinkedserver @server= N'SQLLIN' , @srvproduct= N'SQL Server'
EXEC master.dbo.sp_addlinkedsrvlogin
 @rmtsrvname=N'SQLLIN',@useself=N'False',@locallogin=NULL,@rmtuser=N'username',@rmtpassword='Te
```

Nota 1: insira as credenciais de login que você criou anteriormente no Windows SQL Server no procedimento armazenado. `master.dbo.sp_addlinkedsrvlogin`

Nota 2: `@server` o nome `SQLLIN` e o nome da entrada do arquivo host `172.12.12.4 SQLLIN` devem ser os mesmos.

Você pode usar esse processo para criar servidores vinculados nos seguintes cenários:

- Linux SQL Server para Windows SQL Server por meio de um servidor vinculado (conforme especificado nesse padrão)
- Windows SQL Server para Linux SQL Server por meio de um servidor vinculado
- Linux SQL Server para outro Linux SQL Server por meio de um servidor vinculado

Adicione HA ao Oracle PeopleSoft no Amazon RDS Custom usando uma réplica de leitura

Criado por sampath kathirvel (AWS)

Resumo

Para executar a solução Oracle PeopleSoft Enterprise Resource Planning (ERP) na Amazon Web Services (AWS), você pode usar o Amazon Relational Database Service (Amazon RDS) ou o Amazon RDS Custom for Oracle, que oferece suporte a aplicativos legados, personalizados e empacotados que exigem acesso ao sistema operacional e ao ambiente de banco de dados subjacentes. Para ver os principais fatores a serem considerados ao planejar uma migração, consulte as estratégias de migração do banco de dados Oracle nas Recomendações da AWS.

No momento em que este artigo foi escrito, o RDS Custom for Oracle não oferece suporte à opção Multi-AZ, que está disponível para o Amazon RDS para Oracle como uma solução de HA usando replicação de armazenamento. Em vez disso, esse padrão obtém HA usando um banco de dados em espera que cria e mantém uma cópia física do banco de dados primário. O padrão se concentra nas etapas para executar um banco de dados de PeopleSoft aplicativos no Amazon RDS Custom com HA usando o Oracle Data Guard para configurar uma réplica de leitura.

Esse padrão também altera a réplica de leitura para o modo somente leitura. Ter sua réplica de leitura no modo somente leitura oferece outros benefícios:

- Descarregando workloads somente para leitura do banco de dados principal
- Habilitando o reparo automático de blocos corrompidos recuperando blocos íntegros do banco de dados em espera usando o atributo Oracle Active Data Guard
- Usando o recurso Far Sync para manter o banco de dados remoto em espera sincronizado sem a sobrecarga de desempenho associada à transmissão de redo de log de longa distância.

Usar uma réplica no modo somente leitura requer a opção Oracle Active Data Guard, que tem um custo extra porque é um atributo licenciado separadamente do Oracle Database Enterprise Edition.

Pré-requisitos e limitações

Pré-requisitos

- Um PeopleSoft aplicativo existente no Amazon RDS Custom. Se você não tiver um aplicativo, consulte o padrão Migrate Oracle PeopleSoft to Amazon RDS Custom.

- Um único nível PeopleSoft de aplicativo. No entanto, você pode adaptar esse padrão para trabalhar com vários níveis de aplicativos.
- Amazon RDS Custom configurado com pelo menos 8 GB de espaço de troca.
- Uma licença de banco de dados Oracle Active Data Guard para converter a réplica de leitura em modo somente leitura e usá-la para transferir tarefas de geração de relatórios para o modo de espera. Para receber mais informações, consulte a Lista de Preços Comerciais de Tecnologia da Oracle.

Limitações

- Limitações gerais e configurações não suportadas para o RDS Custom for Oracle
- Limitações associadas às réplicas de leitura do Amazon RDS Custom para Oracle

Versões do produto

- Para versões do Oracle Database suportadas pelo Amazon RDS Custom, consulte RDS Custom for Oracle
- Para classes de instância de banco de dados do Oracle Database suportadas pelo Amazon RDS Custom, consulte Suporte a classes de instância de banco de dados do RDS Custom for Oracle.

Arquitetura

Pilha de tecnologias de destino

- Amazon RDS Custom para Oracle
- AWS Secrets Manager
- Oracle Active Data Guard
- PeopleSoft Aplicativo Oracle

Arquitetura de destino

O diagrama a seguir mostra uma instância de banco de dados do Amazon RDS Custom e uma réplica de leitura personalizada do Amazon RDS Custom. A réplica de leitura usa o Oracle Active Data Guard para replicar em outra zona de disponibilidade. Você também pode usar a réplica de leitura para descarregar o tráfego de leitura no banco de dados principal e para fins de geração de relatórios.

Para uma arquitetura representativa usando o Oracle PeopleSoft na AWS, consulte Configurar uma PeopleSoft arquitetura altamente disponível na AWS.

Ferramentas

Serviços da AWS

- O Amazon RDS Custom para Oracle é um serviço de banco de dados gerenciado para aplicações herdadas, personalizadas e em pacote que exigem acesso ao sistema operacional subjacente e ao ambiente de banco de dados.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente. Nesse padrão, você recupera as senhas de usuário do banco de dados do Secrets Manager for `RDS_DATAGUARD` com o nome secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Outras ferramentas

- O Oracle Data Guard ajuda você a criar, manter, gerenciar e monitorar bancos de dados em espera.

Práticas recomendadas

Para atingir um objetivo de zero perda de dados (RPO=0), use o modo de proteção Data Guard `MaxAvailability`, com a configuração de transporte de redo `SYNC+NOAFFIRM` para melhorar o desempenho. Para obter mais informações sobre como selecionar o modo de proteção do banco de dados, consulte a seção Informações adicionais.

Épicos

Criar a réplica de leitura

Tarefa	Descrição	Habilidades necessárias
Crie a réplica de leitura.	Para criar uma réplica de leitura da instância do Amazon RDS Custom, siga	DBA

Tarefa	Descrição	Habilidades necessárias
	as instruções na documentação do Amazon RDS e use a instância do Amazon RDS Custom que você criou (consulte a seção Pré-requisitos) como banco de dados de origem. Por padrão, a réplica de leitura do Amazon RDS Custom é criada como uma espera física e está no estado montado. Isso é intencional para garantir a conformidade com a licença do Oracle Active Data Guard. Esse padrão inclui código para configurar um banco de dados de contêiner multilocação (CDB) ou uma instância não CDB.	

Altere o modo de proteção do Oracle Data Guard para MaxAvailability

Tarefa	Descrição	Habilidades necessárias
Acesse a configuração do agente do Data Guard no banco de dados principal.	Neste exemplo, a réplica de leitura do Amazon RDS Custom é `RDS_CUSTOM_ORCL_D` para a instância sem CDB e `RDS_CUSTOM_RDSCDB_B` para a instância CDB. Os bancos de dados para não CDB são `orcl_a` (primário) e `orcl_d`	DBA

Tarefa	Descrição	Habilidades necessárias
	(em espera). Os nomes do banco de dados para CDB são `rdscdb_a` (primário) e `rdscdb_b` (em espera). Você pode se conectar à réplica de leitura personalizada do RDS diretamente ou por meio do banco de dados principal. Você pode encontrar o nome do serviço de rede do seu banco de dados no arquivo `tnsnames.ora` localizado no diretório `$ORACLE_HOME/network/admin`. O RDS Custom for Oracle preenche automaticamente essas entradas para seu banco de dados principal e suas réplicas de leitura. A senha do usuário `RDS_DATAGUARD` é armazenada no AWS Secrets Manager, com nome secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`. Para obter mais informações sobre como se conectar a uma instância personalizada do RDS usando a chave SSH (Secure Shell) recuperada do Secrets Manager, consulte Conectando-se à sua	

Tarefa	Descrição	Habilidades necessárias

	instância de banco de dados personalizada do RDS usando SSH.
	
	Para acessar a configuração do operador Oracle Data Guard por meio da linha de comando do Data Guard (`dgmgrl`), use o código a seguir.
	
	Não CDB
	
	`$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_D`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 22:44:49 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for information.`
	`Password:`
	`Connected to "ORCL_D"`
	`Connected as SYSDG.`
	`DGMGRL>`
	`DGMGRL> show database orcl_d`
	`Database - orcl_d`
	`Role: PHYSICAL STANDBY`
	`Intended State: APPLY-ON`	

Tarefa	Descrição	Habilidades necessárias
	Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 11.00 KByte/s Instance(s): ORCL SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 20:24:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "RDSCDB_B " Connected as SYSDG. DGMGRL> DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY	

Tarefa	Descrição	Habilidades necessárias
	Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL>	

Tarefa	Descrição	Habilidades necessárias

Altere a configuração de transporte de log conectando-se ao DGMGRL a partir do nó primário.	Altere o modo de transporte de log para `FastSync`, correspondente à configuração de transporte de redo `SYNC+NOAFFIRM` . Para garantir que você tenha configurações válidas após a troca de função, altere-as tanto para o banco de dados principal quanto para o banco de dados auxiliar.
	
	Não CDB
	
	`DGMGRL>`
	`DGMGRL> edit database orcl_d set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_d LogXptMode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL> edit database orcl_a set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_a logxptmode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL>`
	
	CDB
		DBA

Tarefa	Descrição	Habilidades necessárias
	`DGMGRL> edit database rdscdb_b set property logxptmode=fastsync;DGMGRL> edit database rdscdb_b set property logxptmode=fastsync; Property "logxptmode" updated DGMGRL> show database rdscdb_b LogXptMode; LogXptMode = 'fastsync' DGMGRL> edit database rdscdb_a set property logxptmode=fastsync; Property "logxptmode" updated DGMGRL> show database rdscdb_a logxptmode; LogXptMode = 'fastsync' DGMGRL>`	

Tarefa	Descrição	Habilidades necessárias
Altere o modo de proteção para MaxAvailability.	Altere o modo de proteção para `MaxAvailability` conectando-se ao `DGMGRL` a partir do nó primário. Não CDB `DGMGRL> edit configura tion set protectio n mode as maxavaila bility; Succeeded. DGMGRL> show configura tion; Configuration - rds_dg Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 38 seconds ago) DGMGRL>`  CDB  `DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database`	DBA

Tarefa	Descrição	Habilidades necessárias
	rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL>	

Altere o status da réplica de montagem para somente leitura e ative a aplicação de redo

Tarefa	Descrição	Habilidades necessárias
Pare a aplicação de redo para o banco de dados em espera.	A réplica de leitura é criada no modo `MOUNT` por padrão. Para abri-la no modo somente leitura, primeiro você precisa desativar a aplicação de redo conectando-se ao `DGMGRL` a partir do nó primário ou de espera. Não CDB DGMGRL> show database orcl_dDGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 11.00 KByte/s	DBA

Tarefa	Descrição	Habilidades necessárias
	Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> edit database orcl_d set state=app ly-off; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- OFF Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 42 seconds (computed 1 second ago) Average Apply Rate: (unknown) Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB DGMGRL> show configura tionDGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database	

Tarefa	Descrição	Habilidades necessárias
	rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> edit database rdscdb_b set state=apply-off; Succeeded. DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-OFF Transport Lag: 0 seconds (computed 1 second ago)	

Tarefa	Descrição	Habilidades necessárias
	Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: (unknown) Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS	

Tarefa	Descrição	Habilidades necessárias
Abra a instância de réplica de leitura no modo somente leitura.	Conecte-se ao banco de dados em espera usando a entrada TNS e abra-o no modo somente leitura conectando-se a ele a partir do nó primário ou em espera. Não CDB `$ sqlplus RDS_DATAG UARD@RDS_CUSTOM_OR CL_D as sysdg -bash-4.2$ sqlplus RDS_DATAGUARD@RDS_ CUSTOM_ORCL_D as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Fri Sep 30 23:00:14 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2020, Oracle. All rights reserved. Enter password: Last Successful login time: Fri Sep 30 2022 22:48:27 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.10.0.0.0 SQL> select open_mode from v$database; OPEN_MODE -------------------- MOUNTED SQL> alter database open read only;`	DBA

Tarefa	Descrição	Habilidades necessárias
	Database altered. SQL> select open_mode from v$database; OPEN_MODE -------------------- READ ONLY SQL> CDB -bash-4.2$ sqlplus C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Wed Jan 11 21:14:07 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2022, Oracle. All rights reserved. Enter password: Last Successful login time: Wed Jan 11 2023 21:12:05 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.16.0.0.0 SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- RDSCDB MOUNTED SQL> alter database open read only; Database altered.	

Tarefa	Descrição	Habilidades necessárias
	SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ---------- RDSCDB READ ONLY SQL>	

Tarefa	Descrição	Habilidades necessárias

Ative aplicação de redo na instância da réplica de leitura.	Ative aplicação de redo na instância da réplica de leitura usando DGMGRL do nó primário ou de espera.
	
	Não CDB
	
	`$ dgmgrl RDS_DATAG UARD@RDS_CUSTOM_OR CL_D`
	`DGMGRL for Linux:  Release 19.0.0.0.0 -  Production on Fri Sep  30 23:02:16 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982,  2019, Oracle and/or its  affiliates. All rights  reserved.`
	`Welcome to DGMGRL, type  "help" for informati on.`
	`Password:`
	`Connected to "ORCL_D"`
	`Connected as SYSDG.`
	`DGMGRL>`
	`edit database orcl_d set  state=apply-on;`
	`DGMGRL> edit database  orcl_d set state=app ly-on;`
	`Succeeded.`
	`DGMGRL> show database  orcl_d`
	`Database - orcl_d`
	`Role: PHYSICAL STANDBY`
	`Intended State: APPLY- ON`
		DBA

Tarefa	Descrição	Habilidades necessárias
	Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 496.00 KByte/s Real Time Query: ON Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 21:21:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_B" Connected as SYSDG.	

Tarefa	Descrição	Habilidades necessárias
	DGMGRL> edit database rdscdb_b set state=apply-on; Succeeded. DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 35.00 KByte/s Real Time Query: ON Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 16.00 KByte/s Real Time Query: ON Instance(s): RDSCDB	

Tarefa	Descrição	Habilidades necessárias
	`Database Status: SUCCESS DGMGRL>`	

Recursos relacionados

- Configurando o Amazon RDS como um PeopleSoft banco de dados Oracle (whitepaper da AWS)
- Guia do Oracle Data Guard Broker (documentação de referência da Oracle)
- Conceitos e administração do Data Guard (Documentação de referência do Oracle)

Mais informações

Selecione seu modo de proteção de banco de dados

O Oracle Data Guard fornece três modos de proteção para configurar seu ambiente Data Guard com base em seus requisitos de disponibilidade, proteção e desempenho. A tabela a seguir resume os três modos seguintes:

Modo de proteção	Configuração de transporte de redo	Descrição
MÁXIMA PERFORMANCE	`ASYNC`	Para transações que acontecem no banco de dados principal, os dados de redo são transmitidos e gravados de forma assíncrona no redo log do banco de dados em espera. Portanto, o impacto no desempenho é mínimo. `MaxPerformance` não é possível fornecer RPO=0 devido ao envio assíncrono de log.

PROTEÇÃO MÁXIMA	`SYNC+AFFIRM`	Para transações no banco de dados principal, os dados de redo são transmitidos e gravados de forma síncrona no redo log do banco de dados de espera no disco antes que a transação seja confirmada. Se o banco de dados em espera ficar indisponível, o banco de dados principal se desligará para garantir que as transaçõe s sejam protegidas.
DISPONIBILIDADE MÁXIMA	`SYNC+AFFIRM`	Isso é semelhante ao modo `MaxProtection` , exceto quando nenhuma confirmação é recebida do banco de dados em espera. Nesse caso, ele opera como se estivesse no modo `MaxPerformance` para preservar a disponibi lidade do banco de dados principal até que seja capaz de gravar seu fluxo de redo em um banco de dados em espera sincronizado novamente.

`SYNC+NOAFFIRM`	Para transações no banco de dados principal, o redo é transmitido de forma síncrona para o banco de dados em espera, e o principal espera somente pela confirmação de que o redo foi recebido no de espera, não de ter sido gravado no disco auxiliar. Esse modo, também conhecido como `FastSync`, pode fornecer um benefício de desempenho em detrimento da exposição potencial à perda de dados em um caso especial de várias falhas simultâneas.

As réplicas de leitura no RDS Custom for Oracle são criadas com o modo de proteção de desempenho máximo, que também é o modo de proteção padrão para o Oracle Data Guard. O modo de desempenho máximo fornece o menor impacto no desempenho do banco de dados principal, o que pode ajudá-lo a atender ao requisito de objetivo de ponto de recuperação (RPO) medido em segundos.

Para trabalhar para atingir um objetivo de zero perda de dados (RPO=0), você pode personalizar o modo de proteção do Oracle Data Guard para `MaxAvailability` com a configuração `SYNC +NOAFFIRM` de transporte de redo para melhor desempenho. Como as confirmações no banco de dados primário são reconhecidas somente depois que os vetores de redo correspondentes são transmitidos com sucesso para o banco de dados em espera, a latência da rede entre a instância primária e a réplica pode ser crucial para workloads sensíveis à confirmação. Recomendamos realizar testes de carga para sua workload para avaliar o impacto no desempenho quando a réplica de leitura é personalizada para ser executada no modo `MaxAvailability`.

A implantação da réplica de leitura na mesma zona de disponibilidade do banco de dados principal fornece menor latência de rede em comparação com a implantação da réplica de leitura em uma zona de disponibilidade diferente. No entanto, a implantação das réplicas primária e de leitura na

mesma zona de disponibilidade pode não atender aos requisitos de HA porque, no caso improvável de indisponibilidade da zona de disponibilidade, tanto a instância primária quanto a instância de réplica de leitura são afetadas.

Avaliar o desempenho das consultas para migrar bancos de dados do SQL Server para o MongoDB Atlas na AWS

Criado por Battulga Purevragchaa (AWS), Krishnakumar Sathyanarayana (US Inc) e Babu PeerIslands Srinivasan (MongoDB)

Resumo

Este padrão fornece orientação para carregar o MongoDB com dados quase reais e avaliar o desempenho das consultas do MongoDB o mais próximo possível do cenário de produção. A avaliação fornece informações para ajudar no planejamento de sua migração para o MongoDB a partir de um banco de dados relacional. O padrão usa o Gerador PeerIslands de Dados de Teste e o Analisador de Desempenho para testar o desempenho da consulta.

Esse padrão é particularmente útil para a migração do Microsoft SQL Server para o MongoDB, pois realizar transformações de esquema e carregar dados das instâncias atuais do SQL Server para o MongoDB pode ser muito complexo. Em vez disso, você pode carregar dados quase reais no MongoDB, entender o desempenho do MongoDB e ajustar o design do esquema antes de iniciar a migração efetiva.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Familiaridade com o MongoDB Atlas
- Esquema do MongoDB de destino
- Padrões de consulta típicos

Limitações

- Os tempos de carregamento de dados e o desempenho serão limitados pelo tamanho da instância do cluster MongoDB. Sugerimos que você escolha instâncias recomendadas para uso em produção para entender o desempenho no mundo real.
- PeerIslands Atualmente, o Gerador de Dados de Teste e o Analisador de Desempenho oferecem suporte somente a consultas e cargas de dados on-line. O processamento em lote off-line (por exemplo, carregamento de dados no MongoDB usando conectores Spark) ainda não é compatível.

- PeerIslands O gerador de dados de teste e o analisador de desempenho oferecem suporte às relações de campo dentro de uma coleção. Não é compatível com relacionamentos entre coleções.

Edições do produto

- Este padrão fornece suporte ao MongoDB Atlas e ao MongoDB Enterprise Advanced.

Arquitetura

Pilha de tecnologias de destino

- MongoDB Atlas ou MongoDB Enterprise Advanced

Arquitetura

PeerIslands O gerador de dados de teste e o analisador de desempenho são criados usando Java e Angular e armazenam os dados gerados no Amazon Elastic Block Store (Amazon EBS). A ferramenta consiste em dois fluxos de trabalho: geração de dados de testes e testes de desempenho.

- Na geração de dados de testes, você cria um modelo, que é a representação JSON do modelo de dados que precisa ser gerado. Depois de você criar o modelo, você pode gerar os dados em uma coleção de destino, conforme definido pela configuração de geração de carga.
- Nos testes de desempenho, você cria um perfil. Um perfil é um cenário de teste de vários estágios em que você pode configurar operações de criação, leitura, atualização e exclusão (CRUD), pipelines de agregação, a ponderação de cada operação e a duração de cada estágio. Depois de criar o perfil, você pode executar testes de desempenho no banco de dados de destino com base na configuração.

PeerIslands O Test Data Generator and Performance Analyzer armazena seus dados no Amazon EBS, para que você possa conectar o Amazon EBS ao MongoDB usando qualquer mecanismo de conexão compatível com o MongoDB, incluindo peering, listas de permissões e endpoints privados. Por padrão, a ferramenta não inclui componentes operacionais; no entanto, ela pode ser configurada com o Amazon Managed Service para Prometheus, Amazon Managed Grafana, Amazon e AWS Secrets Manager CloudWatch, se necessário.

Ferramentas

- PeerIslands O gerador de dados de teste e o analisador de desempenho incluem dois componentes. O componente Test Data Generator ajuda você a gerar dados reais altamente específicos do cliente com base no esquema do MongoDB. A ferramenta é totalmente orientada por interface de usuário com uma rica biblioteca de dados e pode ser usada para gerar rapidamente bilhões de registros no MongoDB. A ferramenta também fornece recursos para implementar relacionamentos entre campos no esquema do MongoDB. O componente Performance Analyzer ajuda você a gerar consultas e agregações altamente específicas do cliente, além de realizar testes de desempenho realistas no MongoDB. Você pode usar o Performance Analyzer para testar o desempenho do MongoDB com perfis de carga avançados e consultas parametrizadas para seu caso de uso específico.

Práticas recomendadas

Consulte os recursos a seguir:

- Práticas recomendadas de design do esquema do MongoDB (site do desenvolvedor do MongoDB)
- Práticas recomendadas de implantação do MongoDB Atlas na AWS (site do MongoDB)
- Conectando aplicativos com segurança a um plano de dados MongoDB Atlas com a AWS (publicação no blog da AWS) PrivateLink
- Guia de práticas recomendadas para desempenho do MongoDB (site do MongoDB)

Épicos

Entender seus dados de origem

Tarefa	Descrição	Habilidades necessárias
Entenda o espaço ocupado pelo banco de dados da origem do SQL Server atual.	Entenda o espaço ocupado por seu SQL Server atual. Para isso, execute consultas no esquema `INFORMATION` do banco de dados. Determine o número de tabelas e o tamanho de cada	DBA

Tarefa	Descrição	Habilidades necessárias
	uma delas. Analise o índice associado a cada tabela. Para obter mais informaçõ es sobre análise de SQL, consulte a postagem do blog SQL2Mongo: Data Migration Journey no PeerIslands site.	
Entenda o esquema de origem.	Determine o esquema da tabela e a representação comercial dos dados (por exemplo, códigos postais, nomes e moeda). Use seu diagrama de relaciona mento de entidades (ER) existente ou gere o diagrama ER a partir do banco de dados existente. Para obter mais informações, consulte a postagem do blog SQL2Mongo: Data Migration Journey no PeerIslands site.	DBA

Tarefa	Descrição	Habilidades necessárias
Entenda os padrões de consulta.	Documente as dez principais consultas SQL que você usa. Você pode usar as tabelas performance_schema.events_statements_summary_by_digest que estão disponíveis no banco de dados para entender as principais consultas. Para obter mais informações, consulte a postagem do blog SQL2Mongo: Data Migration Journey no PeerIslands site.	DBA
Entenda os compromissos de SLA.	Documente os contratos de nível de serviço (SLAs) de destino para operações de banco de dados. As medidas típicas incluem latência de consultas e consultas por segundo. As medidas e suas metas geralmente estão disponíveis em documentos de requisitos não funcionais (NFR).	DBA

Definir o esquema do MongoDB

Tarefa	Descrição	Habilidades necessárias
Defina o esquema de destino.	Defina várias opções para o esquema de destino do MongoDB. Para obter mais informações sobre Esquemas	Engenheiro do MongoDB

Tarefa	Descrição	Habilidades necessárias
	consulte a documentação do MongoDB. Considere as práticas recomendadas e os padrões de design com base nas relações da tabela. Consulte Exemplos e padrões de modelos de dados na documentação do MongoDB para obter detalhes.	
Defina padrões de consulta de destino.	Defina consultas e pipelines de agregação do MongoDB. Essas consultas são equivalentes às principais consultas que você registrou para seu workload do SQL Server. Para entender como estruturar pipelines de agregação do MongoDB, consulte a documentação do MongoDB.	Engenheiro do MongoDB
Defina o tipo de instância do MongoDB.	Determine o tamanho da instância que você planeja usar para testes. Para obter orientação, consulte a Documentação do MongoDB.	Engenheiro do MongoDB

Preparar o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Configure o cluster MongoDB Atlas.	Para configurar um cluster MongoDB na AWS, siga as instruções na documentação do MongoDB.	Engenheiro do MongoDB

Tarefa	Descrição	Habilidades necessárias
Criar usuários no banco de dados de destino.	Configure o cluster MongoDB Atlas para acesso e segurança de rede seguindo as instruções na documentação do MongoDB.	Engenheiro do MongoDB
Crie funções apropriadas na AWS e configure o controle de acesso baseado em funções para o Atlas.	Se necessário, configure usuários adicionais seguindo as instruções na documentação do MongoDB. Configure a autenticação e a autorização por meio de funções da AWS.	Engenheiro do MongoDB
Configure o Compass para acesso ao MongoDB Atlas.	Configure o utilitário de GUI do MongoDB Compass para facilitar a navegação e o acesso.	Engenheiro do MongoDB

Configurar a carga base usando o Test Data Generator

Tarefa	Descrição	Habilidades necessárias
Instale o Test Data Generator.	Instale o PeerIsland Test Data Generator em seu ambiente.	Engenheiro do MongoDB
Configure o Test Data Generator para gerar os dados apropriados.	Crie um modelo usando a biblioteca de dados para gerar dados específicos para cada campo no esquema do MongoDB. Para obter mais informações, veja o vídeo MongoDB Data Generator & Perf. Analyzer.	Engenheiro do MongoDB

Tarefa	Descrição	Habilidades necessárias
Escale horizontalmente o Test Data Generator para gerar a carga necessária.	Use o modelo que você criou para iniciar a geração de carga em relação à coleção de destino configurando o paralelismo necessário. Determine os prazos e a escala para gerar os dados necessários.	Engenheiro do MongoDB
Valide a carga no MongoDB Atlas.	Verifique os dados carregados no MongoDB Atlas.	Engenheiro do MongoDB
Gere os índices necessários no MongoDB.	Defina índices conforme necessário, com base nos padrões de consulta. Para obter as melhores práticas, consulte a documentação da MongoDB.	Engenheiro do MongoDB

Realizar testes de desempenho

Tarefa	Descrição	Habilidades necessárias
Configure perfis de carga no Performance Analyzer.	Crie um perfil de teste de desempenho no Performan ce Analyzer configurando consultas específicas e sua ponderação correspondente, duração da execução do teste e estágios. Para obter mais informações, veja o vídeo MongoDB Data Generator & Perf. Analyzer.	Engenheiro do MongoDB

Tarefa	Descrição	Habilidades necessárias
Execute os testes de desempenho.	Use o perfil que você criou para iniciar o teste em relação à coleção de destino configurando o paralelismo necessário. Escale horizontalmente a ferramenta de teste de desempenho para executar consultas no MongoDB Atlas.	Engenheiro do MongoDB
Registre os resultados dos testes.	Registre a latência P95 e P99 para as consultas.	Engenheiro do MongoDB
Ajuste seu esquema e seus padrões de consulta.	Modifique índices e padrões de consulta para resolver quaisquer problemas de desempenho.	Engenheiro do MongoDB

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.	Exclua todos os recursos temporários que você usou para o Test Data Generator and Performance Analyzer.	Administrador da AWS
Atualize os resultados dos testes de desempenho.	Entenda o desempenho de consultas do MongoDB e compare-o com o seu. SLAs Se necessário, ajuste o esquema do MongoDB e execute o processo novamente.	Engenheiro do MongoDB

Tarefa	Descrição	Habilidades necessárias
Conclua o projeto.	Feche o projeto e forneça feedback.	Engenheiro do MongoDB

Recursos relacionados

- GitHub repositório: S3toAtlas
- Esquema: design do esquema do MongoDB
- Pipelines de agregação: pipelines de agregação do MongoDB
- Dimensionamento do MongoDB Atlas: seleção de camadas de dimensionamento
- Vídeo: Data Generator & Perf. Analyzer do MongoDB
- Referências: documentação do MongoDB
- Tutoriais: Guia do desenvolvedor do MongoDB, MongoDB Jumpstart
- AWS Marketplace: MongoDB Atlas no AWS Marketplace
- Soluções de parceiros da AWS: MongoDB Atlas na implantação de referência da AWS

Recursos adicionais:

- Análise SQL
- Fóruns da comunidade de desenvolvedores do MongoDB
- Perguntas sobre ajuste de desempenho do MongoDB
- Análise operacional com Atlas e Redshift
- Modernização de aplicativos com o MongoDB Atlas e o AWS Elastic Beanstalk

Automatize implantações azul/verdes dos bancos de dados globais Amazon Aurora usando princípios de IaC

Criado por Ishwar Chauthaiwale (AWS), ANKIT JAIN (AWS) e Ramu Jagini (AWS)

Resumo

Gerenciar atualizações de bancos de dados, migrações ou esforços de escalabilidade pode ser um desafio para organizações que executam cargas de trabalho críticas em bancos de dados globais do Amazon Aurora. Garantir que essas operações sejam realizadas sem interrupções, sem tempo de inatividade, é essencial para manter a disponibilidade do serviço e evitar interrupções para seus usuários.

Uma blue/green deployment strategy offers a solution to this challenge by allowing you to run two identical environments concurrently: blue (the current environment) and green (the new environment). A blue/green estratégia permite que você implemente mudanças, realize testes e alterne o tráfego entre ambientes com o mínimo de risco e tempo de inatividade.

Esse padrão ajuda você a automatizar o processo de implantação azul/verde dos bancos de dados globais Aurora usando princípios de infraestrutura como código (IaC). Ele usa AWS CloudFormation, AWS Lambda, e o Amazon Route 53 para simplificar as implantações azul/verde. Para melhorar a confiabilidade, ele usa identificadores de transação globais (GTIDs) para replicação. A replicação baseada em GTID fornece melhor consistência de dados e recursos de failover entre ambientes em comparação com a replicação de log binário (binlog).

> **Note**
>
> Esse padrão pressupõe que você esteja usando um cluster de banco de dados global da Edição compatível com o Aurora MySQL. Se você estiver usando o Aurora compatível com o PostgreSQL em vez disso, use os equivalentes PostgreSQL dos comandos do MySQL.

Seguindo as etapas desse padrão, você pode:

- Provisione um banco de dados global Aurora verde: usando CloudFormation modelos, você cria um ambiente verde que reflete seu ambiente azul existente.
- Configurar a replicação baseada em GTID: você configura a replicação GTID para manter os ambientes azul e verde sincronizados.

- Alterne o tráfego sem problemas: você usa o Route 53 e o Lambda para alternar automaticamente o tráfego do ambiente azul para o verde após a sincronização completa.
- Finalize a implantação: você valida que o ambiente ecológico está totalmente operacional como banco de dados principal e, em seguida, interrompe a replicação e limpa todos os recursos temporários.

A abordagem nesse padrão fornece os seguintes benefícios:

- Reduz o tempo de inatividade durante atualizações ou migrações críticas do banco de dados: a automação garante uma transição suave entre ambientes com o mínimo de interrupção do serviço.
- Permite reversões rápidas: se surgir um problema depois que o tráfego for transferido para o ambiente verde, você poderá reverter rapidamente para o ambiente azul e manter a continuidade do serviço.
- Melhora os testes e a verificação: o ambiente verde pode ser totalmente testado sem afetar o ambiente azul ativo, o que reduz a probabilidade de erros na produção.
- Garante a consistência dos dados: a replicação baseada em GTID mantém seus ambientes azul e verde sincronizados, o que evita perda de dados ou inconsistências durante a migração.
- Mantém a continuidade dos negócios: automatizar suas implantações azul/verdes ajuda a evitar longas interrupções e perdas financeiras, mantendo seus serviços disponíveis durante atualizações ou migrações.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Um cluster de banco de dados global de origem compatível com o Aurora MySQL (ambiente azul). Os bancos de dados globais fornecem uma configuração multirregional para alta disponibilidade e recuperação de desastres. Para obter instruções sobre como configurar um cluster de banco de dados global, consulte a documentação do Aurora.
- Replicação baseada em GTID ativada no cluster de origem.

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Versões do produto

- Compatível com Aurora MySQL 8.0 ou posterior

Arquitetura

O diagrama ilustra o seguinte:

- Configuração de banco de dados global: um cluster de banco de dados global Aurora é implantado estrategicamente em dois. Regiões da AWS Essa configuração permite distribuição geográfica e redundância regional para recursos aprimorados de recuperação de desastres.
- Replicação da região primária para a secundária: o mecanismo de replicação lógica garante a sincronização perfeita dos dados da região primária para a região secundária. Essa replicação mantém a consistência dos dados com latência mínima em distâncias geográficas.
- Replicação baseada em GTID entre clusters: a replicação baseada em GTID mantém a consistência transacional e o fluxo de dados ordenado entre o cluster principal azul e o cluster primário verde e garante a sincronização confiável dos dados.
- Replicação azul primária para secundária: a replicação lógica estabelece um pipeline de dados robusto entre o cluster principal azul e seu cluster secundário. Essa replicação permite a sincronização contínua de dados e a alta disponibilidade.
- Configuração de DNS do Route 53: os registros da zona hospedada do Route 53 gerenciam a resolução de DNS para todos os endpoints do banco de dados de cluster azul e verde. Essa configuração fornece mapeamento contínuo de endpoints e permite o roteamento eficiente do tráfego durante cenários de failover.

Ferramentas

Serviços da AWS

- O Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado criado para a nuvem e compatível com o MySQL e o PostgreSQL.

- AWS CloudFormationajuda você a modelar e configurar seus AWS recursos para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando nos aplicativos que são executados em AWS. Você cria um modelo que descreve todos os AWS recursos que você deseja e se CloudFormation encarrega de provisionar e configurar esses recursos para você.
- AWS Lambdaé um serviço de computação que oferece suporte à execução de código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.

Práticas recomendadas

Recomendamos que você analise minuciosamente a AWS documentação para aprofundar sua compreensão da estratégia de implantação azul/verde, da replicação baseada em GTID e das políticas de roteamento ponderado no Route 53. Esse conhecimento é crucial para implementar e gerenciar com eficácia suas migrações de banco de dados, garantindo a consistência dos dados e otimizando o roteamento de tráfego. Ao obter uma compreensão abrangente desses AWS recursos e das melhores práticas, você estará mais bem equipado para lidar com futuras atualizações, minimizar o tempo de inatividade e manter um ambiente de banco de dados resiliente e seguro.

Para obter diretrizes sobre como usar o Serviços da AWS para esse padrão, consulte a AWS documentação a seguir:

- Melhores práticas com o Amazon Aurora MySQL
- AWS CloudFormation melhores práticas
- Práticas recomendadas para trabalhar com AWS Lambda funções
- Melhores práticas para o Amazon Route 53

Épicos

Crie o ambiente verde

Tarefa	Descrição	Habilidades necessárias
Crie um backup instantâneo a partir do cluster azul.	Em uma implantação azul/verde, o ambiente verde representa uma versão nova	DBA

Tarefa	Descrição	Habilidades necessárias
	e idêntica do seu ambiente de banco de dados atual (azul). Você usa o ambiente ecológico para testar atualizações com segurança, validar alterações e garantir a estabilidade antes de mudar o tráfego de produção. Ele atua como um ponto de partida para a implementação de alterações no banco de dados com o mínimo de interrupção no ambiente ativo. Para criar um ambiente ecológico, primeiro você cria um snapshot do cluster primário (azul) em seu banco de dados global compatível com o Aurora MySQL. Esse instantâneo serve como base para a criação do ambiente verde. Para criar um instantâneo: 1. Faça login no console do Amazon Relational Database Service (Amazon RDS) AWS Management Console e abra o console do Amazon Relational Database Service (Amazon RDS). 2. Selecione seu cluster primário (azul).	

Tarefa	Descrição	Habilidades necessárias
	3. Escolha Ações, Tirar instantâneo. 4. Forneça um nome para o instantâneo, como `blue-green-demo`, e inicie o processo de backup. Como alternativa, você pode usar o AWS Command Line Interface (AWS CLI) para criar o instantâneo: `aws rds create-db-cluster-snapshot --db-cluster-snapshot-identifier blue-green-demo --db-cluster-identifier ex-global-cluster --region eu-west-1` Certifique-se de que o instantâneo seja concluído com êxito antes de prosseguir para a próxima etapa.	

Tarefa	Descrição	Habilidades necessárias
Gere o CloudFormation modelo para seu banco de dados global e seus recursos.	O gerador CloudFormation IaC ajuda você a gerar CloudFormation modelos a partir de AWS recursos existentes. Use esse recurso para criar um CloudFormation modelo para seu banco de dados global atual compatível com o Aurora MySQL e seus recursos associados. Esse modelo configura grupos de sub-redes, grupos de segurança, grupos de parâmetros e outras configurações. 1. Siga as instruções na CloudFormation documentação para navegar até a ferramenta e conectá-la ao seu AWS ambiente. 2. Selecione seu banco de dados global do Aurora e os recursos associados para gerar o modelo.	DBA

Tarefa	Descrição	Habilidades necessárias
Modifique o CloudFormation modelo para o ambiente verde.	Personalize o CloudFormation modelo para refletir as configurações do ambiente verde. Isso inclui atualizar nomes e identificadores de recursos para garantir que o ambiente verde opere independentemente do cluster azul. 1. Atualize as `DBInstanceIdentifier` propriedades `DBClusterIdentifier` e para representar o ambiente verde. 2. Modifique outros nomes de recursos (por exemplo, grupos de sub-rede e grupos de segurança) para evitar conflitos com o ambiente azul existente. 3. Ative a replicação baseada em GTID no modelo configurando os parâmetros corretos, conforme descrito na documentação do Aurora. 4. Altere a `SnapshotIdentifier` propriedade para especificar Região da AWS o ID da sua conta e o nome do snapshot da etapa anterior:	DBA

Tarefa	Descrição	Habilidades necessárias
	`SnapshotIdentifier: arn:aws:rds:<region>:<account-id>:snapshot:<snapshot-name>` **Note** Se você usar a `SnapshotIdentifier` propriedade para restaurar um cluster de banco de dados, evite especificar propriedades como `GlobalClusterIdentifier` `MasterUsername` , ou `MasterUserPassword` .	

Tarefa	Descrição	Habilidades necessárias
Implante a CloudFormation pilha para criar recursos para o ambiente verde.	Nesta etapa, você implanta o CloudFormation modelo personalizado para criar os recursos para o ambiente verde. Para implantar a CloudFormation pilha: 1. Abra o console de AWS CloudFormation. 2. No canto superior direito, escolha Criar pilha, Com novos recursos (padrão). 3. Faça o upload do CloudFormation modelo modificado ou especifique o URL do modelo. Escolha Próximo. 4. Insira um nome de pilha`GreenClusterStack`, como, e forneça os parâmetros necessários (por exemplo,`GreenClusterIdentifier`). Escolha Próximo. 5. Configure opções adicionais de pilha conforme necessário e marque a caixa para confirmar que isso CloudFormation pode criar recursos AWS Identity	DBA

Tarefa	Descrição	Habilidades necessárias
	and Access Management (IAM). Escolha Próximo. 6. Revise os detalhes da pilha. 7. Selecione Enviar. CloudFormation inicia o processo de criação de recursos ambientais verdes. Esse processo pode levar alguns minutos para ser concluído.	

Tarefa	Descrição	Habilidades necessárias
Valide a CloudFormation pilha e os recursos.	Quando a implantação da CloudFormation pilha estiver concluída, você precisará verificar se o ambiente ecológico foi criado com sucesso: 1. Na seção Saídas da CloudFormation pilha, verifique os endpoints do cluster do banco de dados e da instância do banco de dados para verificar a configuração correta. 2. Abra o console do Amazon RDS e confirme se o novo cluster de banco de dados Aurora (ambiente verde) está disponível. 3. Certifique-se de que todos os recursos associados, como sub-redes e grupos de segurança, tenham sido criados e vinculados ao ambiente verde. Após a verificação, seu ambiente verde está pronto para configuração adicional , incluindo a replicação do ambiente azul.	DBA

Configurar a replicação baseada em GTID

Tarefa	Descrição	Habilidades necessárias
Verifique as configurações do GTID no cluster azul.	GTIDs forneça um método altamente confiável para replicar dados entre seus ambientes azul e verde. A replicação baseada em GTID oferece uma abordagem resiliente e simplificada ao atribuir um identificador exclusivo a cada transação no ambiente azul. Esse método garante que a sincronização de dados entre ambientes seja perfeita, consistente e mais fácil de gerenciar do que a replicação tradicional de binlogs. Antes de configurar a replicação, você precisa garantir que a replicação baseada em GTID esteja habilitada corretamente no cluster azul. Essa etapa garante que cada transação no ambiente azul seja rastreada de forma exclusiva e possa ser replicada no ambiente verde. Para confirmar se o GTID está ativado: 1. No console do Amazon RDS, revise o grupo de	DBA

Tarefa	Descrição	Habilidades necessárias
	parâmetros atribuído ao cluster azul. 2. Verifique se os seguintes parâmetros estão definidos: • `gtid-mode = ON` • `enforce_gtid_consistency = ON` Essas configurações permitem o rastreamento GTID para todas as transações futuras no ambiente azul. Depois de confirmar essas configurações, você pode começar a configurar a replicação.	

Tarefa	Descrição	Habilidades necessárias
Crie um usuário de replicação.	Para replicar dados do ambiente azul para o ambiente verde, você precisa criar um usuário de replicaçã o dedicado no cluster azul. Esse usuário será responsáv el por gerenciar o processo de replicação. Para configurar o usuário de replicação: 1. Conecte-se ao cluster azul usando um cliente MySQL. 2. Execute os seguintes comandos para criar o usuário de replicação: `CREATE USER 'repl_use r'@'%' IDENTIFIED BY 'repl_password'; GRANT REPLICATI ON SLAVE ON . TO 'repl_user'@'%'; FLUSH PRIVILEGES;` Agora, esse usuário tem as permissões necessárias para replicar dados entre os dois ambientes.	DBA

Tarefa	Descrição	Habilidades necessárias
Configure a replicação baseada em GTID no cluster verde.	A próxima etapa é configurar o cluster verde para replicação baseada em GTID. Essa configuração garante que o ambiente verde espelhe continuamente todas as transações que acontecem no ambiente azul. Para configurar o cluster verde: 1. Conecte-se ao cluster verde usando um cliente MySQL. 2. Execute o comando a seguir para configurar a replicação: `CHANGE MASTER TO MASTER_HOST='blue-cluster-endpoint', MASTER_USER='repl_user', MASTER_PASSWORD='repl_password', MASTER_AUTO_POSITION=1;` em que: • `blue-cluster-endpoint` Substitua pelo endpoint do seu cluster azul. • A `MASTER_AUTO_POSITION=1` configuração instrui o MySQL a usar a	DBA

Tarefa	Descrição	Habilidades necessárias
	replicação baseada em GTID. Ele posiciona automaticamente o cluster verde para replicar as transaçõe s do cluster azul sem precisar rastrear registros e posições manualmente.	
Inicie a replicação no cluster verde.	Agora você pode iniciar o processo de replicação. No cluster verde, execute o comando: `START SLAVE;` Isso permite que o ambiente verde comece a sincronizar dados e a receber e aplicar transações do ambiente azul.	DBA

Tarefa	Descrição	Habilidades necessárias
Verifique o processo de replicação.	Para verificar se o ambiente verde está replicando com precisão os dados do cluster azul: 1. Execute o comando a seguir no cluster verde para verificar o status da replicação: `SHOW SLAVE STATUS\G;` 2. Analise a saída para verificar o seguinte: • `Slave_IO_Running = Yes` • `Slave_SQL_Running = Yes` • Os `Executed_Gtid_Set` valores `Retrieved_Gtid_Set` up-to-date e são sincronizados com o cluster azul. • Não há erros de replicação no `Last_Error` campo. Se todos os indicadores estiverem corretos, a replicação baseada em GTID funcionará sem problemas e o ambiente verde estará	DBA

Tarefa	Descrição	Habilidades necessárias
	totalmente sincronizado com o ambiente azul.	

Mudar o tráfego do cluster azul para o verde

Tarefa	Descrição	Habilidades necessárias
Configure as políticas de roteamento ponderado do Route 53.	Depois de verificar a consistência dos dados entre os ambientes azul e verde, você pode alternar o tráfego do cluster azul para o cluster verde. Essa transição deve ser suave, minimizar o tempo de inatividade e garantir a integridade do banco de dados do seu aplicativo. Para atender a esses requisitos, você pode usar o Route 53 para roteamento de DNS e o Lambda para automatizar a troca de tráfego. Além disso, um plano de reversão bem definido garante que você possa reverter para o cluster azul em caso de problemas. A primeira etapa é configurar o roteamento ponderado no Route 53. O roteamento ponderado permite controlar a distribuição do tráfego entre os clusters azul e verde e transferir gradualmente o	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	tráfego de um ambiente para outro. Para configurar o roteamento ponderado: 1. Abra o console do Route 53 e escolha sua zona hospedada. 2. Crie dois registros DNS (CNAMEs) para o banco de dados: um registro para o cluster azul e um registro para o cluster verde. 3. Atribua pesos iniciais: • Defina um peso inicial baixo (como 5%) para que o cluster verde envie uma pequena parte do tráfego para teste. • Defina um peso maior (como 95%) para o cluster azul, para que ele retenha a maior parte do tráfego. Essa configuração permite que você realize uma transição gradual que reduz o risco e oferece suporte a testes em tempo real antes de você mudar totalmente. Para obter mais informações sobre políticas de roteament	

Tarefa	Descrição	Habilidades necessárias
	o ponderado, consulte a documentação do Route 53.	

Tarefa	Descrição	Habilidades necessárias

Implante uma função Lambda para monitorar o atraso na replicação.	Para garantir que o ambiente verde esteja totalmente sincronizado com o ambiente azul, implante uma função Lambda que monitore o atraso na replicação entre os clusters. Essa função pode verificar o status da replicaçã o, especificamente a métrica Seconds_Behind_Master, para determinar se o cluster verde está pronto para lidar com todo o tráfego.
	
	Aqui está um exemplo da função Lambda que você pode usar:
	
	`import boto3`
	
	`def check_replication_lag(event, context):`
	`client = boto3.client('rds')`
	`response = client.describe_db_instances(DBInstanceIdentifier='green-cluster-instance')`
	`replication_status = response['DBInstances'][0]['ReadReplicaDBInstanceIdentifiers']`
	`if replication_status:`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>lag = replicati
	on_status[0]['Repl
	icationLag']
	return lag
	return -1</pre>
	Essa função verifica o atraso de replicação e retorna o valor. Se o atraso for zero, o cluster verde estará totalment e sincronizado com o cluster azul.	

Tarefa	Descrição	Habilidades necessárias

Automatize o ajuste de peso do DNS usando o Lambda.	Quando o atraso de replicaçã o chegar a zero, é hora de mudar todo o tráfego para o cluster verde. Você pode automatizar essa transição usando outra função Lambda que ajusta os pesos do DNS no Route 53 para direcionar 100% do tráfego para o cluster verde.
	
	Aqui está um exemplo de uma função Lambda que automatiz a a troca de tráfego:
	
	`import boto3`
	
	`def switch_traffic(eve nt, context):`
	`route53 = boto3.cli ent('route53')`
	`lag = check_rep lication_lag(event, context)`
	`if lag == 0:`
	`response = route53.change_res ource_record_sets(`
	`HostedZon eId='YOUR_HOSTED_Z ONE_ID',`
	`ChangeBat ch={`
	`'Changes': [`
	`{`
	`'Action': 'UPSERT',`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	'ResourceRecordSet': {
	'Name': 'db.example.com',
	'Type': 'CNAME',
	'SetIdentifier': 'GreenCluster',
	'Weight': 100,
	'TTL': 60,
	'ResourceRecords': [{'Value': 'green-cluster-endpoint'}]
	}
	},
	{
	'Action': 'UPSERT',
	'ResourceRecordSet': {
	'Name': 'db.example.com',
	'Type': 'CNAME',
	'SetIdentifier': 'BlueCluster',
	'Weight': 0,
	'TTL': 60,
	'ResourceRecords':	

Tarefa	Descrição	Habilidades necessárias

```
 [{'Value': 'blue-clu
ster-endpoint'}]

 }
                    }
                ]
            }
        )
        return response
```

Essa função verifica o atraso de replicação e atualiza os pesos do DNS do Route 53 quando o atraso é zero para mudar totalmente o tráfego para o cluster verde.

> **Note**
>
> Durante o processo de transição, se o cluster azul tiver tráfego intenso de gravação, considere pausar temporari amente as operações de gravação durante a transição. Isso garante que a replicação seja atualizada e evita inconsistências de dados entre os clusters azul e verde.

Tarefa	Descrição	Habilidades necessárias
Verifique o interruptor de tráfego.	Depois que a função Lambda ajustar os pesos do DNS, você deve verificar se todo o tráfego foi direcionado para o cluster verde e se a troca foi bem-sucedida. Para verificar: 1. Monitore os registros DNS do Route 53 para confirmar se o tráfego está sendo direcionado para o cluster verde. Para obter mais informações, consulte a documentação do Route 53. 2. Verifique o desempenho do aplicativo confirmando que os usuários estão sendo atendidos pelo ambiente verde. 3. Verifique as conexões do banco de dados para confirmar se o cluster verde está processando todas as solicitações do banco de dados. 4. Monitore CloudWatch as métricas da Amazon em busca de sinais de latência, atraso na replicaçã o ou degradação do desempenho. Para obter	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	mais informações, consulte a documentação do Aurora. Se tudo estiver funcionando conforme o esperado, a mudança de tráfego estará concluída.	

Tarefa	Descrição	Habilidades necessárias
Se você encontrar algum problema, reverta as alterações.	Ter um plano de reversão é fundamental no caso de surgirem problemas após a mudança de tráfego. Veja como reverter rapidamente para o cluster azul, se necessário: 1. Reverta os pesos do DNS no Route 53: use a mesma função Lambda ou ajuste manualmente os pesos do DNS do Route 53 para direcionar 100% do tráfego de volta para o cluster azul. 2. Monitore o desempenho do aplicativo: monitore imediatamente os registros, CloudWatch as métricas e o desempenho do banco de dados do aplicativo para confirmar se a mudança para o ambiente azul resolveu os problemas. 3. Identifique e resolva problemas: investigue e resolva quaisquer problemas com o cluster verde antes de tentar outra troca de tráfego. Ao implementar esse plano de reversão, você pode garantir o mínimo de interrupção para	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	seus usuários no caso de problemas inesperados.	

Valide e interrompa a replicação baseada em GTID

Tarefa	Descrição	Habilidades necessárias
Pare a replicação baseada em GTID no cluster verde.	Depois de mudar o tráfego do ambiente azul para o ambiente verde, você deve validar o sucesso da transição e garantir que o cluster verde esteja funcionando conforme o esperado. Além disso, a replicação baseada em GTID entre os clusters azul e verde deve ser interromp ida, porque o ambiente verde agora serve como banco de dados principal. A conclusão dessas tarefas garante que seu ambiente esteja seguro, simplificado e otimizado para operações contínuas. Para interromper a replicação: 1. Use um cliente MySQL para se conectar ao cluster verde. 2. Execute o seguinte comando SQL para interromper o processo de replicação no cluster verde:	DBA

Tarefa	Descrição	Habilidades necessárias

	`STOP SLAVE;`
	3. (Opcional) Se desejar, você pode redefinir a configuração de replicação para limpar todas as configurações de replicação residuais:
	`RESET SLAVE ALL;`
	Quando você interrompe a replicação, o cluster verde se torna totalmente independente e opera como o principal ambiente de banco de dados para suas cargas de trabalho.	

Tarefa	Descrição	Habilidades necessárias
Limpar recursos.	A limpeza de todos os recursos temporários ou não utilizados que foram criados durante a migração do cluster azul para o verde garante que seu ambiente permaneça otimizado, seguro e econômico. A limpeza inclui ajustar as configurações de segurança, fazer backups finais e descomissionar recursos desnecessários. Para limpar os recursos: 1. Atualizar grupos de segurança: configure os grupos de segurança associados aos clusters azul e verde para refletir o novo ambiente primário (verde). Restrinja o acesso ao ambiente azul se ele não for mais necessário e verifique se as configura ções de segurança do cluster verde seguem as melhores práticas. 2. Faça um backup final do cluster verde: após a conclusão da migração, tire um instantâneo final do cluster verde para servir como backup. Você pode usar esse instantâneo para	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	restaurar o ambiente no futuro, se necessário.
	
	`aws rds create-db-snapshot --db-instance-identifier green-cluster-instance --db-snapshot-identifier green-cluster-final-snapshot`
	
	3. Revise e remova recursos temporários: revise todos os recursos temporários criados durante a migração, como grupos de segurança temporários, instantâneos ou outras configurações. Exclua recursos que não são mais necessários para evitar custos desnecessários. Por exemplo, exclua o cluster azul se ele não for mais necessário:
	
	`aws rds delete-db-cluster --db-cluster-identifier blue-cluster-identifier --skip-final-snapshot`
	
	A limpeza dos recursos ajuda a manter um ambiente seguro e simplificado, reduz custos e garante que somente a	

Tarefa	Descrição	Habilidades necessárias
	infraestrutura necessária permaneça.	

Recursos relacionados

AWS CloudFormation:

- AWS CloudFormation Guia do usuário
- AWS CloudFormation melhores práticas
- Gere modelos a partir de recursos existentes com o IaC Generator
- Importar aplicativos inteiros para AWS CloudFormation (postagem AWS do blog)

Amazon Aurora:

- Amazon Aurora Guia do usuário
- Gerenciando um cluster de banco de dados Amazon Aurora

Estratégia de implantação azul/verde:

- Visão geral das implantações do Amazon Aurora Blue/Green

Replicação baseada em GTID:

- Usando a replicação baseada em GTID (documentação do Amazon RDS)

AWS Lambda:

- AWS Lambda Guia do desenvolvedor
- Práticas recomendadas para trabalhar com AWS Lambda funções

Amazon Route 53:

- Guia do desenvolvedor do Amazon Route 53
- Roteamento ponderado

Ferramentas do cliente MySQL:

- PyMySQL

Automatize tarefas de banco de dados na edição SQL Server Express em execução na Amazon EC2 usando AWS Lambda um Agendador de Tarefas

Criado por Subhani Shaik (AWS)

Resumo

Esse padrão demonstra como agendar e gerenciar tarefas de banco de dados na edição SQL Server Express, que é a versão gratuita do SQL Server. No entanto, a edição SQL Server Express não tem o serviço SQL Server Agent que normalmente lida com operações automatizadas de banco de dados. Esse padrão explica como você pode usar o Agendador de Tarefas e o Lambda como uma alternativa para automatizar tarefas de banco de dados na edição SQL Server Express em execução em uma instância do Amazon Elastic Compute Cloud (Amazon). EC2

O Agendador de Tarefas é um utilitário de sistema Windows integrado que facilita a execução automática de tarefas rotineiras. Ele fornece um mecanismo para programar e gerenciar operações automatizadas, eliminando a necessidade de intervenção manual em processos recorrentes. AWS Lambdaé um serviço de computação sem servidor que executa automaticamente o código em resposta a eventos, sem exigir que você gerencie a infraestrutura subjacente.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Uma nuvem privada virtual (VPC) criada com a Amazon Virtual Private Cloud (Amazon VPC)
- Uma EC2 instância da Amazon com Windows Server
- Volumes do Amazon Elastic Block Store (Amazon EBS) conectados a uma instância da EC2 Amazon com o Windows Server
- Binários do SQL Server Express Edition

Limitações

- Para obter informações sobre as limitações de recursos da edição SQL Server Express, consulte o site da Microsoft.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- SQL Server 2016 ou posterior com a edição SQL Server Express

Arquitetura

O diagrama a seguir mostra uma EC2 instância da Amazon em execução com a edição SQL Server Express instalada. A instância pode ser acessada por meio do cliente Remote Desktop Protocol (RDP) ou de AWS Systems Manager Session Manager. AWS Key Management Service (AWS KMS) gerencia a criptografia de dados dos volumes do Amazon EBS para garantir a data-at-rest segurança. A infraestrutura também inclui AWS Identity and Access Management (IAM), que fornece controle de acesso e gerencia permissões para a execução das funções do Lambda. O Amazon Simple Storage Service (Amazon S3) armazena funções Lambda.

Ferramentas

Serviços da AWS

- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias da Amazon. EC2
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

- AWS Systems Manager Session Manageré uma AWS Systems Manager ferramenta totalmente gerenciada. Com o Session Manager, você pode gerenciar suas EC2 instâncias da Amazon, dispositivos de borda, servidores locais e máquinas virtuais (VMs).
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- O Microsoft SQL Server Management Studio (SSMS) é uma ferramenta para gerenciar o SQL Server, incluindo acesso, configuração e administração de componentes do SQL Server.
- Python é uma linguagem de programação de computador de uso geral. Você pode usá-lo para criar aplicativos, automatizar tarefas e desenvolver serviços no Nuvem AWS.
- O Agendador de Tarefas é uma ferramenta da Microsoft que você pode usar para agendar tarefas rotineiras em seu computador automaticamente.

Práticas recomendadas

- Melhores práticas para a Amazon EC2
- Melhores práticas para implantar o Microsoft SQL Server na Amazon EC2
- Melhores práticas para trabalhar com AWS Lambda funções
- Práticas recomendadas de segurança no IAM

Épicos

Crie uma EC2 instância da Amazon e instale a edição SQL Server Express

Tarefa	Descrição	Habilidades necessárias
Implante uma EC2 instância da Amazon.	Para criar uma EC2 instância da Amazon, abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/e selecione uma Amazon Machine Image	DBA, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	(AMI) na lista de instâncias disponíveis para o Windows Server. Para obter mais informaçõ es, consulte Iniciar uma EC2 instância da Amazon na AWS documentação.	

Tarefa	Descrição	Habilidades necessárias
Instale a edição SQL Server Express.	Para instalar a edição SQL Server Express, conclua as seguintes etapas: 1. Para se conectar à sua EC2 instância da Amazon, escolha uma opção: • Opção A — Use o Remote Desktop Protocol (RDP). Para obter instruções, consulte Conecte-se à sua instância do Windows usando um cliente RDP na AWS documentação. • Opção B — Use o EC2 console da Amazon AWS Systems Manager Session Manager e. Para obter instruções, consulte Connect to your Amazon EC2 instance using Session Manager na AWS documentação. 2. Para baixar a edição necessária do SQL Server Express, acesse Downloads do SQL Server no site da Microsoft. 3. Para instalar a edição SQL Server Express, siga as instruções em Planejar uma instalação do SQL Server no site da Microsoft.	DBA, AWS DevOps

Crie tarefas automatizadas de manutenção de banco de dados

Tarefa	Descrição	Habilidades necessárias
Identifique tarefas rotineiras.	Identifique as tarefas rotineiras que você deseja automatizar. Por exemplo, as seguintes tarefas são elegíveis para automação: • Backups de banco de dados (registro completo, diferencial e de transações) • Manutenção e reorganização de índices • Atualizações de estatísticas • Operações específicas do aplicativo • Limpeza ou arquivamento de dados	DBA
Prepare scripts SQL.	Para preparar scripts SQL, faça o seguinte: 1. Crie consultas SQL para cada tarefa de manutenção. Veja a seguir um exemplo de consulta T-SQL para realizar um backup de banco de dados específico: `Backup Database <Database_Name> To Disk='C:\Backups\Database_Name.bak'` 2. Salve o arquivo de script como `<File Name>.sql`. Em seguida, salve	DBA

Tarefa	Descrição	Habilidades necessárias
	os scripts em um local acessível na unidade local do servidor na EC2 instância da Amazon ou em um compartilhamento de arquivos de rede.	
Configure as permissões de acesso.	Para configurar as permissões de acesso, faça o seguinte: 1. Defina as permissões apropriadas do sistema de arquivos. Para obter instruções, consulte Configurar permissões do sistema de arquivos para acesso ao Database Engine no site da Microsoft. 2. Verifique se a conta de serviço do SQL Server tem o acesso necessári o. Para obter instruçõe s, consulte Configurar permissões e contas de serviço do Windows no site da Microsoft. 3. Verifique a conectividade de rede para compartil hamentos remotos. Para obter mais informaçõ es, consulte Acessando dados usando compartil hamentos de arquivos na AWS documentação.	DBA

Automatize tarefas com o Agendador de Tarefas

Tarefa	Descrição	Habilidades necessárias

Crie arquivos em lotes.	• Para criar um arquivo em lotes, use um editor de texto para digitar o comando a seguir. Substitua `username` os parâmetros `password` por seus próprios valores. Em seguida, salve o arquivo como`<Name>.bat` .
	
	`sqlcmd -S servername -U username -P password -i <T-SQL query path.sql>`
	
	• Para criar um arquivo em lotes para tarefas SQL, use um editor de texto e digite os comandos a seguir. Substitua os parâmetros `ServerName DatabaseName username`,, e `password` por seus próprios valores. Em seguida, salve o arquivo como`<Name>.bat` .
	
	`@echo off sqlcmd -S [ServerName] -d [DatabaseName] -U username -P password -i "PathToSQLScript\Script.sql"`
		AWS DevOps, DBA

Tarefa	Descrição	Habilidades necessárias
	`-o "PathToOutput\Output.txt"`	

Tarefa	Descrição	Habilidades necessárias
Crie tarefas no Agendador de Tarefas.	Para criar uma tarefa no Agendador de Tarefas, use as seguintes etapas: 1. Para abrir o Agendador de Tarefas, digite taskschd.msc na pesquisa do Windows. 2. Escolha o menu Ação e selecione Criar tarefa básica. 3. Em Nome, forneça um nome para a tarefa e escolha Avançar. 4. Em Trigger, selecione a opção para quando você deseja que a tarefa comece e, em seguida, escolha Avançar. 5. Forneça as informações de Início e Recorrência da tarefa e escolha Avançar. 6. Na seção Ação, selecione Iniciar um programa e escolha Avançar. 7. Para Programa/script, especifique o caminho para o arquivo em lotes que você criou na tarefa anterior e escolha Avançar. 8. Escolha Terminar.	DBA

Tarefa	Descrição	Habilidades necessárias
	Para executar a tarefa manualmente, clique com o botão direito do mouse na tarefa recém-criada e selecione Executar.	
Exibir o status da tarefa.	Para ver o status de uma tarefa no Agendador de Tarefas, use as seguintes etapas: 1. No Agendador de Tarefas, acesse a Biblioteca do Agendador de Tarefas, que exibe todas as tarefas. 2. Para ver o status da tarefa que você criou anteriorm ente, selecione a tarefa e vá para a guia Histórico.	DBA, AWS DevOps

Automatize tarefas com AWS Lambda

Tarefa	Descrição	Habilidades necessárias
Implemente a solução.	Para implementar a solução desse padrão, use as seguintes etapas: 1. Crie uma função do Lambda. Para obter instruções, consulte Criar sua primeira função do Lambda na AWS documentação.	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	2. Agende a função Lambda. Para obter instruções, consulte Invocar uma função Lambda em um cronograma na AWS documentação. 3. Execute consultas T-SQL. Para obter mais informaçõ es, consulte Tutorial: Usando uma função Lambda para acessar um banco de dados do Amazon RDS na documentação. AWS O tutorial explica como conectar bancos de dados Amazon RDS a partir de funções Lambda para executar consultas SQL.	

Solução de problemas

Problema	Solução
Problemas com o Lambda	Para obter ajuda com erros e problemas que você pode encontrar ao usar AWS Lambda, consulte Solução de problemas no Lambda na AWS documentação.

Recursos relacionados

- Tipos de EC2 instância da Amazon
- AWS Lambda documentação
- AWS Lambda preços

- Agendador de tarefas para desenvolvedores (site da Microsoft)

Automatize o failover e o failback entre regiões usando o DR Orchestrator Framework

Criado por Jitendra Kumar (AWS), Oliver Francis (AWS) e Pavithra Balasubramanian (AWS)

Resumo

Esse padrão descreve como usar o DR Orchestrator Framework para orquestrar e automatizar as etapas manuais e propensas a erros para realizar a recuperação de desastres nas regiões da Amazon Web Services ().AWS O padrão abrange os seguintes bancos de dados:

- Amazon Relational Database Service (Amazon RDS) para MySQL, Amazon RDS para PostgreSQL ou Amazon RDS para MariaDB
- Edição compatível com Amazon Aurora MySQL ou edição compatível com Amazon Aurora PostgreSQL (usando um arquivo centralizado)
- Amazon ElastiCache (Redis OSS)

Para demonstrar a funcionalidade do DR Orchestrator Framework, você cria duas instâncias de banco de dados ou clusters. O primário está no Região da AWS `us-east-1`, e o secundário está dentro`us-west-2`. Para criar esses recursos, você usa os AWS CloudFormation modelos na `App-Stack` pasta do GitHub repositório aws-cross-region-dr-databases.

Pré-requisitos e limitações

Pré-requisitos gerais

- Estrutura do DR Orchestrator implantada tanto no primário quanto no secundário Regiões da AWS
- Dois buckets do Amazon Simple Storage Service
- Uma nuvem privada virtual (VPC) com duas sub-redes e um grupo de segurança AWS

Pré-requisitos específicos do motor

- Amazon Aurora — Pelo menos um banco de dados global do Aurora deve estar disponível em dois. Regiões da AWS Você pode usar `us-east-1` como região primária e usar `us-west-2` como região secundária.

- Amazon ElastiCache (Redis OSS) — Um armazenamento de dados ElastiCache global deve estar disponível em dois. Regiões da AWS Você pode usar `use us-east-1` como região primária e usar `us-west-2` como região secundária.

Limitações do Amazon RDS

- O DR Orchestrator Framework não verifica o atraso na replicação antes de fazer um failover ou failback. O atraso na replicação deve ser verificado manualmente.
- Essa solução foi testada usando uma instância de banco de dados primária com uma réplica de leitura. Se você quiser usar mais de uma réplica de leitura, teste a solução minuciosamente antes de implementá-la em um ambiente de produção.

Limitações do Aurora

- A disponibilidade e o suporte dos recursos variam entre as versões específicas de cada mecanismo de banco de dados Regiões da AWS. Para obter mais informações sobre a disponibilidade de recursos e regiões para replicação entre regiões, consulte Réplicas de leitura entre regiões.
- Os bancos de dados globais do Aurora têm requisitos de configuração específicos para as classes de instância de banco de dados Aurora suportadas e o número máximo de. Regiões da AWS Para obter mais informações, consulte Requisitos de configuração de um banco de dados global do Amazon Aurora.
- Essa solução foi testada usando uma instância de banco de dados primária com uma réplica de leitura. Se você quiser usar mais de uma réplica de leitura, teste a solução minuciosamente antes de implementá-la em um ambiente de produção.

ElastiCache Limitações

- Para obter informações sobre a disponibilidade regional para o armazenamento de dados global e os requisitos ElastiCache de configuração, consulte Pré-requisitos e limitações na documentação. ElastiCache

Versões do produto Amazon RDS Up

O Amazon RDS é compatível com as seguintes versões de mecanismo:

- MySQL — O Amazon RDS oferece suporte a instâncias de banco de dados que executam as seguintes versões do MySQL: MySQL 8.0 e MySQL 5.7
- PostgreSQL — Para obter informações sobre as versões compatíveis do Amazon RDS para PostgreSQL, consulte Versões disponíveis do banco de dados PostgreSQL.
- MariaDB — O Amazon RDS oferece suporte a instâncias de banco de dados que executam as seguintes versões do MariaDB:
  - MariaDB 10.11
  - MariaDB 10.6
  - MariaDB 10.5

Versões do produto Aurora

- A transição global do banco de dados Amazon Aurora requer o Aurora MySQL compatível com o MySQL 5.7, versão 2.09.1 e superior

  Para obter mais informações, consulte Limitações dos bancos de dados globais do Amazon Aurora.

ElastiCache Versões do produto (Redis OSS)

A Amazon ElastiCache (Redis OSS) oferece suporte às seguintes versões do Redis:

- Redis 7.1 (aprimorado)
- Redis 7.0 (aprimorado)
- Redis 6.2 (aprimorado)
- Redis 6.0 (aprimorado)
- Redis 5.0.6 (aprimorado)

Para obter mais informações, consulte Versões suportadas ElastiCache (Redis OSS).

Arquitetura

Arquitetura Amazon RDS

A arquitetura do Amazon RDS inclui os seguintes recursos:

- A instância de banco de dados primária do Amazon RDS criada na região primária (`us-east-1`) com acesso de leitura/gravação para clientes
- Uma réplica de leitura do Amazon RDS criada na região secundária (`us-west-2`) com acesso somente de leitura para clientes
- Estrutura do DR Orchestrator implantada nas regiões primária e secundária

O diagrama mostra o seguinte:

1. Replicação assíncrona entre a instância primária e a instância secundária
2. Acesso de leitura/gravação para clientes na região principal
3. Acesso somente de leitura para clientes na região secundária

Arquitetura Aurora

A arquitetura do Amazon Aurora inclui os seguintes recursos:

- O cluster de banco de dados Aurora principal criado na região primária (`us-east-1`) com um endpoint de gravação ativa
- Um cluster de banco de dados Aurora criado na região secundária (`us-west-2`) com um endpoint de gravador inativo
- Estrutura do DR Orchestrator implantada nas regiões primária e secundária

O diagrama mostra o seguinte:

1. Replicação assíncrona entre o cluster primário e o cluster secundário
2. O cluster de banco de dados principal com um endpoint de gravação ativa
3. O cluster de banco de dados secundário com um endpoint de gravação inativa

ElastiCache Arquitetura (Redis OSS)

A arquitetura Amazon ElastiCache (Redis OSS) inclui os seguintes recursos:

- Um armazenamento de dados global ElastiCache (Redis OSS) criado com dois clusters:

1. O cluster primário na região primária (`us-east-1`)
2. O cluster secundário na região secundária (`us-west-2`)

- Um link entre regiões da Amazon com criptografia TLS 1.2 entre os dois clusters
- Estrutura do DR Orchestrator implantada nas regiões primária e secundária

Automação e escala

O DR Orchestrator Framework é escalável e oferece suporte ao failover ou failback de mais de um banco de dados em paralelo. AWS

Você pode usar o seguinte código de carga útil para fazer o failover de vários AWS bancos de dados em sua conta. Neste exemplo, três AWS bancos de dados (dois bancos de dados globais, como o Aurora compatível com MySQL ou o Aurora PostgreSQL, e uma instância do Amazon RDS for MySQL) fazem o failover para a região de recuperação de desastres:

```
{
  "StatePayload": [
    {
      "layer": 1,
      "resources": [
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (MySQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-mysql-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-mysql-cluster-
identifier"
          }
        },
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (PostgreSQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-postgres-global-
identifier",
```

```
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-postgres-cluster-
identifier"
          }
        },
        {
          "resourceType": "PromoteRDSReadReplica",
          "resourceName": "Promote RDS for MySQL Read Replica",
          "parameters": {
            "RDSInstanceIdentifier": "!Import rds-mysql-instance-identifier",
            "TargetClusterIdentifier": "!Import rds-mysql-instance-global-arn"
          }
        }
      ]
    }
  ]
}
```

Ferramentas

AWS serviços

- O Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado criado para a nuvem e compatível com o MySQL e o PostgreSQL.
- ElastiCacheA Amazon ajuda você a configurar, gerenciar e escalar ambientes distribuídos de cache na memória no Nuvem AWS. Esse padrão usa Amazon ElastiCache (Redis OSS).
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado. Nesse padrão, as funções Lambda são usadas AWS Step Functions para executar as etapas.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional no. Nuvem AWS Esse padrão é compatível com Amazon RDS para MySQL, Amazon RDS para PostgreSQL e Amazon RDS para MariaDB.
- AWS SDK para Python (Boto3)ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS Nesse padrão, o Boto3 APIs é usado para se comunicar com as instâncias do banco de dados ou bancos de dados globais.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios. Nesse padrão, as máquinas de estado do Step Functions são usadas para orquestrar e executar

o failover e o failback entre regiões das instâncias do banco de dados ou dos bancos de dados globais.

Repositório de código

O código desse padrão está disponível no repositório aws-cross-region-dr-databases em. GitHub

Épicos

Instale o DR Orchestrator Framework

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Para clonar o repositório, execute o seguinte comando: `git clone https://github.com/aws-samples/aws-cross-region-dr-databases.git`	AWS DevOps, administrador da AWS

O código de funções do Package Lambda em um arquivo de arquivos.zip.	Crie os arquivos de arquivamento das funções Lambda para incluir as dependências do DR Orchestrator Framework:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts`
	
	`bash scripts/deploy-orchestrator-sh.sh`
		Administrador da AWS

Crie buckets S3.	Os buckets S3 são necessários para armazenar o DR Orchestrator Framework junto com sua configuração mais recente. Crie dois buckets S3, um na região primária (`us-`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`east-1`) e outro na região secundária (`us-west-2`): • `dr-orchestrator-xxxxxx-us-east-1` • `dr-orchestrator-xxxxxx-us-west-2` `xxxxxx`Substitua por um valor aleatório para tornar os nomes dos buckets exclusivos.	
Crie sub-redes e grupos de segurança.	Tanto na região primária (`us-east-1`) quanto na região secundária (`us-west-2`), crie duas sub-redes e um grupo de segurança para a implantação da função Lambda em sua VPC: • `subnet-XXXXXXX` • `subnet-YYYYYYY` • `sg-XXXXXXXXXXX`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Atualize os arquivos de parâmetros do DR Orchestrator.	Na `<YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation` pasta, atualize os seguintes arquivos de parâmetros do DR Orchestrator: • `Orchestrator-Deployer-parameters-us-east-1.json` • `Orchestrator-Deployer-parameters-us-west-2.json` Use os seguintes valores de parâmetros, substituindo `x` e `y` pelos nomes dos seus recursos: `[ { "ParameterKey": "TemplateStoreS3BucketName", "ParameterValue": "dr-orchestrator-xxxxxx-us-east-1" }, { "ParameterKey": "TemplateVPCId", "ParameterValue": "vpc-xxxxxx" }, {`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	"ParameterKey": "TemplateLambdaSubnetID1", "ParameterValue": "subnet-xxxxx" }, { "ParameterKey": "TemplateLambdaSubnetID2", "ParameterValue": "subnet-yyyyy" }, { "ParameterKey": "TemplateLambdaSecurityGroupID", "ParameterValue": "sg-xxxxxxxxxx" }]	

Tarefa	Descrição	Habilidades necessárias
Faça upload do código do DR Orchestrator Framework para o bucket do S3.	O código estará mais seguro em um bucket do S3 do que no diretório local. Faça upload do `DR-Orchestration-artifacts` diretório, incluindo todos os arquivos e subpastas, para os buckets do S3. Para fazer o upload do código, faça o seguinte: 1. Faça login no AWS Management Console. 2. Acesse o console do Amazon S3. 3. Selecione o `dr-orchestrator-xxxxxx-us-east-1 bucket` . 4. Escolha Carregar e, em seguida, escolha Adicionar pasta. 5. Selecione a pasta `DR-Orchestration-artifacts` . 6. Escolha Carregar. 7. Selecione o `dr-orchestrator-xxxxxx-us-west-2` bucket. 8. Repita as etapas de 4 a 7.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Implante o DR Orchestrator Framework na região primária.	Para implantar o DR Orchestrator Framework na região primária (`us-east-1`), execute os seguintes comandos:
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Implante o DR Orchestrator Framework na região secundária.	Na região secundária (`us-west-2`), execute os seguintes comandos:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Verificar a implantação.	Se o AWS CloudFormation comando for executado com êxito, ele retornará a seguinte saída: `Successfully created/ updated stack - dr-orchestrator` Como alternativa, você pode navegar até o AWS CloudFormation console e verificar o status da `dr-orchestrator` pilha.	Administrador da AWS

Crie as instâncias ou clusters do banco de dados

Tarefa	Descrição	Habilidades necessárias
Crie as sub-redes do banco de dados e os grupos de segurança.	Em sua VPC, crie duas sub-redes e um grupo de segurança para a instância de banco de dados ou banco de dados global nas regiões primária (`us-east-1`) e secundária (): `us-west-2` • `subnet-XXXXXX` • `subnet-XXXXXX` • `sg-XXXXXXXXXX`	Administrador da AWS
Atualize o arquivo de parâmetros para a instância	Na `<YOUR LOCAL GIT FOLDER>/App-Stack` pasta, atualize o arquivo de	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
de banco de dados ou cluster primário.	parâmetros para a região principal. Amazon RDS No `RDS-MySQL-parameter-us-east-1.json` arquivo, `SubnetIds` atualize e `DBSecurityGroup` com os nomes dos recursos que você criou: `{ "Parameters": { "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId" } }` Amazon Aurora	

Tarefa	Descrição	Habilidades necessárias

	No `Aurora-MySQL-parameter-us-east-1.json` arquivo, `SubnetIds` atualize e `DBSecurityGroup` com os nomes dos recursos que você criou:
	
	`{`
	`  "Parameters": {`
	`  "SubnetIds": "subnet1-xxxxxx,subnet2-xxxxxx",`
	`  "DBSecurityGroup": "sg-xxxxxxxxxx",`
	`  "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql",`
	`  "DBClusterName":"dbcluster-01",`
	`  "SourceDBClusterName":"dbcluster-02",`
	`  "DBPortNumber": "3787",`
	`  "DBInstanceClass": "db.r5.large",`
	`  "InitialDatabaseName": "sampledb",`
	`  "PrimaryRegion": "us-east-1",`
	`  "SecondaryRegion": "us-west-2",`
	`  "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId"`
	`  }`
	`}`
	
	Amazon ElastiCache (Redis OSS)	

Tarefa	Descrição	Habilidades necessárias
	No `ElastiCache-parameter-us-east-1.json` arquivo, `SubnetIds` atualize e `DBSecurityGroup` com os nomes dos recursos que você criou. `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-xxxxxxxxxx", "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2" }`	

Tarefa	Descrição	Habilidades necessárias
	} }	

Tarefa	Descrição	Habilidades necessárias

Implante sua instância de banco de dados ou cluster na região primária.	Para implantar sua instância ou cluster na região primária (`us-east-1`), execute os comandos a seguir com base no seu mecanismo de banco de dados.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-Primary.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-Primary.yaml \`
	`--parameter-overrides file://Aurora-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon ElastiCache (Redis OSS)
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 --stack-name elasticache-ds-app-stack \`
	`--template-file ElastiCache-Primary.yaml \`
	`--parameter-overrides file://ElastiCache-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`	

Tarefa	Descrição	Habilidades necessárias
	Verifique se os AWS CloudFormation recursos foram implantados com êxito.	

Tarefa	Descrição	Habilidades necessárias
Atualize o arquivo de parâmetros para a instância de banco de dados ou cluster secundário.	Na `<YOUR LOCAL GIT FOLDER>/App-Stack` pasta, atualize o arquivo de parâmetros para a região secundária. Amazon RDS No `RDS-MySQL-parameter-us-west-2.json` arquivo, `SubnetIDs` atualize e `DBSecurityGroup` com os nomes dos recursos que você criou. Atualize o `PrimaryRegionKMSKeyArn` com o valor de `MySQLKmsKeyId` obtido da seção Saídas da AWS CloudFormation pilha para a instância de banco de dados primária: `{ "Parameters": { "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1",`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	<pre>"SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId", "PrimaryRegionKMSKeyArn":"arn:aws:kms:us-east-1:xxxxxxxxx:key/mrk-xxxxxxxxxxxxxxxxx" } }</pre> Amazon Aurora No `Aurora-MySQL-parameter-us-west-2.json` arquivo, `SubnetIDs` atualize e `DBSecurityGroup` com os nomes dos recursos que você criou. Atualize o `PrimaryRegionKMSKeyArn` com o valor de `AuroraKmsKeyId` obtido da seção Saídas da AWS CloudFormation pilha para a instância de banco de dados primária: <pre>{ "Parameters": { "SubnetIds": "subnet1-aaaaaaaaa,subnet2-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql",</pre>	

Tarefa	Descrição	Habilidades necessárias

	<pre>"DBClusterName":"dbcluster-01",
	"SourceDBClusterName":"dbcluster-02",
	"DBPortNumber": "3787",
	"DBInstanceClass": "db.r5.large",
	"InitialDatabaseName": "sampledb",
	"PrimaryRegion": "us-east-1",
	"SecondaryRegion": "us-west-2",
	"KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId"
	}
	}</pre>
	Amazon ElastiCache (Redis OSS)
	
	No `ElastiCache-parameter-us-west-2.json` arquivo, `SubnetIDs` atualize e `DBSecurityGroup` com os nomes dos recursos que você criou. Atualize o `PrimaryRegionKMSKeyArn` com o valor de `ElastiCacheKmsKeyId` obtido da seção Saídas da AWS CloudFormation pilha para a instância de banco de dados primária:	

Tarefa	Descrição	Habilidades necessárias

	{
	  "Parameters": {
	    "CacheNodeType":
	 "cache.m5.large",
	    "DBSecurityGroup":
	 "sg-ccccccccc",
	    "SubnetIds":
	 "subnet-aaaaaaaaa,
	subnet-bbbbbbbbb",
	    "EngineVersion":
	 "5.0.6",
	    "GlobalReplication
	GroupIdSuffix": "demo-
	redis-global-datastor
	e",
	    "NumReplicas": "1",
	    "NumShards": "1",
	    "ReplicationGroupI
	d": "demo-redis-cluste
	r",
	    "DBPortNumber":
	 "3788",
	    "TransitEncryption
	": "true",
	    "KMSKeyAliasName":
	 "elasticache/demo-
	redis-global-datas
	tore-KmsKeyId",
	    "PrimaryRegion":
	 "us-east-1",
	    "SecondaryRegion":
	 "us-west-2"
	  }
	}	

Tarefa	Descrição	Habilidades necessárias

Implante sua instância de banco de dados ou cluster na região secundária.	Execute os comandos a seguir, com base em seu mecanismo de banco de dados.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-DR.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-DR.yaml \`
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	`--parameter-overrides file://Aurora-MySQL-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`
	
	Amazon ElastiCache (Redis OSS)
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \ --region us-west-2 \ --stack-name elasticache-ds-app-stack \ --template-file ElastiCache-DR.yaml \ --parameter-overrides file://ElastiCache-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`
	
	Verifique se os AWS CloudFormation recursos foram implantados com êxito.	

Recursos relacionados

- Estratégia de recuperação de desastres para bancos de dados em AWS (estratégia de orientação AWS prescritiva)
- Automatize sua solução de DR para bancos de dados relacionais em AWS(guia de orientação AWS prescritiva)
- Usar bancos de dados globais do Amazon Aurora
- Replicação Regiões da AWS usando datastores globais
- Automatize sua solução de DR para bancos de dados relacionais em AWS(guia de orientação AWS prescritiva)

Automatize a replicação de instâncias do Amazon RDS em Contas da AWS

Criado por Parag Nagwekar (AWS) e Arun Chandapillai (AWS)

Resumo

Esse padrão mostra como automatizar o processo de replicação, rastreamento e reversão de suas instâncias de banco de dados do Amazon Relational Database Service (Amazon RDS) em diferentes instâncias usando e. Contas da AWS AWS Step Functions AWS Lambda Você pode usar essa automação para realizar a replicação em larga escala de instâncias de banco de dados do RDS sem nenhum impacto no desempenho ou sobrecarga operacional, independentemente do tamanho da sua organização. Você também pode usar esse padrão para ajudar sua organização a cumprir as estratégias obrigatórias de governança de dados ou os requisitos de conformidade que exigem que seus dados sejam replicados e redundantes em diferentes e. Contas da AWS Regiões da AWS A replicação entre contas de dados do Amazon RDS em escala é um processo manual ineficiente e propenso a erros que pode ser caro e demorado, mas a automação nesse padrão pode ajudar você a obter a replicação entre contas com segurança, eficácia e eficiência.

Pré-requisitos e limitações

Pré-requisitos

- Dois Contas da AWS
- Uma instância de banco de dados do RDS, ativa e em execução na origem Conta da AWS
- Um grupo de sub-redes para a instância de banco de dados do RDS no destino Conta da AWS
- Uma chave AWS Key Management Service (AWS KMS) criada na origem Conta da AWS e compartilhada com a conta de destino (para obter mais informações sobre os detalhes da política, consulte a seção Informações adicionais desse padrão.)
- Um AWS KMS key no destino Conta da AWS para criptografar o banco de dados na conta de destino

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Versões do produto

- Python 3.9 (usando) AWS Lambda
- PostgreSQL 11.3, 13.x e 14.x

Arquitetura

Pilha de tecnologia

- Amazon Relational Database Service (Amazon RDS)
- Amazon Simple Notification Service (Amazon SNS)
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- AWS Step Functions

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para usar o Step Functions para orquestrar a replicação agendada e sob demanda de instâncias de banco de dados do RDS de uma conta de origem (conta A) para uma conta de destino (conta B).

Na conta de origem (conta A no diagrama), a máquina de estado Step Functions executa o seguinte:

1. Cria um snapshot da instância de banco de dados do RDS na conta A.
2. Copia e criptografa o snapshot com um AWS KMS key da conta A. Para garantir a criptografia em trânsito, o snapshot é criptografado, independentemente de a instância de banco de dados estar criptografada ou não.
3. Compartilha o snapshot do banco de dados com a conta B dando à conta B acesso ao snapshot.
4. Envia uma notificação para o tópico do SNS e, em seguida, o tópico do SNS invoca a função do Lambda na conta B.

Na conta de destino (conta B no diagrama), a função do Lambda executa a máquina de estado Step Functions para orquestrar o seguinte:

1. Copia o instantâneo compartilhado da conta A para a conta B, enquanto usa o AWS KMS key da conta A para descriptografar os dados primeiro e depois criptografar os dados usando a conta B. AWS KMS key
2. Lê o segredo do Secrets Manager para capturar o nome da instância de banco de dados atual.
3. Restaura a instância de banco de dados do snapshot com um novo nome e padrão para o AWS KMS key Amazon RDS.
4. Lê o endpoint do novo banco de dados e atualiza o segredo no Secrets Manager com o novo endpoint do banco de dados e, em seguida, marca a instância de banco de dados anterior para que ela possa ser excluída posteriormente.
5. Mantém as N instâncias mais recentes dos bancos de dados e exclui todas as outras instâncias.

Ferramentas

Serviços da AWS

- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional no. Nuvem AWS
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS
- O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar funções do Lambda e outras para criar aplicativos essenciais para os negócios. Serviços da AWS

Repositório de código

O código desse padrão está disponível no repositório GitHub Crossaccount RDS Replication.

Épicos

Automatize a replicação de instâncias de banco de dados do RDS Contas da AWS com um único clique

Tarefa	Descrição	Habilidades necessárias
Implante a CloudFormation pilha na conta de origem.	1. Faça login na conta AWS Management Console de origem (conta A) e abra o CloudFormation console. 2. No painel de navegação, escolha Pilhas. 3. escolha Criar pilha e, em seguida, escolha Com recursos existentes (importar recursos). 4. Na página Identificar recursos, escolha Próximo. 5. Na página Especificar modelo, selecione Fazer upload de um modelo. 6. Escolha Escolher arquivo, selecione o **`Cloudformation-SourceAccountRDS.yaml`** arquivo no repositório de replicação RDS entre GitHub contas e, em seguida, escolha Avançar. 7. Em Nome da pilha, insira o nome da sua pilha.	Administrador de nuvem, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	8. Na seção Parâmetros, especifique os parâmetros que são definidos no modelo da pilha: • Para DestinationAccountNumber, insira o número da conta da sua instância de banco de dados RDS de destino. • Para KeyName, insira seu AWS KMS key. • Para ScheduleExpression, insira uma expressão cron (o padrão é 12:00 da manhã diariamente). • DBIdentifierEm Origem, insira o nome do banco de dados de origem. • Em DBSnapshotNome da Fonte, insira o nome do snapshot ou aceite o padrão. 9. Escolha Próximo. 10. Na página Configurar as opções da pilha, mantenha os padrões e selecione Avançar. 11. Revise sua configuração de pilha e escolha Enviar. 12. Escolha a guia Recursos para sua pilha e anote o nome do recurso da	

Tarefa	Descrição	Habilidades necessárias
	Amazon (ARN) do tópico do SNS.	

Tarefa	Descrição	Habilidades necessárias
Implante a CloudFormation pilha na conta de destino.	1. Faça login na conta AWS Management Console de destino (conta B) e abra o CloudFormation console. 2. No painel de navegação, escolha Pilhas. 3. escolha Criar pilha e, em seguida, escolha Com recursos existentes (importar recursos). 4. Na página Identificar recursos, escolha Próximo. 5. Na página Especificar modelo, selecione Fazer upload de um modelo. 6. Escolha o arquivo, selecione o **`Cloudformation-DestinationAccountRDS.yaml`** arquivo no repositório GitHub Crossaccount RDS Replication e, em seguida, escolha Avançar. 7. Em Nome da pilha, insira o nome da sua pilha. 8. Na seção Parâmetros, especifique os parâmetros que são definidos no modelo da pilha: • Para DatabaseName, insira um nome para seu banco de dados.	Arquiteto de nuvem, DevOps engenheiro, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	• Em Mecanismo, insira o tipo de mecanismo de banco de dados que corresponde ao banco de dados de origem. • Em DBInstanceClasse, insira o tipo de instância de banco de dados preferencial ou aceite o padrão. • Em Grupos de sub-redes, insira o grupo de sub-redes VPC existente. Para obter instruções sobre como criar um grupo de sub-redes, consulte Etapa 2: Criar um grupo de sub-redes de banco de dados na documentação do Amazon RDS. • Para SecretName, insira o caminho e o nome secreto ou aceite o padrão. • Para SGID, insira o ID do grupo de segurança do seu cluster de destino. • Para KMSKey, insira o ARN da chave KMS na sua conta de destino. • Para NoOfOlderInstances, insira o número de	

Tarefa	Descrição	Habilidades necessárias
	cópias antigas das instâncias de banco de dados do RDS que você deseja manter para a reversão. 9. Escolha Próximo. 10. Na página Configurar as opções da pilha, mantenha os padrões e selecione Avançar. 11. Revise sua configuração de pilha e escolha Enviar. 12. Escolher a guia Recursos para sua pilha e, em seguida, anote o ID físico e o ARN de `InvokeStepFunction` .	
Verificar a criação da instância de banco de dados do RDS na conta de destino.	1. Faça login no AWS Management Console e abra o console do Amazon RDS. 2. No painel de navegação, escolha Bancos de dados e, em seguida, verifique se a nova instância de banco de dados do RDS aparece sob o novo cluster.	Administrador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Inscrever a função do Lambda no tópico do SNS.	Você deve executar os seguintes comandos AWS Command Line Interface (AWS CLI) para inscrever a função Lambda na conta de destino (conta B) no tópico SNS na conta de origem (conta A).
	
	Na conta A, execute o comando a seguir:
	
	`aws sns add-permission \ --label lambda-access --aws-account-id <DestinationAccount> \ --topic-arn <Arn of SNSTopic > \ --action-name Subscribe ListSubscriptionsB yTopic`
	
	Na conta B, execute o comando a seguir:
	
	`aws lambda add-permi ssion \ --function-name <Name of InvokeStepFunction > \ --source-arn <Arn of SNSTopic > \ --statement-id function-with-sns \ --action lambda:In vokeFunction \`
		Administrador de nuvem, arquiteto de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias

	`--principal sns.amazonaws.com`
	
	Na conta B, execute o comando a seguir:
	
	`aws sns subscribe \ --protocol "lambda" \ --topic-arn <Arn of SNSTopic> \ --notification-endpoint <Arn of InvokeStepFunction>`	

Tarefa	Descrição	Habilidades necessárias
Sincronizar a instância de banco de dados do RDS da conta de origem com a conta de destino.	Iniciar a replicação do banco de dados sob demanda iniciando a máquina de estado Step Functions na conta de origem. 1. Abrir o console Step Functions. 2. No painel de navegação, escolha Máquinas de estado. 3. Escolha sua máquina de estado. 4. Na guia Execuções, selecione sua função e escolha Iniciar execução para iniciar o fluxo de trabalho. **Note** Existe um agendador para ajudá-lo a executar a replicação automaticamente dentro do cronograma, mas o agendador está desativado por padrão. Você pode encontrar o nome da CloudWatch regra da Amazon para o agendador na guia Recursos	Arquiteto de nuvem, DevOps engenheiro, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	da CloudFormation pilha na conta de destino. Para obter instruções sobre como modificar a regra de CloudWatch eventos, consulte Excluindo ou desativando uma regra de CloudWatch eventos na CloudWatch documentação.	
Reverter seu banco de dados para qualquer uma das cópias anteriores quando necessário.	1. Abra o console do Secrets Manager. 2. Na lista de segredos, escolha o segredo que você criou usando o CloudFormation modelo anterior. Seu aplicativo usa o segredo para acessar o banco de dados no cluster de destino. 3. Para atualizar o valor do segredo na página de detalhes, na seção Valor do segredo, escolha Recuperar o valor do segredo e depois escolha Editar. 4. Inserir os detalhes do endpoint do banco de dados.	Administrador de nuvem, DBA, engenheiro DevOps

Recursos relacionados

- Réplicas de leitura entre regiões (documentação do Amazon RDS)
- Implantações em azul/verde (documentação do Amazon RDS)

Mais informações

Você pode usar o exemplo de política a seguir para compartilhar suas AWS KMS key informações Contas da AWS.

```
{
    "Version": "2012-10-17",
    "Id": "cross-account-rds-kms-key",
    "Statement": [
        {
            "Sid": "Enable user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<SourceAccount>:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<DestinationAccount>:root"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::<DestinationAccount>:root",
                    "arn:aws:iam::<SourceAccount>:root"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Faça backup automático dos bancos de dados SAP HANA usando o Systems Manager e EventBridge

Criado por Ambarish Satarkar (AWS) e Gaurav Rath (AWS)

Resumo

Esse padrão descreve como automatizar os backups do banco de dados SAP HANA usando o AWS Systems Manager, a Amazon, o EventBridge Amazon Simple Storage Service (Amazon S3) e o AWS Backint Agent para SAP HANA.

Esse padrão fornece uma abordagem baseada em shell script usando o comando `BACKUP DATA` e elimina a necessidade de manter scripts e configurações de tarefas para cada instância do sistema operacional (SO) em vários sistemas.

> **Note**
>
> Em abril de 2023, o AWS Backup anunciou suporte para bancos de dados SAP HANA no Amazon Elastic Compute Cloud (Amazon EC2). Para obter mais informações, consulte Bancos de dados SAP HANA no backup de EC2 instâncias da Amazon.

Com base nas necessidades da sua organização, você pode usar o serviço AWS Backup para fazer backup automático de seus bancos de dados SAP HANA ou usar esse padrão.

Pré-requisitos e limitações

Pré-requisitos

- Uma instância existente do SAP HANA com uma versão compatível em estado de execução em uma instância gerenciada do Amazon Elastic Compute Cloud EC2 (Amazon) que está configurada para Systems Manager
- Systems Manager Agent (SSM Agent) 2.3.274.0 ou mais recente instalado
- Um bucket S3 que não tenha acesso público habilitado
- Uma `hdbuserstore`chave nomeada `SYSTEM`

- Um perfil do AWS Identity and Access Management (IAM) para o runbook de automação ser executado dentro da agenda
- As políticas `AmazonSSMManagedInstanceCore` e `ssm:StartAutomationExecution` são anexadas ao perfil de serviço do Systems Manager Automation.

Limitações

- O AWS Backint Agent para SAP HANA não é compatível com a desduplicação.
- O AWS Backint Agent para SAP HANA não é compatível com a compactação de dados.

Versões do produto

O AWS Backint Agent é compatível com os seguintes sistemas operacionais:

- SUSE Linux Enterprise Server
- SUSE Linux Enterprise Server para SAP
- Red Hat Enterprise Linux para SAP

O AWS Backint Agent oferece suporte aos seguintes bancos de dados:

- SAP HANA 1.0 SP12 (nó único e vários nós)
- SAP HANA 2.0 e mais recente (nó único e nós múltiplos)

Arquitetura

Pilha de tecnologias de destino

- AWS Backint Agent
- Amazon S3
- AWS Systems Manager
- Amazon EventBridge
- SAP HANA

Arquitetura de destino

O diagrama a seguir mostra os scripts de instalação que instalam o AWS Backint Agent, o bucket S3 e o Systems Manager EventBridge e, que usam um documento de comando para agendar backups regulares.

Automação e escala

- Vários AWS Backint Agents podem ser instalados usando um runbook do Systems Manager Automation.
- Cada execução do runbook do Systems Manager pode ser escalada para um número n de instâncias do SAP HANA, com base na seleção de destinos.
- EventBridge pode automatizar os backups do SAP HANA.

Ferramentas

- O AWS Backint Agent for SAP HANA é um aplicativo independente que se integra aos seus fluxos de trabalho existentes para fazer backup do seu banco de dados SAP HANA em um bucket S3 que você especifica no arquivo de configuração. O AWS Backint Agent oferece suporte a backups completos, incrementais e diferenciais de bancos de dados SAP HANA. Ele é executado em um servidor de banco de dados SAP HANA, onde backups e catálogos são transferidos do banco de dados SAP HANA para o AWS Backint Agent.
- EventBridgeA Amazon é um serviço de barramento de eventos sem servidor que você pode usar para conectar seus aplicativos a dados de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus aplicativos, aplicativos de software como serviço (SaaS) e serviços da AWS para destinos como funções do AWS Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras contas.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objeto. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.
- O AWS Systems Manager ajuda você a visualizar e controlar a infraestrutura na AWS. Usando o console do Systems Manager, você pode visualizar dados operacionais de vários serviços da AWS e automatizar tarefas operacionais nos recursos da AWS.

Código

O código desse padrão está disponível no aws-backint-automated-backup GitHub repositório.

Épicos

Crie uma chave hdbuserstore SYSTEM

Tarefa	Descrição	Habilidades necessárias

Crie uma chave hdbuserstore.	1. Acesse `/usr/sap/<SID>/HDB<InstNo>/exe`.
	2. Execute o comando a seguir, com XX como o número da instância do banco de dados SAP HANA.
	`hdbuserstore -i set SYSTEM <hostname>:3XX13@SYSTEMDB SYSTEM`
	Por exemplo, para um host SAP HANA `saphanadb` com número de instância `00`, execute o comando a seguir.
	`hdbuserstore -i set SYSTEM saphanadb:30013@SYSTEMDB SYSTEM`
		Administrador da AWS, administrador do SAP HANA

Instale o AWS Backint Agent

Tarefa	Descrição	Habilidades necessárias
Instale o AWS Backint Agent.	Siga as instruções em Instalar e configurar o AWS Backint	Administrador da AWS, administrador do SAP HANA

Tarefa	Descrição	Habilidades necessárias
	Agent para SAP HANA na documentação do AWS Backint Agent.	

Crie um documento de comando do Systems Manager

Tarefa	Descrição	Habilidades necessárias
Crie um documento de comando do Systems Manager.	1. Faça login no Console de Gerenciamento da AWS e abra o console do AWS Systems Manager 2. Escolha Documentos e escolha Propriedade minha. 3. Confirme se você está na mesma região da AWS que seu banco de dados SAP HANA. 4. Escolha Criar documento, Comando ou sessão para criar seu documento. 5. Use um nome exclusivo e descritivo, sem espaços (por exemplo, SAP HANA-backup). 6. Verifique se o Tipo de documento está definido como Documento de comando. 7. Abaixo do cabeçalho Conteúdo, há alguns exemplos de código. Certifique-se de escolher	Administrador da AWS, administrador do SAP HANA

Tarefa	Descrição	Habilidades necessárias
	o tipo de código JSON e substitua o código pelo código do `HDB_Backup_SSM_Document.json` arquivo do GitHub repositório. 8. Escolha Criar documento. 9. Verifique seu documento na seção Propriedade minha.	

Agende backups com uma frequência regular

Tarefa	Descrição	Habilidades necessárias
Agende backups regulares usando a Amazon EventBridge.	1. Abra o EventBridge console da Amazon, escolha Regras e escolha Criar regra. 2. Na tela Definir detalhes da regra, insira um nome e uma descrição exclusivos para sua regra e use o barramento de eventos padrão. 3. Em Tipo de regra, escolha Agenda e escolha Avançar. 4. Na tela Definir agenda, escolha o padrão de agenda e a expressão rate ou cron apropriados com base na frequência necessária.	Administrador da AWS, administrador do SAP HANA

Tarefa	Descrição	Habilidades necessárias
	5. Na tela Selecionar destinos, em Tipo de destino, escolha o serviço da AWS. Em Selecionar um destino, escolha executar comando do Systems Manager . 6. Escolha o documento que você criou anteriormente. 7. Em Chave de destino e Valor de destino, forneça o ID da instância. Você pode usar nomes e valores de tags para adicionar várias instâncias. 8. Em Configurar parâmetro s de automação, escolha Constante para backups incrementais ou diferenci ais. Se você quiser um backup completo, escolha Sem parâmetros. 9. Escolha entre criar um movo perfil ou usar um perfil existente. Se você usa um perfil existente, certifiqu e-se de que ele tenha as políticas necessárias para invocar o destino. 10. Mantenha as configurações adicionais padrão e escolha Próximo. 11. A tela Configurar tags é opcional. Escolha avançar.	

Tarefa	Descrição	Habilidades necessárias
	12. Na tela Revisar e criar, revise as configurações da regra e escolha Criar. A regra deve ser criada com sucesso. Você pode verificar o sucesso do backup no caminho do bucket do S3. `s3:/<your_bucket_name>/<target folder>/<SID>/usr/sap/<SID>/SYS/global/hdb/backint/DB_<SID>/` Você também pode verificar os backups do catálogo de backup do SAP HANA.	

Recursos relacionados

- AWS Backint Agent para SAP HANA
- Instale e configure o AWS Backint Agent para SAP HANA

Gere automaticamente um modelo PyNamoDB e funções CRUD para o Amazon DynamoDB usando um aplicativo Python

Criado por Vijit Vashishtha (AWS), Dheeraj Alimchandani (AWS) e Dhananjay Karanjkar (AWS)

Resumo

É comum exigir entidades e funções de operações de criação, leitura, atualização e exclusão (CRUD) para realizar com eficiência as operações do banco de dados do Amazon DynamoDB. PyNamoDB é uma interface baseada em Python que suporta Python 3. Ele também fornece recursos como suporte para transações do Amazon DynamoDB, serialização e desserialização automáticas de valores de atributos e compatibilidade com estruturas comuns do Python, como Flask e Django. Esse padrão ajuda os desenvolvedores que trabalham com Python e DynamoDB fornecendo uma biblioteca que simplifica a criação automática de modelos PyNamoDB e funções de operação CRUD. Embora gere funções CRUD essenciais para tabelas de banco de dados, também pode fazer engenharia reversa de modelos do PyNamoDB e funções CRUD das tabelas do Amazon DynamoDB. Esse padrão foi projetado para simplificar as operações do banco de dados usando um aplicativo baseado em Python.

A seguir estão os principais recursos dessa solução:

- Esquema JSON para modelo PyNamoDB — Gere automaticamente modelos PyNamoDB em Python importando um arquivo de esquema JSON.
- Geração de funções CRUD — Gere automaticamente funções para realizar operações CRUD em tabelas do DynamoDB.
- Engenharia reversa do DynamoDB — Use o mapeamento objeto-relacional (ORM) do PyNamoDB para fazer engenharia reversa dos modelos do PyNamoDB e das funções CRUD das tabelas existentes do Amazon DynamoDB.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Python versão 3.8 ou posterior, baixado e instalado
- Jinja2 versão 3.1.2 ou posterior, baixado e instalado
- Tabelas do Amazon DynamoDB para as quais você deseja gerar ORM

- AWS Command Line Interface (AWS CLI), instalado e configurado
- PyNamoDB versão 5.4.1 ou posterior, instalado

Arquitetura

Pilha de tecnologias de destino

- Script JSON
- Aplicação Python
- modelo PyNamoDB
- Instância de banco de dados Amazon DynamoDB

Arquitetura de destino

1. Você cria um arquivo de esquema JSON de entrada. Esse arquivo de esquema JSON representa os atributos das respectivas tabelas do DynamoDB a partir das quais você deseja criar modelos PyNamoDB e para as quais você deseja criar funções CRUD. Ele contém as três chaves importantes a seguir:
   - `name`— O nome da tabela de destino do DynamoDB.
   - `region`— O Região da AWS local onde a mesa está hospedada
   - `attributes`— Os atributos que fazem parte da tabela de destino, como a chave de partição (também conhecida como atributo de hash), chave de classificação, índices secundários locais, índices secundáriosglobais e quaisquer atributos que não sejam chave. Essa ferramenta espera que o esquema de entrada forneça apenas os atributos não essenciais, pois o aplicativo busca os atributos-chave diretamente da tabela de destino. Para ver um exemplo de como especificar atributos no arquivo do esquema JSON, consulte a seção Informações adicionais desse padrão.
2. Execute o aplicativo Python e forneça o arquivo do esquema JSON como entrada.
3. O aplicativo Python lê o arquivo do esquema JSON.
4. O aplicativo Python se conecta às tabelas do DynamoDB para derivar o esquema e os tipos de dados. O aplicativo executa a operação describe_table e busca os atributos de chave e índice da tabela.
5. O aplicativo Python combina os atributos do arquivo de esquema JSON e da tabela do DynamoDB. Ele usa o mecanismo de modelo Jinja para gerar um modelo PyNamoDB e as funções CRUD correspondentes.

6. Você acessa o modelo PyNamoDB para realizar operações CRUD na tabela do DynamoDB.

Ferramentas

Serviços da AWS

- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.

Outras ferramentas

- O Jinja é um mecanismo de modelagem extensível que compila modelos em código Python otimizado. Esse padrão usa o Jinja para gerar conteúdo dinâmico incorporando espaços reservados e lógica nos modelos.
- O PyNamoDB é uma interface baseada em Python para o Amazon DynamoDB.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório de modelos PyNamoDB de GitHub geração automática e funções CRUD. O repositório é dividido em duas partes principais: o pacote do controlador e os modelos.

Pacote de controlador

O pacote Python do controlador contém a lógica principal do aplicativo que ajuda a gerar o modelo PyNamoDB e as funções CRUD. Ele contém o seguinte:

- `input_json_validator.py`— Esses scripts Python validam o arquivo de esquema JSON de entrada e criam os objetos Python que contêm a lista de tabelas de destino do DynamoDB e os atributos necessários para cada uma.
- `dynamo_connection.py`— Esse script estabelece uma conexão com a tabela do DynamoDB e usa a operação para extrair `describe_table` os atributos necessários para criar o modelo do PyNamoDB.
- `generate_model.py`— Esse script contém uma classe Python `GenerateModel` que cria o modelo PyNamoDB com base no arquivo de esquema JSON de entrada e na operação. `describe_table`

- `generate_crud.py`— Para as tabelas do DynamoDB definidas no arquivo de esquema JSON, esse script usa a `GenerateCrud` operação para criar as classes do Python.

Modelos

Esse diretório Python contém os seguintes modelos do Jinja:

- `model.jinja`— Esse modelo do Jinja contém a expressão do modelo para gerar o script do modelo PyNamoDB.
- `crud.jinja`— Este modelo Jinja contém a expressão de modelo para gerar o script de funções CRUD.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Digite o comando a seguir para clonar o repositório de modelos PyNamoDB e funções CRUD de geração automática. `git clone https://github.com/aws-samples/amazon-reverse-engineer-dynamodb.git`	Desenvolvedor de aplicativos
Configure o ambiente Python.	1. Navegue até o diretório de nível superior no repositório clonado. `cd amazon-reverse-engineer-dynamodb`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	2. Digite o comando a seguir para instalar as bibliotecas e os pacotes necessários. `pip install -r requirements.txt`	

Gere o modelo PyNamoDB e as funções CRUD

Tarefa	Descrição	Habilidades necessárias
Modifique o arquivo do esquema JSON.	1. Navegue até o diretório de nível superior no repositório clonado. `cd amazon-reverse-engineer-dynamodb` 2. Abra o `test.json` arquivo no editor de sua preferência. Você pode usar esse arquivo como referência para criar seu próprio arquivo de esquema JSON ou pode atualizar os valores desse arquivo para que correspondam ao seu ambiente. 3. Modifique o nome Região da AWS, os valores e os atributos das tabelas de destino do DynamoDB.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Note Se você definir uma tabela que não existe no arquivo do esquema JSON, essa solução não gera modelos ou funções CRUD para essa tabela. 4. Salve e feche o arquivo `test.json` . Recomendamos que você salve esse arquivo com um novo nome.	
Execute o aplicativo Python.	Digite o comando a seguir para gerar os modelos PyNamoDB e as funções CRUD, `<input_schema.json>` onde está o nome do seu arquivo de esquema JSON. `python main.py --file <input_schema.json>`	Desenvolvedor de aplicativos

Verifique o modelo PyNamoDB e as funções CRUD

Tarefa	Descrição	Habilidades necessárias
Verifique o modelo PyNamoDB gerado.	1. No diretório de nível superior do repositório	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	clonado, digite o comando a seguir para navegar até o repositório. `models` `cd models` 2. Por padrão, essa solução nomeia o arquivo de modelo PyNamoDB. `demo_model.py` Valide se esse arquivo está presente.	
Verifique as funções CRUD geradas.	1. No diretório de nível superior do repositório clonado, digite o comando a seguir para navegar até o repositório. `crud` `cd crud` 2. Por padrão, essa solução nomeia o script`demo_crud.py` . Valide se esse arquivo está presente. 3. Use as classes Python no `demo_crud.py` arquivo para realizar uma operação CRUD na tabela de destino do DynamoDB. Confirme se a operação foi concluída com êxito.	Desenvolvedor de aplicativos

Recursos relacionados

- Componentes principais do Amazon DynamoDB (documentação do DynamoDB)
- Melhorando o acesso aos dados com índices secundários (documentação do DynamoDB)

Mais informações

Atributos de amostra para o arquivo do esquema JSON

```
[
{
"name": "test_table",
"region": "ap-south-1",
"attributes": [
{
"name": "id",
"type": "UnicodeAttribute"
},
{
"name": "name",
"type": "UnicodeAttribute"
},
{
"name": "age",
"type": "NumberAttribute"
}
]
}
]
```

Bloqueie o acesso público ao Amazon RDS usando o Cloud Custodian

Criado por Abhay Kumar (AWS) e Dwarika Patra (AWS)

Resumo

Muitas organizações executam suas cargas de trabalho e serviços em vários fornecedores de nuvem. Nesses ambientes de nuvem híbrida, a infraestrutura de nuvem precisa de uma governança rígida da nuvem, além da segurança fornecida pelos provedores de nuvem individuais. Um banco de dados na nuvem, por exemplo, Amazon Relational Database Service (Amazon RDS) é um serviço importante que deve ser monitorado para detectar quaisquer vulnerabilidades de acesso e permissão. Embora você possa restringir o acesso ao banco de dados do Amazon RDS configurando um grupo de segurança, você pode adicionar uma segunda camada de proteção para proibir ações como acesso público. O bloqueio do acesso público ajuda você a cumprir o Regulamento Geral de Proteção de Dados (GDPR), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA), o Instituto Nacional de Padrões e Tecnologia (NIST) e o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS).

O Cloud Custodian é um mecanismo de regras de código aberto que você pode usar para impor restrições de acesso aos recursos da Amazon Web Services (AWS), como o Amazon RDS. Com o Cloud Custodian, você pode definir regras que validam o ambiente em relação aos padrões definidos de segurança e conformidade. Você pode usar o Cloud Custodian para gerenciar seus ambientes de nuvem ajudando a garantir a conformidade com políticas de segurança, políticas de tags e coleta de resíduos de recursos não utilizados e gerenciamento de custos. Com o Cloud Custodian, você pode usar uma única interface para implementar a governança em um ambiente de nuvem híbrida. Por exemplo, você pode usar a interface do Cloud Custodian para interagir com o AWS Microsoft Azure, reduzindo o esforço de trabalhar com mecanismos como AWS Config grupos de AWS segurança e políticas do Azure.

Esse padrão fornece instruções para usar o Cloud Custodian on para impor AWS a restrição de acessibilidade pública nas instâncias do Amazon RDS.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um par de chaves

- AWS Lambda instalado

Arquitetura

O diagrama a seguir mostra o Cloud Custodian implantando a política AWS Lambda, AWS CloudTrail iniciando o `CreateDBInstance` evento e a configuração da função Lambda como falsa no Amazon RDS. `PubliclyAccessible`

Ferramentas

Serviços da AWS

- AWS CloudTrailajuda você a auditar a governança, a conformidade e o risco operacional do seu Conta da AWS.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional no. Nuvem AWS

Outras ferramentas

- O Cloud Custodian unifica as ferramentas e os scripts que muitas organizações usam para gerenciar suas contas de nuvem pública em uma ferramenta de código aberto. Ele usa um mecanismo de regras sem estado para definição e aplicação de políticas, com métricas, resultados estruturados e relatórios detalhados para a infraestrutura de nuvem. Ele se integra perfeitamente a um runtime de tecnologia sem servidor para fornecer remediação e resposta em tempo real com baixa sobrecarga operacional.

Épicos

Configure o AWS CLI

Tarefa	Descrição	Habilidades necessárias
Instale AWS CLI o.	Para instalar o AWS CLI, siga as instruções na AWS documentação.	Administrador da AWS

Configure as AWS credencia is.	Defina as configurações que ele AWS CLI usa para interagir AWS, incluindo o formato de saída Região da AWS e o que você deseja usar.
	`$>aws configure`
	`AWS Access Key ID`
	`[None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	`[None]: <your_sec`
	`ret_access_key>`
	`Default region name`
	`[None]:`
	`Default output format`
	`[None]:`
	Para obter mais informações, consulte a documentação do AWS.
		Administrador da AWS

Criar um perfil do IAM.	Para criar um perfil do IAM com a função de execução do Lambda, execute o comando a seguir.
	`aws iam create-role --`
	`role-name lambda-ex --`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`assume-role-policy-document '{"Version": "2012-10-17","Statement": [{ "Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action": "sts:AssumeRole"}]}`	

Configurar o Cloud Custodian

Tarefa	Descrição	Habilidades necessárias
Instale o Cloud Custodian.	Para instalar o Cloud Custodian em seu sistema operacional e ambiente, siga as instruções na documentação do Cloud Custodian.	DevOps engenheiro
Verifique o esquema do Cloud Custodian.	Para ver a lista completa dos recursos do Amazon RDS com os quais você pode executar políticas, use o comando a seguir. `custodian schema aws.rds`	DevOps engenheiro
Crie a política do Cloud Custodian.	Salve o código que está no arquivo de política do Cloud Custodian na seção Informações adicionais usando uma extensão YAML.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Defina as ações do Cloud Custodian para alterar a bandeira de acesso público.	1. Localize o código do custodiante (por exemplo, `/Users/abcd/custodian/lib/python3.9/site-packages/c7n/resources/rds.py`). 2. Localize a classe `RDSSetPublicAvailability` em `rds.py` e modifique essa classe usando o código que está no arquivo rds.py de atributos c7n na seção Informações adicionais.	DevOps engenheiro
Execute uma simulação.	(Opcional) Para verificar quais recursos são identificados pela política sem executar nenhuma ação nos recursos, use o comando a seguir. `custodian run -dryrun <policy_name>.yaml -s <output_directory>`	DevOps engenheiro

Implante a política

Tarefa	Descrição	Habilidades necessárias
Implante a política usando o Lambda.	Para criar a função do Lambda que executará a política, use o comando a seguir.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`custodian run -s policy.yaml` Essa política será então iniciada pelo AWS CloudTrail `CreateDBInstance` evento. Como resultado, AWS Lambda definirá o sinalizador de acesso público `false` para instâncias que correspondam aos critérios.	

Recursos relacionados

- AWS Lambda site
- Site do Amazon RDS
- Documentação do Cloud Custodian

Mais informações

Arquivo YAML da política do Cloud Custodian

```
policies:
  - name: "block-public-access"
    resource: rds
    description: |
      This Enforcement blocks public access for RDS instances.
    mode:
      type: cloudtrail
      events:
        - event: CreateDBInstance # Create RDS instance cloudtrail event
          source: rds.amazonaws.com
          ids: requestParameters.dBInstanceIdentifier
      role: arn:aws:iam::1234567890:role/Custodian-compliance-role
```

```
    filters:
      - type: event
        key: 'detail.requestParameters.publiclyAccessible'
        value: true
    actions:
      - type: set-public-access
        state: false
```

arquivo rds.py de atributos c7n

```
@actions.register('set-public-access')
 class RDSSetPublicAvailability(BaseAction):

     schema = type_schema(
         "set-public-access",
         state={'type': 'boolean'})
     permissions = ('rds:ModifyDBInstance',)

     def set_accessibility(self, r):
         client = local_session(self.manager.session_factory).client('rds')
         waiter = client.get_waiter('db_instance_available')
         waiter.wait(DBInstanceIdentifier=r['DBInstanceIdentifier'])
         client.modify_db_instance(
             DBInstanceIdentifier=r['DBInstanceIdentifier'],
             PubliclyAccessible=self.data.get('state', False))


     def process(self, rds):
         with self.executor_factory(max_workers=2) as w:
             futures = {w.submit(self.set_accessibility, r): r for r in rds}
             for f in as_completed(futures):
                 if f.exception():
                     self.log.error(
                         "Exception setting public access on %s  \n %s",
                         futures[f]['DBInstanceIdentifier'], f.exception())
         return rds
```

Integração com o Security Hub

O Cloud Custodian pode ser integrado AWS Security Hubpara enviar descobertas de segurança e tentar ações de remediação. Para obter mais informações, consulte Anunciando a integração do Cloud Custodian com. AWS Security Hub

Configurar o acesso entre contas ao Amazon DynamoDB

Criado por Shashi Dalmia (AWS), Esteban Serna Parra (AWS) e Imhoertha Ojior (AWS)

Resumo

Esse padrão explica as etapas para configurar o acesso entre contas ao Amazon DynamoDB usando políticas baseadas em recursos. Para cargas de trabalho que usam o DynamoDB, está se tornando mais comum usar estratégias de isolamento de carga de trabalho para minimizar as ameaças à segurança e atender aos requisitos de conformidade. A implementação de estratégias de isolamento da carga de trabalho geralmente requer acesso entre contas e regiões aos recursos do DynamoDB usando políticas baseadas em identidade (IAM). AWS Identity and Access Management Isso envolve definir permissões do IAM e estabelecer uma relação de confiança entre Contas da AWS o.

As políticas baseadas em recursos para o DynamoDB simplificam muito a postura de segurança para cargas de trabalho entre contas. Esse padrão fornece etapas e exemplos de código para demonstrar como você pode configurar AWS Lambda funções em uma Conta da AWS para gravar dados em uma tabela de banco de dados do DynamoDB em uma conta diferente.

Pré-requisitos e limitações

Pré-requisitos

- Dois ativos Contas da AWS. Esse padrão se refere a essas contas como Conta A e Conta B.
- AWS Command Line Interface (AWS CLI) instalado e configurado para acessar a Conta A, para criar a tabela do DynamoDB. As outras etapas desse padrão fornecem instruções para usar os consoles IAM, DynamoDB e Lambda. Se você planeja usar AWS CLI em vez disso, configure-o para acessar as duas contas.

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra uma arquitetura de conta única. AWS Lambda, Amazon Elastic Compute Cloud (Amazon EC2) e DynamoDB estão todos na mesma conta. Nesse cenário, as funções Lambda

e as EC2 instâncias da Amazon podem acessar o DynamoDB. Para conceder acesso à tabela do DynamoDB, você pode criar uma política baseada em identidade no IAM ou criar uma política baseada em recursos no DynamoDB.

O diagrama a seguir mostra uma arquitetura de várias contas. Se os recursos em um Conta da AWS precisarem acessar uma tabela do DynamoDB em uma conta diferente, você precisará configurar uma política baseada em recursos no DynamoDB para conceder o acesso necessário. Por exemplo, no diagrama a seguir, o acesso à tabela do DynamoDB na Conta A é concedido a uma função Lambda na Conta B usando uma política baseada em recursos.

Esse padrão descreve o acesso entre contas entre o Lambda e o DynamoDB. Você pode usar etapas semelhantes para outras, Serviços da AWS se as permissões apropriadas estiverem configuradas em ambas as contas. Por exemplo, se você quiser fornecer acesso à função Lambda a um bucket do Amazon Simple Storage Service (Amazon S3) na Conta A, você pode criar uma política baseada em recursos no Amazon S3 e adicionar as permissões à função de execução do Lambda na Conta B.

Ferramentas

Serviços da AWS

- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Código

Esse padrão inclui código de amostra na seção Informações adicionais para mostrar como você pode configurar uma função Lambda na Conta B para gravar na tabela do DynamoDB na Conta A. O código é fornecido somente para fins de ilustração e teste. Se você estiver implementando

esse padrão em um ambiente de produção, use o código como referência e personalize-o para seu próprio ambiente.

Práticas recomendadas

- Siga as melhores práticas para políticas baseadas em recursos na documentação do DynamoDB.
- Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Crie uma política e uma função do IAM para a função Lambda na Conta B

Tarefa	Descrição	Habilidades necessárias
Crie uma política na Conta B.	Essa política do IAM permite a PutItemação de uma tabela do DynamoDB na Conta A. 1. Faça login na Conta B no AWS Management Console. 2. Abra o console do IAM. 3. No painel de navegação, selecione Políticas e, em seguida, Criar política. 4. Na página Especificar permissões, para o editor de políticas, selecione JSON. 5. Insira a seguinte política. `{ "Version": "2012-10-17", "Statement": [`	AWS geral

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	"Sid": "Statement1",
	"Effect": "Allow",
	"Action": "dynamodb:PutItem",
	"Resource": "arn:aws:dynamodb:<Region>:<Account-A-ID>:table/Table-Account-A"
	}
	]
	}</pre>
	6. Substitua `<Region>` e `<Account-A-ID>` por seus valores e, em seguida, escolha Avançar.
	7. Em Nome da política, insira um nome exclusivo para sua política, como `DynamoDB-PutItem-Policy`.
	8. (Opcional) Adicione uma descrição da política.
	9. Selecione Criar política.	

Tarefa	Descrição	Habilidades necessárias
Crie uma função na Conta B.	A função Lambda na Conta B usa essa função do IAM para acessar a tabela do DynamoDB na Conta A. 1. Abra o console do IAM. 2. No painel de navegação, escolha Roles (Funções) e Create role (Criar função). 3. Em Select trusted entity (Selecionar entidade confiável), escolha AWS service (Serviço da AWS). 4. Na seção Caso de uso, escolha Lambda. 5. Escolha Próximo: Permissões. 6. Na caixa Políticas de filtro insira DynamoDB. 7. Na lista de políticas do DynamoDB, escolha. `DynamoDB-PutItem-Policy` 8. Desmarque a caixa Filtrar políticas e, em seguida, insira Lambda. 9. Na lista de políticas do Lambda, escolha AWSLambda Executar. 10. Escolha Avançar: nomear, revisar e criar. 11. Em Nome do perfil, insira um nome exclusivo para o	AWS geral

Tarefa	Descrição	Habilidades necessárias
	perfil, como `DynamoDB-PutItemAccess` . 12. (Opcional) Adicione uma descrição da função. 13. (Opcional) Adicione metadados à função anexando etiquetas como pares de chave-valor. 14. Selecione Criar perfil. Para obter mais informações sobre a criação de funções, consulte a documentação de IAM.	
Anote o ARN do perfil do .	1. Abra o console do IAM. 2. No painel de navegação, selecione Perfis. 3. Na caixa de pesquisa`DynamoDB-PutItemAccess` , insira e escolha a função. 4. Na página de resumo da função, copie o Amazon Resource Name (ARN). Você usa o ARN ao configurar a função Lambda.	AWS geral

Crie uma tabela do DynamoDB na conta A

Tarefa	Descrição	Habilidades necessárias

Crie uma tabela do DynamoDB.	Use o AWS CLI comando a seguir para criar uma tabela do DynamoDB.
	
	`aws dynamodb create-table \`
	`  --table-name Table-Account-A \`
	`  --attribute-definitions \`
	`  AttributeName=category,AttributeType=S \`
	`  AttributeName=item,AttributeType=S \`
	`  --key-schema \`
	`  AttributeName=category,KeyType=HASH \`
	`  AttributeName=item,KeyType=RANGE \`
	`  --provisioned-throughput \`
	`  ReadCapacityUnits=5,WriteCapacityUnits=5 \`
	`  --resource-policy \`
	`  '{`
	`  "Version": "2012-10-17",`
	`  "Statement": [`
	`  {`
	`  "Sid": "Statement1",`
		AWS geral

Tarefa	Descrição	Habilidades necessárias

	<pre>"Effect": "Allow",
	"Principal": {
	"AWS": "arn:aws:iam::<Account-B-ID>:role/<Role-Name>"
	},
	"Action": "dynamodb:PutItem",
	"Resource": "arn:aws:dynamodb:<Region>:<Account-A-ID>:table/Table-Account-A"
	}
	
	]
	}'</pre> Substitua o seguinte neste exemplo de código:
	• `<Account-B-ID>` é o ID da Conta B.
	• `<Role-Name>` é o nome da função do IAM que você criou, como `DynamoDB-PutItemAccess` .
	• `<Region>` é Região da AWS onde você está criando a tabela do DynamoDB.
	• `<Account-A-ID>` é o ID da Conta A.	

Tarefa	Descrição	Habilidades necessárias
	Note Você especifica a configuração da política baseada em recursos na `create-table` declaração usando o `--resource-policy` sinalizador. Essa política se refere ao ARN da tabela do DynamoDB na Conta A. Para obter mais informações sobre criar tabelas, consulte a documentação do DynamoDB.	

Crie uma função Lambda na Conta B

Tarefa	Descrição	Habilidades necessárias
Crie uma função do Lambda para gravar dados no DynamoDB.	1. Faça login na Conta B no AWS Management Console. 2. Abra o console do lambda. 3. No painel de navegação, escolha Funções e selecione Criar função. 4. Em Nome, digite `lambda_write_function`.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	5. Em Runtime, escolha Python 3.8 ou superior. 6. Em Alterar função de execução padrão, escolha Usar uma função existente. 7. Em Função existente, escolha a função do IAM que você criou, como `DynamoDB-PutItemAccess`. 8. Escolha a opção Criar função. 9. Na guia Código, cole o código de amostra fornecido na seção Informações adicionais desse padrão. Substitua o seguinte neste exemplo de código: • `<Account-A-ID>` é o ID da Conta A. • `<Region>` é Região da AWS onde você criou a tabela do DynamoDB. 10. Escolha Implantar. 11. Escolha Testar. Isso solicita que você configure um evento de teste. Crie um novo evento com seu nome preferido, como `MyTestEventForWrite`, e salve a configuração.	

Tarefa	Descrição	Habilidades necessárias
	12. Escolha Test (Testar) novamente. Isso executa a função Lambda com o nome do evento que você forneceu. 13. Verifique a saída da função. Isso deve indicar que a função acessou a tabela do DynamoDB na Conta A e conseguiu gravar dados nela. Para obter mais informaçõ es sobre como criar funções do Lambda, consulte a documentação do Lambda.	

Limpeza

Tarefa	Descrição	Habilidades necessárias
Excluir recursos.	Para evitar incorrer em custos associados aos recursos criados nesse padrão, faça o seguinte para excluir esses recursos: 1. Na Conta B, exclua a função Lambda que você criou para se conectar ao DynamoDB. Para obter instruções, consulte a documentação do Lambda.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	2. Na Conta A, exclua a tabela do DynamoDB que você criou. Para obter instruções, consulte a documentação do DynamoDB. 3. Para obter as melhores práticas de segurança, exclua a política do IAM (`DynamoDB-PutItem-Policy`) quando ela não for mais necessária. Para ter mais informações, consulte a documentação do IAM. 4. Para obter as melhores práticas de segurança, exclua a função do IAM (`DynamoDB-PutItemAccess`) quando ela não for mais necessária. Para ter mais informações, consulte a documentação do IAM.	

Solução de problemas

Problema	Solução
Ao criar a função Lambda, você recebe um `ResourceNotFoundException` erro.	Confirme se você inseriu corretamente a ID Região da AWS e a ID da Conta A. Elas fazem parte do ARN da tabela do DynamoDB.

Recursos relacionados

- Introdução ao DynamoDB (Documentação do DynamoDB)
- Introdução ao Lambda (documentação do Lambda)
- Usando políticas baseadas em recursos para o DynamoDB (documentação do DynamoDB)
- Criação de políticas do IAM (Documentação do IAM)
- Lógica de avaliação de políticas entre contas (Documentação do IAM)
- Referência de elementos de política JSON do IAM (Documentação do IAM)

Mais informações

Código de exemplo

```
import boto3
from datetime import datetime

dynamodb_client = boto3.client('dynamodb')

def lambda_handler(event, context):
     now = datetime.now().isoformat()
     data = dynamodb_client.put_item(TableName='arn:aws:dynamodb:<Region>:<Account-
A-ID>:table/Table-Account-A', Item={"category": {"S": "Fruit"},"item": {"S":
 "Apple"},"time": {"S": now}})
     return data
```

> **Note**
>
> Quando o cliente do DynamoDB é instanciado, o ARN da tabela do DynamoDB é fornecido em vez do nome da tabela. Isso é necessário para que a função Lambda se conecte à tabela correta do DynamoDB quando executada.

Configurar o roteamento somente leitura em um grupo de disponibilidade Always On (Sempre ativo) no SQL Server na AWS

Criado por Subhani Shaik (AWS)

Resumo

Esse padrão aborda como usar a réplica secundária em espera no SQL Server Always On (Sempre ativo), transferindo as workloads somente leitura da réplica primária para a réplica secundária.

O espelhamento do banco de dados tem one-to-one mapeamento. Você não pode ler o banco de dados secundário diretamente, então deve criar snapshots. O atributo de grupo de disponibilidade Always On (Sempre ativo) foi introduzido no Microsoft SQL Server 2012. Em versões posteriores, as principais funcionalidades foram introduzidas, incluindo roteamento somente leitura. Nos grupos de disponibilidade Always On (Sempre ativo), você pode ler os dados diretamente da réplica secundária alterando o modo de réplica para somente leitura.

A solução de grupos de disponibilidade Always On (Sempre ativo) oferece suporte à alta disponibilidade (HA), recuperação de desastres (DR) e uma alternativa ao espelhamento de banco de dados. Os grupos de disponibilidade Always On (Sempre ativo) processam no nível do banco de dados e maximizam a disponibilidade de um conjunto de bancos de dados de usuários.

O SQL Server usa o mecanismo de roteamento somente leitura para redirecionar as conexões somente leitura de entrada para a réplica de leitura secundária. Para fazer isso, você deve adicionar os seguintes parâmetros e valores na string de conexão:

- `ApplicationIntent=ReadOnly`
- `Initial Catalog=<database name>`

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa com uma nuvem privada virtual (VPC), duas zonas de disponibilidade, sub-redes privadas e um grupo de segurança
- Duas máquinas Amazon Elastic Compute Cloud (Amazon EC2) com SQL Server 2019 Enterprise Edition Amazon Machine Image com Windows Server Failover Clustering (WSFC) configurado no nível da instância e um grupo de disponibilidade Always On configurado no nível do SQL Server

entre o nó primário (`WSFCNODE1`) e o nó secundário (`WSFCNODE2`), que fazem parte do diretório do AWS Directory Service for Microsoft Active Directory chamado `tagechtalk.com`

- Um ou mais nós configurados para aceitar `read-only` na réplica secundária
- Um receptor com o nome de `SQLAG1` para o grupo de disponibilidade Always On (Sempre ativo)
- Mecanismo de banco de dados do SQL Server em execução com a mesma conta de serviço em dois nós
- SQL Server Management Studio (SSMS)
- Um banco de dados de teste chamado `test`

Versões do produto

- SQL Server 2014 e versões posteriores

Arquitetura

Pilha de tecnologias de destino

- Amazon EC2
- AWS Managed Microsoft AD
- Amazon FSx

Arquitetura de destino

O diagrama a seguir mostra como o receptor do Grupo de disponibilidade Always On (AG) redireciona as consultas que contêm o parâmetro `ApplicationIntent` na conexão para o nó secundário apropriado.

1. Uma solicitação é enviada para o receptor do grupo de disponibilidade Always On (Sempre ativo).
2. Se a string de conexão não tiver o parâmetro `ApplicationIntent`, a solicitação será enviada para a instância primária.
3. Se a string de conexão contiver `ApplicationIntent=ReadOnly`, a solicitação será enviada para a instância secundária com configuração de roteamento somente leitura, que é WSFC com um grupo de disponibilidade Always On (Sempre ativo).

Ferramentas

Serviços da AWS

- O AWS Directory Service para Microsoft Active Directory permite que cargas de trabalho com reconhecimento de diretório e recursos da AWS usem o Microsoft Active Directory na Nuvem AWS.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- FSxA Amazon fornece sistemas de arquivos que suportam protocolos de conectividade padrão do setor e oferecem alta disponibilidade e replicação em todas as regiões da AWS.

Outros serviços

- O SQL Server Management Studio (SSMS) é uma ferramenta para conectar, gerenciar e administrar as instâncias do SQL Server.
- sqlcmd é um utilitário de linha de comando.

Práticas recomendadas

Para obter mais informações sobre grupos de disponibilidade Always On (Sempre ativo), consulte a documentação do SQL Server.

Épicos

Configurar roteamento somente leitura

Tarefa	Descrição	Habilidades necessárias
Atualizar as réplicas para somente leitura.	Para atualizar a réplica primária e a secundária para somente leitura, conecte-se à réplica primária a partir do SSMS e execute o código da Etapa 1 na seção Informações adicionais.	DBA

Tarefa	Descrição	Habilidades necessárias
Criar o URL de roteamento.	Para criar o URL de roteamento para ambas as réplicas, execute o código da Etapa 2 na seção Informações adicionais. Nesse código, `tagechtalk.com` é o nome do diretório AWS Managed Microsoft AD.	DBA
Criar a lista de roteamento.	Para criar a lista de roteamento para ambas as réplicas, execute o código da Etapa 3 na seção Informações adicionais.	DBA
Validar a lista de roteamento.	Conecte-se à instância primária do SQL Server Management Studio e execute o código da Etapa 4 na seção Informações adicionais para validar a lista de roteamento.	DBA

Teste o roteamento somente leitura

Tarefa	Descrição	Habilidades necessárias
Conecte-se usando o ApplicationIntent parâmetro.	1. No SSMS, conecte-se ao nome do receptor do grupo de disponibilidade Always On (Sempre ativo) com `ApplicationIntent=ReadOnly;Initial Catalog=test` .	DBA

Tarefa	Descrição	Habilidades necessárias
	2. A conexão é estabelecida com a réplica secundári a. Para testar, execute o comando a seguir para mostrar o nome do servidor conectado. `SELECT SERVERPRO PERTY('Computernam ePhysicalNetBios')` A saída mostrará o nome da réplica secundária atual (`WSFCNODE2 `).	

Tarefa	Descrição	Habilidades necessárias
Executar um failover.	1. No SSMS, conecte-se ao nome do receptor do grupo de disponibilidade Always On (Sempre ativo). 2. Verifique se os bancos de dados primário e secundário estão sincronizados, sem perda de dados. 3. Execute um failover para que a réplica primária atual se torne a réplica secundária e a réplica secundária se torne a réplica primária. 4. No SSMS, conecte-se ao nome do receptor do grupo de disponibilidade Always On (Sempre ativo) com `ApplicationIntent=ReadOnly;Initial Catalog=test` . 5. A conexão é estabelecida com a réplica secundária. Para testar isso, mostre o nome do servidor conectado executando o seguinte comando. `SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios')` Ele exibirá o nome da réplica secundária atual (`WSFCNODE1`).	DBA

Conectar usando o utilitário de linha de comando sqlcmd

Tarefa	Descrição	Habilidades necessárias
Conectar usando sqlcmd.	Para se conectar a partir do sqlcmd, execute o código da Etapa 5 na seção Informaçõ es adicionais na mensagem de comando. Após conectar, execute o comando a seguir para mostrar o nome do servidor conectado. `SELECT SERVERPRO PERTY('Computernam ePhysicalNetBios') .` A saída exibirá o nome da réplica secundária atual (`WSFCNODE1`).	DBA

Solução de problemas

Problema	Solução
A criação do receptor falha com a mensagem “O cluster WSFC não pôde colocar o recurso de nome de rede online”.	Para obter mais informações, consulte a postagem do blog da Microsoft Criar receptor falha com a mensagem “O cluster WSFC não pôde colocar o recurso de nome da rede online”.
Problemas potenciais, incluindo outros problemas de receptor ou problemas de acesso à rede.	Consulte Solução de problemas configuração de Grupos de disponibilidade Always On (SQL Server) na documentação da Microsoft.

Recursos relacionados

- Configurar o roteamento somente leitura para um Grupo de disponibilidade Always On (Sempre ativo)
- Solução de problemas de configuração de grupos de disponibilidade Always On (SQL Server)

Mais informações

Etapa 1. Atualizar as réplicas para somente leitura

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
```

Etapa 2. Criar o URL de roteamento

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode1.tagechtalk.com:1433'))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode2.tagechtalk.com:1433'))
GO
```

Etapa 3. Criar a lista de roteamento

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH
 (PRIMARY_ROLE(READ_ONLY_ROUTING_LIST=('WSFCNODE2','WSFCNODE1')));
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (PRIMARY_ROLE
 (READ_ONLY_ROUTING_LIST=('WSFCNODE1','WSFCNODE2')));
GO
```

Etapa 4. Validar a lista de roteamento

```
SELECT AGSrc.replica_server_name AS PrimaryReplica, AGRepl.replica_server_name AS
 ReadOnlyReplica, AGRepl.read_only_routing_url AS RoutingURL , AGRL.routing_priority
 AS RoutingPriority FROM sys.availability_read_only_routing_lists AGRL INNER JOIN
```

```
sys.availability_replicas AGSrc ON AGRL.replica_id = AGSrc.replica_id INNER JOIN
sys.availability_replicas AGRepl ON AGRL.read_only_replica_id = AGRepl.replica_id
INNER JOIN sys.availability_groups AV ON AV.group_id = AGSrc.group_id ORDER BY
PrimaryReplica
```

Etapa 5. Utilitário de comando SQL

```
sqlcmd -S SQLAG1,1433 -E -d test -K ReadOnly
```

Conecte-se usando um túnel SSH no pgAdmin

Criado por Jeevan Shetty (AWS) e Bhanu Ganesh Gudivada (AWS)

Resumo

Por motivos de segurança, é sempre bom colocar bancos de dados em uma sub-rede privada. As consultas no banco de dados podem ser executadas conectando-se por meio de um host bastion do Amazon Elastic Compute Cloud (Amazon EC2) em uma sub-rede pública na nuvem da Amazon Web Services (AWS). Isso requer a instalação de software, como o pGADmin DBeaver ou, que são comumente usados por desenvolvedores ou administradores de banco de dados, no host da Amazon. EC2

Executar o pgAdmin em um servidor Linux e acessá-lo por meio de um navegador da Web requer a instalação de dependências adicionais, configuração e configuração de permissões.

Como solução alternativa, desenvolvedores ou administradores de banco de dados podem se conectar a um banco de dados PostgreSQL usando o pgAdmin para habilitar um túnel SSH a partir do sistema local. Nessa abordagem, o pGadmin usa o host da EC2 Amazon na sub-rede pública como um host intermediário antes de se conectar ao banco de dados. O diagrama na seção Arquitetura mostra a configuração.

> **Note**
>
> Certifique-se de que o grupo de segurança conectado ao banco de dados PostgreSQL permita a conexão na porta 5432 do host da Amazon. EC2

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da AWS existente
- Uma nuvem privada virtual (VPC) com uma sub-rede pública e uma sub-rede privada
- Uma EC2 instância com um grupo de segurança anexado
- Um banco de dados Amazon Aurora Edição Compatível com PostgreSQL com um grupo de segurança anexado
- Um par de chaves Secure Shell (SSH) para configurar o túnel

Versões do produto

- pgAdmin versão 6.2+
- Amazon Aurora Edição Compatível com PostgreSQL 12.7+

Arquitetura

Pilha de tecnologias de destino

- Amazon EC2
- Amazon Aurora compatível com PostgreSQL

Arquitetura de destino

O diagrama a seguir mostra o uso do pGADmin com um túnel SSH para se conectar por meio de um gateway de internet à instância, que se conecta EC2 ao banco de dados.

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.

Outros serviços

- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.

Épicos

Criar a conexão

Tarefa	Descrição	Habilidades necessárias
Crie um servidor.	No pgAdmin escolha Criar e, em seguida, escolha Servidor. Para obter ajuda adicional com a configuração do pgAdmin para registrar um servidor, configurar uma conexão e conectar-se por meio de tunelamento SSH usando a caixa de diálogo do servidor, consulte os links na seção Recursos relacionados.	DBA
Forneça um nome para o servidor.	Na guia Geral, insira um nome.	DBA
Insira os detalhes do banco de dados.	Na guia Conexão, insira valores para o seguinte: • Nome/endereço do host • Porta • Manutenção do banco de dados • Nome de usuário • Senha	DBA
Insira os detalhes EC2 do servidor Amazon.	Na guia Túnel SSH, forneça os detalhes da EC2 instância da Amazon que está na sub-rede pública. • Defina Usar tunelamento SSH como Sim para	DBA

Tarefa	Descrição	Habilidades necessárias
	especificar que o pgAdmin deve usar um túnel SSH ao se conectar ao servidor especificado. • No campo Host do túnel, especifique o nome ou endereço IP do host SSH (por exemplo, 10.x.x.x). • No campo Porta do túnel, especifique a porta do host SSH (por exemplo, 22). • No campo Nome de usuário, especifique o nome de um usuário com privilégios de login para o host SSH (por exemplo, ec2-user). • Especifique o tipo de autenticação como Arquivo de identidade para que o pgAdmin use um arquivo de chave privada ao se conectar. • Inclua a localização do arquivo Privacy Enhanced Mail (PEM) no campo Arquivo de identidade. O arquivo.pem é o par de EC2 chaves da Amazon.	
Salve e conecte-se.	Escolha Salvar para concluir a configuração e conectar-se ao banco de dados Aurora compatível com o PostgreSQL usando o túnel SSH.	DBA

Recursos relacionados

- Diálogo do servidor
- Conectar-se ao servidor

Converta consultas JSON Oracle em SQL do banco de dados PostgreSQL

Criado por Pinesh Singal (AWS) e Lokesh Gurram (AWS)

Resumo

Esse processo de migração do on-premises para a nuvem da Amazon Web Services (AWS) usa a AWS Schema Conversion Tool (AWS SCT) para converter o código de um banco de dados Oracle em um banco de dados PostgreSQL. A maior parte do código é convertida automaticamente pela AWS SCT. No entanto, as consultas Oracle relacionadas ao JSON não são convertidas automaticamente.

A partir da versão Oracle 12.2, o Oracle Database suporta várias funções JSON que ajudam na conversão de dados baseados em JSON em dados baseados em ROW. No entanto, a AWS SCT não converte automaticamente dados baseados em JSON em linguagem compatível com o PostgreSQL.

Esse padrão de migração se concentra principalmente na conversão manual das consultas Oracle relacionadas ao JSON com funções como `JSON_OBJECT`, `JSON_ARRAYAGG` e `JSON_TABLE` de um banco de dados Oracle para um banco de dados PostgreSQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância do banco de dados Oracle on-premises (em funcionamento)
- Uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS) para PostgreSQL ou Amazon Aurora Edição Compatível com PostgreSQL (em funcionamento)

Limitações

- As consultas relacionadas ao JSON exigem um formato fixo de `KEY` e `VALUE`. Não usar esse formato retorna o resultado errado.
- Se alguma alteração na estrutura JSON adicionar novos pares `KEY` e `VALUE` na seção de resultados, o procedimento ou função correspondente deverá ser alterado na consulta SQL.
- Algumas funções relacionadas ao JSON são suportadas em versões anteriores do Oracle e do PostgreSQL, mas com menos recursos.

Versões do produto

- Oracle Database versão 12.2 e posterior
- Amazon RDS para PostgreSQL ou Aurora compatível com PostgreSQL versão 9.5 e posterior
- Versão mais recente da AWS SCT (testada usando a versão 1.0.664)

Arquitetura

Pilha de tecnologia de origem

- Uma instância de banco de dados Oracle com a versão 19c

Pilha de tecnologias de destino

- Uma instância de banco de dados do Amazon RDS para PostgreSQL ou Aurora compatível com PostgreSQL com a versão 13

Arquitetura de destino

1. Use a AWS SCT com o código da função JSON para converter o código-fonte do Oracle para o PostgreSQL.
2. A conversão produz arquivos .sql migrados compatíveis com o PostgreSQL.
3. Converta manualmente os códigos de função Oracle JSON não convertidos em códigos de função JSON do PostgreSQL.
4. Execute os arquivos .sql na instância de banco de dados de destino do Aurora compatível com o PostgreSQL.

Ferramentas

Serviços da AWS

- O Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado que é construído para a nuvem e compatível com o MySQL e o PostgreSQL.
- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.

- O AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.

Outros serviços

- O Oracle SQL Developer é um ambiente de desenvolvimento integrado que simplifica o desenvolvimento e o gerenciamento de bancos de dados Oracle em implantações tradicionais e baseadas em nuvem.
- pgAdmin ou. DBeaver O pgAdmin é uma ferramenta de gerenciamento de código aberto para o PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados. DBeaveré uma ferramenta de banco de dados universal.

Práticas recomendadas

A consulta Oracle tem o tipo `CAST` como padrão ao usar a função `JSON_TABLE`. Uma prática recomendada é usar `CAST` no PostgreSQL também, usando caracteres duplos maiores que caracteres (>>).

Para obter mais informações, consulte Postgres_SQL_Read_JSON na seção Informações adicionais.

Épicos

Gere os dados JSON nos bancos de dados Oracle e PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Armazene os dados JSON no banco de dados Oracle.	Crie uma tabela no banco de dados Oracle e armazene os dados JSON na coluna `CLOB`. Use o Oracle_Table_Creation_Insert_Script que está na seção Informações adicionais.	Engenheiro de migração
Armazene os dados JSON no banco de dados PostgreSQL.	Crie uma tabela no banco de dados PostgreSQL e armazene os dados JSON na coluna `TEXT`. Use o Postgres_	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	Table_Creation_Insert_Script que está na seção Informaçõ es adicionais.	

Converta o JSON em formato ROW

Tarefa	Descrição	Habilidades necessárias
Converta os dados JSON no banco de dados Oracle.	Escreva uma consulta Oracle SQL para ler os dados JSON no formato ROW. Para obter mais detalhes e exemplos de sintaxe, consulte Oracle_SQ L_Read_JSON na seção Informações adicionais.	Engenheiro de migração
Converta os dados JSON no banco de dados PostgreSQL.	Escreva uma consulta PostgreSQL para ler os dados JSON no formato ROW. Para obter mais detalhes e exemplos de sintaxe, consulte Postgres_SQL_Read_JSON na seção Informações adicionais.	Engenheiro de migração

Converta manualmente os dados JSON usando a consulta SQL e relate a saída no formato JSON

Tarefa	Descrição	Habilidades necessárias
Execute agregações e validação na consulta Oracle SQL.	Para converter manualmen te os dados JSON, execute uma junção, agregação e validação na consulta Oracle SQL e relate a saída no	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	formato JSON. Use o código em Oracle_SQL_JSON_Aggregation_Join na seção Informações adicionais. 1. JOIN: os dados formatados em JSON são passados como um parâmetro de entrada para a consulta. Um JOIN interno é feito entre esses dados estáticos e os dados JSON na tabela `aws_test_table` do banco de dados Oracle. 2. Agregação com validação: os dados JSON têm parâmetros de `KEY` e `VALUE` com valores como `accountNumber`, `parentAccountNumber`, `businessUnitId` e `positionId`, que são usados para agregações de `SUM` e `COUNT`. 3. Formato JSON: após a junção e a agregação, os dados são reportados no formato JSON usando `JSON_OBJECT` e `JSON_ARRAYAGG`.	

Tarefa	Descrição	Habilidades necessárias
Execute agregações e validação na consulta Postgres SQL.	Para converter manualmente os dados JSON, execute uma junção, agregação e validação na consulta PostgreSQL e relate a saída no formato JSON. Use o código em Postgres_SQL_JSON_ aggregation_join na seção Informações adicionais. 1. JOIN: os dados formatado s em JSON (`tab1`) são passados como um parâmetro de entrada para a consulta da cláusula `WITH`. Um JOIN é feito entre esses dados estáticos e os dados JSON, que estão na tabela `tab`. Um JOIN também é feito com a cláusula `WITH`, que tem dados JSON na tabela `aws_test_pg_table` . 2. Agregação: os dados JSON têm parâmetro s de `KEY` e `VALUE` com valores como `accountNu mber` ,`parentAcc ountNumber` , `businessUnitId` e `positionId` , que são usados para as agregações `SUM` e `COUNT`.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	3. Formato JSON: após a junção e a agregação, os dados são reportados no formato JSON usando `JSON_BUILD_OBJECT` e `JSON_AGG`.	

Converta o procedimento Oracle em uma função PostgreSQL que contém consultas JSON

Tarefa	Descrição	Habilidades necessárias
Converta as consultas JSON no procedimento Oracle em linhas.	Para o exemplo de procedimento Oracle, use a consulta Oracle anterior e o código em Oracle_Procedure_with_JSON_Query na seção Informações adicionais.	Engenheiro de migração
Converta as funções do PostgreSQL que têm consultas JSON em dados baseados em linhas.	Para os exemplos de funções do PostgreSQL, use a consulta anterior do PostgreSQL e o código que está em Postgres_Function_with_JSON_Query na seção Informações adicionais.	Engenheiro de migração

Recursos relacionados

- Funções Oracle JSON
- Funções JSON do PostgreSQL
- Exemplos de funções Oracle JSON
- Exemplos de funções JSON do PostgreSQL
- AWS Schema Conversion Tool

Mais informações

Para converter o código JSON do banco de dados Oracle para o banco de dados PostgreSQL, use os scripts a seguir, em ordem.

1. Oracle_Table_Creation_Insert_Script

```
create table aws_test_table(id number,created_on date default sysdate,modified_on
 date,json_doc clob);

REM INSERTING into EXPORT_TABLE
SET DEFINE OFF;
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc)
values (1,to_date('02-AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022
 12:30:14','DD-MON-YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -'",
    "a]')
|| TO_CLOB(q'[ccount" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
```

```
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
]')
|| TO_CLOB(q'[        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc) values (2,to_date('02-
AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022 12:30:14','DD-MON-
YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "pqr@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -'",
    "account" : {
      "companyId" : "CARS",
      "busin]')
|| TO_CLOB(q'[essUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
```

```
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
      ]')
|| TO_CLOB(q'[  "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));

commit;
```

2. Postgres_Table_Creation_Insert_Script

```
create table aws_test_pg_table(id int,created_on date ,modified_on date,json_doc text);
insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(1,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
```

```
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');


insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(2,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "a*b**@h**.k**",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "CARS",
      "businessUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
```

```
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');
```

3. Oracle_SQL_Read_JSON

Os blocos de código a seguir mostram como converter dados Oracle JSON em formato de linha.

Exemplo de consulta e sintaxe

```
SELECT   JSON_OBJECT(
 'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) ) FROM
    (SELECT   tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
```

```
           SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
clerk_count
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
 COLUMNS (
         parent_account_number NUMBER PATH
          '$.data.account.parentAccountNumber',
           account_number NUMBER PATH '$.data.account.accountNumber',
           business_unit_id NUMBER PATH '$.data.account.businessUnitId',
           position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
           ) AS tab_data
           INNER JOIN JSON_TABLE ( '{
       "accounts": [{
         "accountNumber": 42000,
         "parentAccountNumber": 32000,
         "businessUnitId": 7
       }, {
         "accountNumber": 42001,
         "parentAccountNumber": 32001,
         "businessUnitId": 6
       }]
     }', '$.accounts[*]' ERROR ON ERROR
     COLUMNS (
     parent_account_number PATH '$.parentAccountNumber',
     account_number PATH '$.accountNumber',
     business_unit_id PATH '$.businessUnitId')
     ) static_data
     ON ( static_data.parent_account_number = tab_data.parent_account_number
          AND static_data.account_number = tab_data.account_number
          AND static_data.business_unit_id = tab_data.business_unit_id )
       GROUP BY
           tab_data.business_unit_id,
           tab_data.parent_account_number,
           tab_data.account_number );
```

O documento JSON armazena os dados como coleções. Cada coleção pode ter pares de `KEY` e `VALUE`. Todos os `VALUE` podem ter pares de `KEY` e `VALUE` aninhados. A tabela a seguir fornece informações sobre como ler o `VALUE` específico do documento JSON.

CHAVE	HIERARCHY ou PATH a ser usado para obter o VALUE	VALUE
`profileType`	`metadata -> profileType`	"P"

positionId	data -> positionId	"0100"
accountNumber	data -> account -> accountNumber	42000

Na tabela anterior, o KEY profileType é um VALUE dos metadata KEY. O KEY positionId é um VALUE da data KEY. O KEY accountNumber é um VALUE da account KEY, e a account KEY é um VALUE da data KEY.

Exemplo de documento JSON

```
{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
"profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
"positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
"accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
```

```
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}
```

Consulta SQL usada para obter os campos selecionados do documento JSON

```
select parent_account_number,account_number,business_unit_id,position_id from
 aws_test_table aws,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
COLUMNS (
parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
account_number NUMBER PATH '$.data.account.accountNumber',
business_unit_id NUMBER PATH '$.data.account.businessUnitId',
position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'
)) as sc
```

Na consulta anterior, `JSON_TABLE` é uma função embutida no Oracle que converte os dados JSON em formato de linha. A função JSON_TABLE espera parâmetros no formato JSON.

Cada item em `COLUMNS` tem um `PATH` predefinido, e um `VALUE` apropriado para uma determinada `KEY` é retornado em formato de linha.

Resultado da consulta anterior

PARENT_AC COUNT_NUMBER	ACCOUNT_NUMBER	BUSINESS_UNIT_ID	POSITION_ID
32000	42000	7	0100
32001	4/2001	6	0090

4. Postgres_SQL_Read_JSON

Exemplo de consulta e sintaxe

```
select *
```

```
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::VARCHAR as positionId
from aws_test_pg_table) d ;
```

No Oracle, o PATH é usado para identificar o KEY e VALUE específicos. No entanto, o PostgreSQL usa um modelo HIERARCHY para leitura de KEY e VALUE a partir do JSON. Os mesmos dados JSON mencionados abaixo de Oracle_SQL_Read_JSON são usados nos exemplos a seguir.

Consulta SQL com tipo CAST não permitida

(Se você forçar o tipo CAST, a consulta falhará com um erro de sintaxe.)

```
select *
from (
select (json_doc::json->'data'->'account'->'parentAccountNumber') as
 parentAccountNumber,
(json_doc::json->'data'->'account'->'accountNumber')as accountNumber,
(json_doc::json->'data'->'account'->'businessUnitId') as businessUnitId,
(json_doc::json->'data'->'positionId')as positionId
from aws_test_pg_table) d ;
```

Usar um único operador maior que (>) retornará o VALUE definido para essa KEY. Por exemplo, KEY: positionId, e VALUE: "0100".

O tipo CAST não é permitido quando você usa o único operador maior que (>).

Consulta SQL com tipo CAST permitida

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) d ;
```

Para usar o tipo CAST, você deve usar o operador duplo maior que. Se você usar o único operador maior que, a consulta retornará o VALUE definido (por exemplo KEY: positionId e VALUE: "0100"). Usar o operador duplo maior que (>>) retornará o valor real definido para essa KEY (por exemplo, KEY: positionId e VALUE: 0100, sem aspas duplas).

No caso anterior, o parentAccountNumber é do tipo CAST para INT, accountNumber é do tipo CAST para INT, businessUnitId é do tipo CAST para INT e positionId é do tipo CAST para VARCHAR.

As tabelas a seguir mostram os resultados da consulta que explicam o papel do único operador maior que (>) e do operador duplo maior que (>>).

Na primeira tabela, a consulta usa o único operador maior que (>). Cada coluna está no tipo JSON e não pode ser convertida em outro tipo de dados.

parentAccountNumber	accountNumber	businessUnitId	positionId
2003565430	2003564830	7	"0100"
2005 284042	2005 284042	6	“0090”
2000272719	2000272719	1	"0100"

Na segunda tabela, a consulta usa o operador duplo maior que (>>). Cada coluna oferece suporte ao tipo CAST com base no valor da coluna. Por exemplo, INTEGER neste contexto.

parentAccountNumber	accountNumber	businessUnitId	positionId
2003565430	2003564830	7	0100
2005 284042	2005 284042	6	0090
2000272719	2000272719	1	0100

5. Oracle_SQL_JSON_Aggregation_Join

Consulta de exemplo

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
  COLUMNS (
          parent_account_number NUMBER PATH
           '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
```

```
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Para converter os dados em nível de linha no formato JSON, o Oracle tem funções integradas como `JSON_OBJECT`, `JSON_ARRAY`, `JSON_OBJECTAGG` e `JSON_ARRAYAGG`.

- `JSON_OBJECT` aceita dois parâmetros: `KEY` e `VALUE`. O parâmetro `KEY` deve ser codificado ou de natureza estática. O parâmetro `VALUE` é derivado da saída da tabela.
- O `JSON_ARRAYAGG` aceita `JSON_OBJECT` como parâmetro. Isso ajuda a agrupar o conjunto de elementos `JSON_OBJECT` como uma lista. Por exemplo, se você tiver um elemento `JSON_OBJECT` que tenha vários registros (vários pares de `KEY` e `VALUE` no conjunto de dados), o `JSON_ARRAYAGG` anexa o conjunto de dados e cria uma lista. De acordo com a linguagem Data Structure, `LIST` é um grupo de elementos. Nesse contexto, `LIST` é um grupo de elementos `JSON_OBJECT`.

O exemplo a seguir mostra um elemento `JSON_OBJECT`.

```
{
   "taxProfessionalCount": 0,
   "attorneyCount": 0,
   "nonAttorneyCount": 1,
   "clerkCount": 0
}
```

O próximo exemplo mostra dois elementos `JSON_OBJECT`, com `LIST` indicado por colchetes (`[ ]`).

```
[
    {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
,
    {
        "taxProfessionalCount": 2,
        "attorneyCount": 1,
        "nonAttorneyCount": 3,
        "clerkCount":4
      }
]
```

Exemplo de consulta SQL

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               )
                        )
                                          )
              )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE   0 END
```

```
           )      tax_count,
           SUM(CASE    WHEN tab_data.position_id = '0100' THEN        1    ELSE
 0 END
           )      attorney_count,

           SUM(CASE    WHEN tab_data.position_id = '0090' THEN        1    ELSE
 0 END
           )      non_attorney_count,

           SUM(CASE    WHEN tab_data.position_id = '0050' THEN        1    ELSE
 0 END
           )      clerk_count

       FROM
           aws_test_table scco,  JSON_TABLE ( json_doc, '$' ERROR ON ERROR
           COLUMNS (
           parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
           account_number NUMBER PATH '$.data.account.accountNumber',
           business_unit_id NUMBER PATH '$.data.account.businessUnitId',
           position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
           ) AS tab_data
           INNER JOIN JSON_TABLE ( '{
       "accounts": [{
         "accountNumber": 42000,
         "parentAccountNumber": 32000,
         "businessUnitId": 7
       }, {
         "accountNumber": 42001,
         "parentAccountNumber": 32001,
         "businessUnitId": 6
       }]
     }', '$.accounts[*]' ERROR ON ERROR
     COLUMNS (
     parent_account_number PATH '$.parentAccountNumber',
     account_number PATH '$.accountNumber',
     business_unit_id PATH '$.businessUnitId')
     ) static_data ON ( static_data.parent_account_number =
tab_data.parent_account_number
                        AND static_data.account_number = tab_data.account_number

                        AND static_data.business_unit_id =
tab_data.business_unit_id )
       GROUP BY
           tab_data.business_unit_id,
```

```
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Exemplo de saída da consulta SQL anterior

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

6. Postgres_SQL_JSON_Aggregation_Join

As funções incorporadas do PostgreSQL `JSON_BUILD_OBJECT` e `JSON_AGG` convertem os dados em nível de LINHA no formato JSON. A `JSON_BUILD_OBJECT` e `JSON_AGG` do PostgreSQL são equivalentes à `JSON_OBJECT` e `JSON_ARRAYAGG` do Oracle.

Consulta de exemplo

```
select
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            )
        )
    )
)
from (
with tab as (select * from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) a ) ,
tab1 as ( select
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer
 businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
from (
select '{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }'::json as jc) b)
```

```
select
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
from tab1,tab
where tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
and tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
and tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
```

Exemplo de saída da consulta anterior

A saída do Oracle e do PostgreSQL é exatamente a mesma.

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
```

```
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

7.Oracle_procedure_with_JSON_Query

Esse código converte o procedimento Oracle em uma função PostgreSQL que tem consultas SQL JSON. Mostra como a consulta transpõe o JSON em linhas e vice-versa.

```
CREATE OR REPLACE PROCEDURE p_json_test(p_in_accounts_json IN varchar2,
 p_out_accunts_json  OUT varchar2)
IS
BEGIN
/*
p_in_accounts_json paramter should have following format:
       {
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }
*/
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
```

```
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
into p_out_accunts_json
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
        FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( p_in_accounts_json, '$.accounts[*]' ERROR ON ERROR

      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
EXCEPTION
WHEN OTHERS THEN
   raise_application_error(-20001,'Error while running the JSON query');
END;
```

```
/
```

Executando o procedimento

O bloco de código a seguir explica como você pode executar o procedimento Oracle criado anteriormente com um exemplo de entrada JSON para o procedimento. Também fornece o resultado ou a saída desse procedimento.

```
set serveroutput on;
declare
v_out varchar2(30000);
v_in varchar2(30000):= '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }';
begin
  p_json_test(v_in,v_out);
  dbms_output.put_line(v_out);
end;
/
```

Saída do procedimento

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
```

```
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

8.Postgres_function_with_JSON_Query

Exemplos de função

```
CREATE OR REPLACE  FUNCTION f_pg_json_test(p_in_accounts_json  text)
RETURNS text
LANGUAGE plpgsql
AS
$$
DECLARE
 v_out_accunts_json   text;
BEGIN
SELECT
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            ))))
INTO v_out_accunts_json
```

```
FROM (
WITH tab AS (SELECT * FROM (
SELECT (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER AS
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER AS accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER AS businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar AS positionId
FROM aws_test_pg_table) a ) ,
tab1 AS ( SELECT
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
FROM (
SELECT p_in_accounts_json::json AS jc) b)
SELECT
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
FROM tab1,tab
WHERE tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
AND tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
AND tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
RETURN v_out_accunts_json;
END;
$$;
```

Execução da função

```
select    f_pg_json_test('{
        "accounts": [{
          "accountNumber": 42001,
```

```
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }')   ;
```

Saída da função

A saída a seguir é semelhante à saída do procedimento Oracle. A diferença é que essa saída está no formato de texto.

```
{
  "accountCounts": [
    {
      "businessUnitId": "6",
      "parentAccountNumber": "32001",
      "accountNumber": "42001",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": "7",
      "parentAccountNumber": "32000",
      "accountNumber": "42000",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

Copie tabelas do Amazon DynamoDB entre contas usando AWS Backup

Criado por Ramkumar Ramanujam (AWS)

Resumo

Ao trabalhar com o Amazon DynamoDB AWS no, um caso de uso comum é copiar ou sincronizar tabelas do DynamoDB em ambientes de desenvolvimento, teste ou preparação com os dados da tabela que estão no ambiente de produção. Como prática padrão, cada ambiente usa um diferente Conta da AWS.

AWS Backup suporta backup e restauração de dados entre regiões e entre contas para DynamoDB, Amazon Simple Storage Service (Amazon S3) e outros. Serviços da AWS Esse padrão fornece as etapas para usar o backup e a restauração AWS Backup entre contas para copiar tabelas do DynamoDB entre elas. Contas da AWS

Pré-requisitos e limitações

Pré-requisitos

- Dois ativos Contas da AWS que pertencem à mesma organização em AWS Organizations
- Permissões para criar tabelas do DynamoDB em ambas as contas
- AWS Identity and Access Management Permissões (IAM) para criar e usar AWS Backup cofres

Limitações

- A origem e o destino Contas da AWS devem fazer parte da mesma organização em AWS Organizations.

Arquitetura

Pilha de tecnologias de destino

- AWS Backup
- Amazon DynamoDB

Arquitetura de destino

1. Crie o backup da tabela do DynamoDB no cofre de backup AWS Backup na conta de origem.
2. Copie o backup para o cofre de backup na conta de destino.
3. Restaure a tabela do DynamoDB na conta de destino usando o backup do cofre de backup na conta de destino.

Automação e escala

Você pode usar AWS Backup para programar backups para serem executados em intervalos específicos.

Ferramentas

- AWS Backupé um serviço totalmente gerenciado para centralizar e automatizar a proteção de dados na nuvem e no local. Serviços da AWS Usando esse serviço, você pode configurar políticas de backup e monitorar a atividade de seus AWS recursos em um só lugar. Ele permite automatizar e consolidar tarefas de backup que antes eram executadas serviço por serviço e elimina a necessidade de criar scripts personalizados e processos manuais.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade integrada.

Épicos

Ativar AWS Backup recursos nas contas de origem e de destino

Tarefa	Descrição	Habilidades necessárias
Ative os atributos avançados para o DynamoDB e o backup entre contas.	Tanto na origem quanto no destino Contas da AWS, faça o seguinte: 1. No AWS Managemen t Console, abra o AWS Backup console. 2. Escolha Settings. 3. Em Atributos avançados para backups do Amazon	AWS DevOps, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	DynamoDB, confirme se os Atributos avançados estão habilitados ou escolha Ativar. 4. Em Gerenciamento entre contas, em Backup entre contas, escolha Habilitar.	

Crie cofres de backup nas contas de origem e de destino

Tarefa	Descrição	Habilidades necessárias
Crie cofres de backup	Tanto na origem quanto no destino Contas da AWS, faça o seguinte: 1. No AWS Backup console, escolha Backup vaults. 2. Escolha Criar cofre de backup. 3. Copie o nome do recurso da Amazon (ARN) do cofre de backup e salve-o. Os cofres ARNs de backup de origem e de destino serão necessários quando você copiar o backup da tabela do DynamoDB entre as contas de origem e de destino.	AWS DevOps, engenheiro de migração

Execute backup e restauração usando cofres de backup

Tarefa	Descrição	Habilidades necessárias
Na conta de origem, crie uma tabela do DynamoDB.	Para criar um backup para a tabela do DynamoDB na conta de origem, faça o seguinte: 1. Na página AWS Backup Painel, escolha Criar backup sob demanda. 2. Na seção Configurações, em Tipo de recurso, selecione DynamoDB e, em seguida, selecione o nome da tabela. 3. Na lista suspensa Cofre de backup, selecione o cofre de backup que você criou na conta de origem. 4. Selecione o Período de retenção desejado. 5. Escolha Criar backup sob demanda. Uma nova tarefa de backup é criada. Para monitorar o status da tarefa de backup, na página AWS Backup Trabalhos, escolha a guia Trabalhos de Backup. Todas as tarefas de backup ativas, em andamento e concluídas estão listadas nessa guia.	AWS DevOps, DBA, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Copie o backup da conta de origem para a conta de destino.	Depois que a tarefa de backup for concluída, copie o backup da tabela do DynamoDB do cofre de backup na conta de origem para o cofre de backup na conta de destino. Para copiar o cofre de backup, na conta de origem, faça o seguinte: 1. No AWS Backup console, escolha Backup vaults. 2. Em Backups, escolha o backup da tabela do DynamoDB. 3. Selecione Actions (Ações) e Copy (Copiar). 4. Insira o Região da AWS da conta de destino. 5. Em ARN do cofre externo, insira o ARN do cofre de backup que você criou na conta de destino. 6. Para copiar backups da conta de origem para a conta de destino, no cofre de backup da conta de destino, habilite o acesso de uma conta diferente.	AWS DevOps, engenheiro de migração, DBA

Tarefa	Descrição	Habilidades necessárias
Restaure o backup na conta de destino.	No alvo Conta da AWS, faça o seguinte: 1. No AWS Backup console, escolha Backup vaults. 2. Em Backups, selecione o backup que você copiou da conta de origem. 3. Em Ações, escolha Reiniciar. 4. Insira o nome da tabela do DynamoDB de destino que você deseja restaurar.	AWS DevOps, DBA, engenheiro de migração

Recursos relacionados

- Usando AWS Backup com o DynamoDB
- Criação de cópias de backup em Contas da AWS
- AWS Backup preços

Copiar tabelas do Amazon DynamoDB entre contas usando uma implementação personalizada

Criado por Ramkumar Ramanujam (AWS)

Resumo

Ao trabalhar com o Amazon DynamoDB no Amazon Web Services (AWS), um caso de uso comum é copiar ou sincronizar tabelas do DynamoDB em ambientes de desenvolvimento, teste ou preparação com os dados da tabela que estão no ambiente de produção. Como prática padrão, cada ambiente usa uma conta diferente da AWS.

O DynamoDB agora fornece suporte ao backup entre contas usando o AWS Backup. Para obter informações sobre os custos de armazenamento associados ao uso do AWS Backup, consulte os Preços do AWS Backup. Quando você usa o AWS Backup para copiar entre contas, as contas de origem e de destino devem fazer parte de uma organização do AWS Organizations. Existem outras soluções para backup e restauração entre contas usando serviços da AWS, como o AWS Glue. O uso dessas soluções, no entanto, aumenta o espaço ocupado pelo aplicativo porque há mais serviços da AWS para implantar e manter.

Você também pode usar o Amazon DynamoDB Streams para registrar alterações na tabela na conta de origem. Em seguida, você pode iniciar uma função do AWS Lambda e fazer as alterações correspondentes na tabela de destino na conta de destino. Mas essa solução se aplica a casos de uso nos quais as tabelas de origem e destino devem sempre ser mantidas em sincronia. Isso talvez não se aplique a ambientes de desenvolvimento, teste e preparação em que os dados são atualizados com frequência.

Esse padrão fornece etapas para implementar uma solução personalizada para copiar uma tabela do Amazon DynamoDB de uma conta para outra. Esse padrão pode ser implementado usando linguagens de programação comuns, como C#, Java e Python. Recomendamos usar uma linguagem compatível com um AWS SDK.

Pré-requisitos e limitações

Pré-requisitos

- Duas contas da AWS ativas
- Tabelas do DynamoDB em ambas as contas
- Conhecimento do perfil e política do AWS Identity and Access Management (IAM)

- Informações sobre como acessar tabelas do Amazon DynamoDB usando qualquer linguagem de programação comum, como C#, Java ou Python

Limitações

Esse padrão se aplica às tabelas do DynamoDB com cerca de 2 GB ou menos. Com lógica adicional para lidar com interrupções de conexão ou sessão, controle de utilização, falhas e novas tentativas, ele pode ser usado para tabelas maiores.

A operação de verificação do DynamoDB, que lê itens da tabela de origem, pode buscar somente até 1 MB de dados em uma única chamada. Para tabelas maiores, superiores a 2 GB, essa limitação pode aumentar o tempo total para a realização de uma cópia completa.

Arquitetura

O diagrama a seguir mostra a implementação personalizada entre as contas de origem e de destino da AWS. As políticas do IAM e os tokens de segurança são usados com a implementação personalizada. Os dados são lidos do Amazon DynamoDB na conta de origem e gravados no DynamoDB na conta de destino.

Automação e escala

Esse padrão se aplica às tabelas do DynamoDB com cerca de 2 GB ou menos.

Para aplicar esse padrão a tabelas maiores, resolva os seguintes problemas:

- Durante a operação de cópia da tabela, duas sessões ativas são mantidas usando tokens de segurança diferentes. Se a operação de cópia da tabela demorar mais do que os prazos de expiração do token, você deverá implementar uma lógica para atualizar os tokens de segurança.
- Se unidades de capacidade de leitura (RCUs) e unidades de capacidade de gravação (WCUs) suficientes não forem provisionadas, as leituras ou gravações na tabela de origem ou de destino poderão ser limitadas. Certifique-se de identificar e lidar com essas exceções.
- Lide com quaisquer outras falhas ou exceções e implemente um mecanismo de repetição para tentar novamente ou continuar do ponto no qual a operação de cópia falhou.

Ferramentas

Ferramentas

- Amazon DynamoDB: o Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade integrada.
- As ferramentas adicionais necessárias serão diferentes com base na linguagem de programação que você escolher para a implementação. Por exemplo, se você usa C#, precisará do Microsoft Visual Studio e dos seguintes NuGet pacotes:
  - `AWSSDK`
  - `AWSSDK.DynamoDBv2`

Código

O trecho de código Python a seguir exclui e recria uma tabela do DynamoDB usando a biblioteca do Boto3.

Não use o `AWS_ACCESS_KEY_ID` e a `AWS_SECRET_ACCESS_KEY` de um usuário do IAM porque são credenciais de longo prazo que devem ser evitadas para acesso programático aos serviços da AWS. Para obter mais informações sobre as credenciais temporárias, consulte a seção Práticas recomendadas.

O `AWS_ACCESS_KEY_ID`, a `AWS_SECRET_ACCESS_KEY` e o `TEMPORARY_SESSION_TOKEN` usados no trecho de código a seguir são credenciais temporárias obtidas do AWS Security Token Service (AWS STS).

```
import boto3
import sys
import json

#args = input-parameters = GLOBAL_SEC_INDEXES_JSON_COLLECTION,
 ATTRIBUTES_JSON_COLLECTION, TARGET_DYNAMODB_NAME, TARGET_REGION, ...

#Input param: GLOBAL_SEC_INDEXES_JSON_COLLECTION
#[{"IndexName":"Test-index","KeySchema":[{"AttributeName":"AppId","KeyType":"HASH"},
{"AttributeName":"AppType","KeyType":"RANGE"}],"Projection":
{"ProjectionType":"INCLUDE","NonKeyAttributes":["PK","SK","OwnerName","AppVersion"]}}]

#Input param: ATTRIBUTES_JSON_COLLECTION
#[{"AttributeName":"PK","AttributeType":"S"},
{"AttributeName":"SK","AttributeType":"S"},
{"AttributeName":"AppId","AttributeType":"S"},
{"AttributeName":"AppType","AttributeType":"N"}]
```

```
region = args['TARGET_REGION']
target_ddb_name = args['TARGET_DYNAMODB_NAME']

global_secondary_indexes = json.loads(args['GLOBAL_SEC_INDEXES_JSON_COLLECTION'])
attribute_definitions = json.loads(args['ATTRIBUTES_JSON_COLLECTION'])

# Drop and create target DynamoDB table
dynamodb_client = boto3.Session(
        aws_access_key_id=args['AWS_ACCESS_KEY_ID'],
        aws_secret_access_key=args['AWS_SECRET_ACCESS_KEY'],
        aws_session_token=args['TEMPORARY_SESSION_TOKEN'],
    ).client('dynamodb')

# Delete table
print('Deleting table: ' + target_ddb_name + ' ...')

try:
    dynamodb_client.delete_table(TableName=target_ddb_name)

    #Wait for table deletion to complete
    waiter = dynamodb_client.get_waiter('table_not_exists')
    waiter.wait(TableName=target_ddb_name)
    print('Table deleted.')
except dynamodb_client.exceptions.ResourceNotFoundException:
    print('Table already deleted / does not exist.')
    pass

print('Creating table: ' + target_ddb_name + ' ...')

table = dynamodb_client.create_table(
    TableName=target_ddb_name,
    KeySchema=[
        {
            'AttributeName': 'PK',
            'KeyType': 'HASH'  # Partition key
        },
        {
            'AttributeName': 'SK',
            'KeyType': 'RANGE'  # Sort key
        }
    ],
    AttributeDefinitions=attribute_definitions,
    GlobalSecondaryIndexes=global_secondary_indexes,
    BillingMode='PAY_PER_REQUEST'
```

```
)

waiter = dynamodb_client.get_waiter('table_exists')
waiter.wait(TableName=target_ddb_name)

print('Table created.')
```

Práticas recomendadas

Credenciais temporárias

Como melhor prática de segurança, ao acessar os serviços da AWS de forma programática, evite usar a `AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY` de um usuário do IAM, pois essas são credenciais de longo prazo. Sempre tente usar credenciais temporárias para acessar os serviços da AWS de forma programática.

Por exemplo, um desenvolvedor codifica o `AWS_ACCESS_KEY_ID` e a `AWS_SECRET_ACCESS_KEY` de um usuário do IAM no aplicativo durante o desenvolvimento, mas não consegue remover os valores codificados antes de enviar as alterações para o repositório de códigos. Essas credenciais expostas podem ser usadas por usuários mal-intencionados ou maliciosos, o que pode ter sérias implicações (principalmente se as credenciais expostas tiverem privilégios de administrador). Essas credenciais expostas devem ser desativadas ou excluídas imediatamente usando o console do IAM ou a AWS Command Line Interface (AWS CLI).

Sempre tente usar credenciais temporárias para acessar os serviços da AWS de forma programática. As credenciais temporárias são válidas somente pelo tempo especificado (de 15 minutos a 36 horas). A duração máxima permitida de credenciais temporárias varia de acordo com fatores como configurações de função e encadeamento de funções. Para obter mais informações sobre a AWS STS, consulte a documentação.

Épicos

Configurar tabelas do DynamoDB

Tarefa	Descrição	Habilidades necessárias
Crie uma tabela do DynamoDB.	Crie tabelas do DynamoDB, com índices, nas contas de origem e de destino da AWS.	Desenvolvedor de aplicativos, DBA, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	Defina o provisionamento de capacidade como modo sob demanda, o que permite que o DynamoDB escale dinamicamente as capacidades de leitura/gravação com base na workload. Como alternativa, você pode usar a capacidade provisionada com 4000 RCUs e 4000. WCUs	
Preencha a tabela de origem.	Preencha a tabela do DynamoDB na conta de origem com dados de teste. Ter pelo menos 50 MB ou mais de dados de teste ajuda você a ver o pico e a média RCUs consumidos durante a cópia da tabela. Em seguida, você pode alterar o provisionamento de capacidade conforme necessário.	Desenvolvedor de aplicativos, DBA, engenheiro de migração

Configurar credenciais para acessar as tabelas do DynamoDB

Tarefa	Descrição	Habilidades necessárias
Crie perfis do IAM para acessar as tabelas de origem e destino do DynamoDB.	Crie um perfil do IAM na conta de origem com permissões para acessar (ler) a tabela do DynamoDB na conta de origem.	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Adicione a conta de origem como uma entidade confiável para esse perfil. Crie um perfil do IAM na conta de destino com permissões para acessar (criar, ler, atualizar, excluir) a tabela do DynamoDB na conta de destino. Adicione a conta de destino como uma entidade confiável para esse perfil.	

Copiar dados da tabela de uma conta para outra

Tarefa	Descrição	Habilidades necessárias
Obtenha credenciais temporárias para os perfis do IAM.	Obtenha credenciais temporárias para o perfil do IAM criado na conta de origem. Obtenha credenciais temporárias para o perfil do IAM criado na conta de destino. Uma forma de obter as credenciais temporárias para o perfil do IAM é usar o AWS STS da AWS CLI. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/<role-name> --`	Desenvolvedor de aplicativos, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	`role-session-name <session-name> --profile <profile-name>` Use o perfil apropriado da AWS (correspondente à conta de origem ou de destino). Para obter mais informaçõ es sobre as credenciais de segurança temporárias, consulte: • Referência de APIs do AWS Security Token Service • Obtenção de credenciais do perfil do IAM para acesso à CLI	

Tarefa	Descrição	Habilidades necessárias
Inicialize os clientes DynamoDB para acesso ao DynamoDB de origem e de destino.	Inicialize os clientes DynamoDB, que são fornecidos pelo AWS SDK, para as tabelas de origem e de destino do DynamoDB. • Para o cliente DynamoDB de origem, use as credenciais temporárias obtidas da conta de origem. • Para o cliente DynamoDB de origem, use as credenciais temporárias obtidas da conta de destino. Para obter mais informações sobre como fazer solicitações usando credenciais temporárias do IAM, consulte a documentação da AWS.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Solte e recrie a tabela de destino.	Exclua e recrie a tabela do DynamoDB de destino (junto com os índices) na conta de destino usando o cliente DynamoDB da conta de destino. Excluir todos os registros de uma tabela do DynamoDB é uma operação cara porque consome provisionados. WCUs Excluir e recriar a tabela evita esses custos extras. Você pode adicionar índices a uma tabela depois de criá-la, mas isso leva de dois a cinco minutos a mais. Criar índices durante a criação da tabela, transferindo a coleção de índices para a chamada `createTable` , é mais eficiente.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Execute a cópia da tabela.	Repita as etapas a seguir até que todos os dados sejam copiados: • Execute uma verificação na tabela na conta de origem usando o cliente DynamoDB de origem. Cada verificação do DynamoDB recupera somente 1 MB de dados da tabela, então você deve repetir essa operação até que todos os itens ou registros sejam lidos. • Para cada conjunto de itens verificados, grave os itens na tabela na conta de destino com o cliente DynamoDB de destino ao usar a chamada `BatchWriteItem` no AWS SDK para DynamoDB. Isso reduz o número de solicitações `PutItem` feitas ao DynamoDB. • `BatchWriteItem` tem uma limitação de 25 gravações ou colocações, ou até 16 MB. Você deve adicionar lógica para acumular itens verificados em contagens de 25 antes de chamar `BatchWriteItem`. `BatchWrit`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`eItem` retorna uma lista de itens que não puderam ser copiados com sucesso. Usando essa lista, adicione a lógica de nova tentativa para realizar outra chamada `BatchWriteItem` somente com os itens que não tiveram êxito. Para obter mais informaçõ es, consulte a implementação de referência em C# (para eliminar, criar e preencher tabelas) na seção Anexos. Um exemplo de arquivo de notação de JavaScript objeto de configuração de tabela (JSON) também está anexado.	

Recursos relacionados

- Documentação do Amazon DynamoDB
- Criação de um usuário do IAM na sua conta da AWS
- AWS SDKs
- Uso de credenciais temporárias com recursos da AWS

Mais informações

Esse padrão foi implementado usando C# para copiar uma tabela do DynamoDB com 200.000 itens (tamanho médio do item de 5 KB e tamanho da tabela de 250 MB). A tabela de destino do DynamoDB foi configurada com capacidade provisionada de 4000 e 4000. RCUs WCUs

A operação completa de cópia da tabela (da conta de origem para a conta de destino), incluindo a remoção e a recriação da tabela, levou cinco minutos. Total de unidades de capacidade consumidas: 30.000 RCUs e aproximadamente WCUs 400.000.

Para obter mais informações sobre os modos de capacidade do DynamoDB, consulte Modo de capacidade de leitura/gravação na documentação da AWS.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie relatórios detalhados de custos e uso para o Amazon RDS e o Amazon Aurora

Criado por Lakshmanan Lakshmanan (AWS) e Sudarshan Narasimhan

Resumo

Este padrão mostra como rastrear os custos de uso dos clusters Amazon Relational Database Service (Amazon RDS) ou Amazon Aurora configurando tags de alocação de custos definidas pelo usuário. Você pode usar essas tags para criar relatórios detalhados de custo e uso no Explorador de Custos da AWS para clusters em várias dimensões. Por exemplo, você pode rastrear os custos de uso no nível da equipe, do projeto ou do centro de custo, e, em seguida, analisar os dados no Amazon Athena.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma ou mais instâncias do Amazon RDS ou Amazon Aurora

Limitações

Para restrições de tags, consulte o Guia do usuário do AWS Billing.

Arquitetura

Pilha de tecnologias de destino

- Amazon RDS ou Amazon Aurora
- Relatório de custos e uso da AWS
- AWS Cost Explorer
- Amazon Athena

Fluxo de trabalho e arquitetura

O fluxo de trabalho de marcação e análise consiste nas seguintes etapas:

1. Um engenheiro de dados, administrador de banco de dados ou administrador da AWS cria tags de alocação de custos definidas pelo usuário para os clusters do Amazon RDS ou Aurora.
2. Um administrador da AWS ativa as tags.
3. As tags reportam metadados para o Explorador de Custos da AWS.
4. Um engenheiro de dados, administrador de banco de dados ou administrador da AWS cria um relatório mensal de alocação de custos.
5. Um engenheiro de dados, administrador de banco de dados ou administrador da AWS analisa o relatório mensal de alocação de custos usando o Amazon Athena.

O diagrama a seguir mostra como aplicar tags para monitorar os custos de uso das instâncias do Amazon RDS ou do Aurora.

O diagrama de arquitetura a seguir mostra como o relatório de alocação de custos é integrado ao Amazon Athena para análise.

O relatório de alocação de custos mensal é armazenado em um bucket do Amazon S3 que você especificar. Quando você configura o Athena com o CloudFormation modelo da AWS, conforme descrito na seção Epics, o modelo fornece vários recursos adicionais, incluindo um rastreador do AWS Glue, um banco de dados do AWS Glue, um evento do Amazon Simple Notification System (Amazon SNS), funções do AWS Lambda e funções do AWS Identity and Access Management (IAM) para as funções do Lambda. À medida que novos arquivos de dados de custo chegam ao bucket do S3, as notificações de eventos são usadas para encaminhar esses arquivos a uma função do Lambda para processamento. A função do Lambda inicia uma tarefa de crawler do AWS Glue para criar ou atualizar a tabela no catálogo de dados do AWS Glue. Em seguida, essa tabela é usada para consultar dados no Athena.

Ferramentas

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão.
- O Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado que é construído para a nuvem e compatível com o MySQL e o PostgreSQL.

- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- CloudFormationA AWS é um serviço de infraestrutura como código (IaC) que permite modelar, provisionar e gerenciar facilmente recursos da AWS e de terceiros.
- O Explorador de Custos da AWS permite que você visualize e analise seus custos e uso.

Épicos

Crie e ative tags para seus clusters do Amazon RDS e Aurora

Tarefa	Descrição	Habilidades necessárias
Crie tags de alocação de custos definidas pelo usuário para seus clusters do Amazon RDS ou Aurora.	Para adicionar tags a um cluster novo ou existente do Amazon RDS ou do Aurora, siga as instruções em Adição, listagem e remoção de tags no Guia do usuário do Amazon Aurora. **Note** Para obter informaçõ es sobre como configurar um cluster Amazon Aurora, consulte as instruçõe s para MySQL e PostgreSQL no Guia do usuário do Amazon Aurora.	Administrador da AWS, engenheiro de dados, DBA
Ativar as tags de alocação de custos definidas pelo usuário.	Siga as instruções em Ativação de tags de alocação de custos definidas pelo	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	usuário no Guia do usuário do AWS Billing.	

Criação de relatórios de custos e uso

Tarefa	Descrição	Habilidades necessárias
Crie e configure relatórios de custo e uso para seus clusters.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Console de Faturamento da AWS. 2. No painel de navegação à esquerda, escolha Relatórios de Custos e Uso. 3. Escolha Criar relatório. 4. Forneça um nome de relatório, mantenha as configurações padrão para outras opções e escolha Próximo. 5. Escolha Configurar e forneça os detalhes de um bucket existente do S3. Você também pode optar por criar um novo bucket do S3 a partir dessa tela. Escolha Próximo. 6. Verifique a política padrão que será aplicada ao seu bucket, marque a caixa de seleção de confirmação e escolha Salvar.	Proprietário do aplicativo, administrador da AWS, DBA, AWS geral, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	7. Em Prefixo do caminho do relatório, digite o prefixo que você deseja colocar no início do nome do relatório. 8. Em Granularidade de tempo, escolha Por hora, Por dia ou Por mês, dependendo da frequência com que você deseja que os dados sejam coletados para o relatório. 9. Em Versionamento do relatório, escolha se você deseja que novas versões do relatório sejam criadas separadamente ou que o relatório existente seja substituído por cada versão. 10. Em Habilitar a integração de dados de relatórios para, escolha Amazon Athena. Verifique se o tipo de compressão está definido como Parquet. 11. Escolha Próximo. 12. Depois de rever as configurações de seu relatório, escolha Revisar e concluir. Os dados estarão disponíveis em 24 horas.	

Analisar dados do relatório de custos e uso

Tarefa	Descrição	Habilidades necessárias
Analisar dados do relatório de custos e uso.	1. Configure e use o Athena para analisar os dados do relatório. Para obter instruções, consulte Consulta dos relatórios de custos e uso utilizando o Amazon Athena no Guia do usuário dos relatórios de custos e uso da AWS. Recomendamos que você use o CloudFormation modelo da AWS fornecido pela Athena. 2. Execute consultas do Athena. Por exemplo, você pode usar a consulta SQL a seguir para verificar o status da atualização dos dados. `select status from cost_and_usage_data_status` Para obter mais informações, consulte Como executar consultas no Amazon Athena no Guia do usuário dos Relatórios de Custos e Uso do AWS.	Proprietário do aplicativo, administrador da AWS, DBA, AWS geral, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	Note Ao executar sua consulta SQL, verifique se o banco de dados correto está selecionado na lista suspensa.	

Recursos relacionados

Referências

- Configurar o Athena usando CloudFormation modelos da AWS (recomendado)
- Configuração manual do Athena
- Execução de consultas do Amazon Athena
- Carregar dados do relatório para outros recursos

Tutoriais e vídeos

- Analise relatórios de custo e uso usando o Amazon Athena (vídeo) YouTube

Implante instâncias de cluster de failover do SQL Server na Amazon EC2 e na Amazon FSx usando o Terraform

Criado por Mark Hudson (AWS) e Matt Burgess (AWS)

Resumo

Esse padrão usa o Terraform para implantar instâncias de cluster de failover do SQL Server (FCIs) em nós do Windows Server Failover Cluster (WSFC) no Amazon Elastic Compute Cloud (Amazon). EC2 Além disso, o padrão usa o armazenamento FSx compartilhado da Amazon para dados e arquivos de log.

Quando os bancos de dados do SQL Server são migrados para AWS, a primeira opção é o Amazon RDS for SQL Server. No entanto, às vezes o Amazon RDS for SQL Server não é adequado e o SQL Server deve ser implantado na EC2 Amazon em uma arquitetura altamente disponível. Nessa solução, o SQL Server FCIs é instalado nos nós do WSFC.

O módulo Terraform incluído nesse padrão provisiona até duas instâncias EC2 do Amazon SQL Server. Um sistema de arquivos Amazon FSx para Windows File Server atua como testemunha do quórum e armazena dados compartilhados e arquivos de log. Independentemente do número de instâncias configuradas, os nós da instância do SQL Server sempre criarão e ingressarão em um cluster FCI para garantir a paridade ambiental. (Normalmente, uma instância é configurada para desenvolvimento e duas instâncias para ambientes de produção.) Para configurações que usam dois nós para alta disponibilidade, um Network Load Balancer interno é provisionado. O Network Load Balancer usa uma sonda de integridade configurada no cluster FCI para identificar qual nó é o principal.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Amazon Virtual Private Cloud (Amazon VPC) com duas sub-redes em zonas de disponibilidade separadas.
- Conjunto de opções DHCP do Amazon VPC. Configure o nome de domínio para resolver seu nome de domínio do Active Directory e o domínio e os servidores de nomes NetBIOS para apontar para seus controladores de domínio do Active Directory. Para obter mais informações, consulte Configuração de VPC em Informações adicionais.

- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD).
- Imagem de máquina personalizada da Amazon (AMI). Para obter mais detalhes, consulte Configuração da AMI em Informações adicionais.
- Bucket do Amazon Simple Storage Service (Amazon S3) contendo a imagem ISO do SQL Server. Esse pré-requisito só é necessário se você estiver usando o EC2 Image Builder com o `component.yaml` arquivo fornecido para criar a AMI personalizada.
- AWS Key Management Service (AWS KMS) chave de criptografia.
- Por padrão, o SQL Server é instalado usando uma chave do produto Developer Edition. Espera-se que os sistemas de produção usem uma chave de produto válida passada para o módulo pela variável relevante.

Limitações

- Essa solução requer AWS Managed Microsoft AD. No entanto, se preferir, você pode usar uma implementação autogerenciada do Active Directory em vez disso. Para fazer isso, modifique o módulo Amazon FSx Terraform incluído para remover o `active_directory_id` atributo. Em seguida, adicione os quatro atributos necessários para o Active Directory autogerenciado, conforme mostrado na documentação do Terraform.
- O SQL Server está configurado para usar a autenticação de modo misto. Se preferir, você pode usar a autenticação somente para Windows. Para fazer isso, no script de dados do usuário fornecido, remova os `/SAPWD` parâmetros `/SECURITYMODE` e fornecidos ao `setup.exe` comando. Você pode remover o `sql_accounts.tf` arquivo e modificá-lo para remover a `sql_sa_password` entrada. `instances.tf`
- Ao excluir um cluster implantado, você deve remover os objetos correspondentes do computador virtual e os objetos individuais do computador no Active Directory. Para remover os objetos, use as ferramentas administrativas do Active Directory.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

Essa solução foi testada com as seguintes versões:

- Windows Server 2019

- SQL Server 2019
- Terraform v0.13.0

Arquitetura

Pilha de tecnologia de origem

- SQL Server

Pilha de tecnologias de destino

- SQL Server FCI em nós WSFC usando a Amazon EC2
- Servidor FSx de arquivos Amazon para Windows
- Bucket do Amazon S3
- AWS Secrets Manager
- AWS Managed Microsoft AD
- AWS KMS
- AWS Identity and Access Management (IAM)

Arquitetura de destino

O diagrama a seguir mostra a arquitetura dessa solução.

O diagrama mostra o seguinte:

- Uma função do IAM que fornece às EC2 instâncias acesso ao Secrets Manager AWS KMS e ao Secrets Manager
- Dois nós do SQL Server implantados em EC2 instâncias da Amazon em sub-redes privadas em duas zonas de disponibilidade
- Um Network Load Balancer para facilitar as conexões com a instância ativa do SQL Server (não implantado ao configurar um cluster de nó único)
- Sistema de arquivos Amazon FSx para Windows File Server implantado em ambas as sub-redes privadas para armazenamento compartilhado pelos nós do SQL Server
- Secrets Manager para armazenar credenciais e configurações do Active Directory e do SQL Server

- Bucket Amazon S3 para armazenar a imagem de instalação do SQL Server
- AWS Managed Microsoft AD para autenticação do Windows
- AWS KMS para criar a chave de criptografia

Automação e escala

Você pode automatizar a implantação da arquitetura de destino usando os módulos do Terraform que estão no GitHub repositório. Você deve modificar o `terraform.tfvars` arquivo para incluir valores de variáveis específicos do seu ambiente. O bucket, os AWS Managed Microsoft AD componentes, a chave de AWS KMS criptografia e alguns segredos do Amazon S3 são pré-requisitos para essa implantação e não estão incluídos no código do Terraform.

Ferramentas

Serviços da AWS

- AWS Directory Service for Microsoft Active Directorypermite que suas cargas de trabalho e AWS recursos com reconhecimento de diretório usem o Microsoft Active Directory no. Nuvem AWS Nesse padrão, AWS Managed Microsoft AD é usado para autenticação do Windows Server e SQL Server e para DNS.
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente. Nesse padrão, as instâncias do cluster de failover do SQL Server são instaladas nas EC2 instâncias da Amazon.
- EC2 O Image Builder ajuda você a automatizar a criação, o gerenciamento e a implantação de imagens personalizadas do servidor.
- O Amazon FSx para Windows File Server fornece armazenamento compartilhado totalmente gerenciado no Windows Server. Nesse padrão, FSx para Windows, o File Server fornece armazenamento compartilhado para dados e arquivos de log do SQL Server e para a testemunha do quórum.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados. Nesse padrão, ele é usado para criptografar segredos do Secrets Manager, o armazenamento do SQL Server nos volumes do Amazon Elastic Block Store (Amazon EBS) e o sistema de arquivos do FSx Windows File Server.

- O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação. Nesse padrão, as credenciais do Active Directory para instalar e executar o SQL Server, as credenciais do `sa` usuário e as informações de conexão do banco de dados são armazenadas no Secrets Manager.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados. Esse padrão usa um bucket do Amazon S3 para armazenar a imagem de instalação do SQL Server.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- O Microsoft SQL Server FCIs é instalado nos nós de cluster do Windows Server. Além disso, eles podem ser instalados em várias sub-redes. Nesse padrão, as instâncias FCI do SQL Server são instaladas nos nós do WSFC.
- O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem. Nesse padrão, o Terraform é usado para criar os recursos e configurar as instâncias FCI do SQL Server.
- O Clustering de Failover do Windows Server fornece recursos de infraestrutura que oferecem suporte à alta disponibilidade de aplicativos de servidor hospedados, como o SQL Server. Nesse padrão, os nós FCI usam a funcionalidade do WSFC para fornecer alta disponibilidade local por meio de redundância no nível da instância.

Repositório de código

O código desse padrão está disponível no repositório GitHub cluster-amazon-elastic-compute- cloud-amazon-fsx-microsoft -sql-server. Os seguintes recursos estão disponíveis no repositório:

- Um `README.md` arquivo que fornece uma visão geral da solução e informações adicionais de instalação e uso
- Um conjunto básico de arquivos de configuração do Terraform e um módulo FSx específico da Amazon para provisionar os componentes desse padrão
- Um script de configuração de instância que é executado como um script de dados EC2 do usuário da Amazon

- Um arquivo `component.yaml` que o Image Builder pode usar para criar uma AMI personalizada

Práticas recomendadas

Segurança e aplicação de patches

- As instalações e configurações pré-requisitos da AMI são os requisitos mínimos para implantar clusters FCI do SQL Server. Software e configurações adicionais podem ser necessários para cumprir os padrões e os requisitos de segurança da sua organização.
- Após a implantação, corrija o Windows continuamente. Corrija diretamente as instâncias em execução ou crie uma nova AMI com os patches mais recentes do Windows e substitua as instâncias (uma por vez) usando a nova AMI. AWS lança AMIs mensalmente o novo Windows que contém os patches, drivers e agentes de lançamento mais recentes do sistema operacional. Recomendamos que você verifique a AMI mais recente ao executar novas instâncias ou ao criar suas próprias imagens personalizadas.
- As EC2 instâncias da Amazon são configuradas para permitir todo o tráfego de saída. Quando implantado em um ambiente de produção, as regras de saída no grupo de segurança devem ser implementadas para restringir esse tráfego aos destinos necessários.
- O sistema FSx de arquivos do Windows File Server pode registrar automaticamente os registros de auditoria para compartilhamento de arquivos e acesso a arquivos e pastas e enviá-los para o destino desejado, se isso for um requisito em seu ambiente.
- Alterne os segredos do Secrets Manager automaticamente e regularmente. Para o par de chaves de EC2 instância da Amazon, considere uma solução de rotação automatizada, conforme descrito em Como usar o AWS Secrets Manager para armazenar e alternar pares de chaves SSH com segurança. Para as credenciais do Active Directory e os segredos das `sa` credenciais do SQL Server, configure a rotação automática de acordo com suas políticas de gerenciamento de senhas.

Gerenciamento do Active Directory

- Como parte do cluster FCI, o Windows gera um objeto de nome de computador (CNO) no Active Directory. O CNO responde às solicitações de DNS e encaminha o tráfego para o nó SQL ativo. Não recomendamos o uso desse DNS fornecido pelo Active Directory. O TTL é muito alto para fornecer um tempo razoável de failover e geralmente leva mais de 5 minutos para refletir o novo endereço IP primário. Por outro lado, para instalações de alta disponibilidade, o Network Load Balancer interno é configurado para failover em 30 segundos.

- É necessário um administrador de domínio do Active Directory para criar o cluster. Esse requisito se deve às permissões elevadas necessárias para criar os objetos de cluster e modificar as permissões no Active Directory. No entanto, os serviços do SQL Server não precisam ser executados como administrador de domínio. Portanto, recomendamos que você crie um segundo usuário do Active Directory para essa finalidade. No entanto, você pode eliminar esse usuário se os serviços forem executados como usuário administrador do domínio. Nesse caso, o usuário administrador do domínio deve ser adicionado ao grupo de administradores do Active Directory criado como parte desse padrão.

Épicos

Configurar credenciais do cluster

Tarefa	Descrição	Habilidades necessárias
Crie grupos do Active Directory.	Em AWS Managed Microsoft AD, crie os seguintes grupos: • Grupo de administradores de cluster — Esse grupo será adicionado ao grupo local de administradores em cada nó do cluster. • Grupo de área de trabalho remota em cluster — Esse grupo será adicionado ao grupo local de usuários de área de trabalho remota em cada nó do cluster. Para obter mais detalhes, consulte Criação de um AWS Managed Microsoft AD grupo na AWS documentação.	Administrador do AD
Crie usuários do Active Directory.	Em AWS Managed Microsoft AD, crie os seguintes usuários	Administrador do AD

Tarefa	Descrição	Habilidades necessárias
	• Usuário administrador do domínio — Use essa conta para criar o cluster. • Usuário do domínio — Os serviços do SQL Server usarão essa conta para execução. Adicione esse usuário ao grupo de administradores de cluster que você criou na tarefa anterior. Para obter mais detalhes, consulte Criação de um AWS Managed Microsoft AD usuário na AWS documentação.	

Tarefa	Descrição	Habilidades necessárias
Adicione credenciais do Active Directory aos segredos.	Use o Secrets Manager para criar quatro segredos para armazenar as seguintes informações: • Nome de usuário do usuário administrador do domínio • Senha do usuário administrador do domínio • Nome de usuário do usuário do domínio • Senha do usuário do domínio Para obter mais detalhes, consulte Criar um AWS Secrets Manager segredo na AWS documentação.	Administrador da AWS

Prepare o ambiente

Tarefa	Descrição	Habilidades necessárias
Crie a AMI do Windows.	Crie uma AMI personalizada do Windows que inclua o software e as configurações pré-requisitos. Para obter mais detalhes, consulte Informações adicionais.	Administrador da AWS, AWS DevOps
Instale o Terraform.	Para instalar o Terraform, siga as instruções no site do Terraform.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Clone o repositório desse padrão. Para obter mais detalhes, consulte Clonar um repositório no GitHub site.	AWS DevOps

Instale o cluster

Tarefa	Descrição	Habilidades necessárias
Modifique as variáveis do Terraform.	Atualize o `terraform.tfvars` arquivo fornecido para definir todas as variáveis com valores apropriados para seu ambiente. Por exemplo, `domain_group_administrators` atualize `domain_group_rdp_users` as variáveis e para usar seu nome de domínio do Active Directory e o nome dos grupos do Active Directory criados anteriormente.	AWS DevOps
Inicializar o Terraform.	Para ver a implantação proposta, navegue até a raiz do repositório. Use a interface de linha de comando (CLI) do Terraform para `terraform init` executar e depois executar. `terraform plan`	AWS DevOps
Implante recursos.	Para implantar o cluster SQL e os recursos associados,	AWS DevOps, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	use a CLI do Terraform para executar. `terraform apply`	

Tarefa	Descrição	Habilidades necessárias
Valide a implantação.	Para validar a implantação, use as seguintes etapas: 1. Conecte-se a uma das EC2 instâncias implantadas do Windows Amazon usando o Remote Desktop. 2. Para obter mais detalhes, consulte Conecte-se à sua instância do Windows usando RDP na AWS documentação. 3. Abra o Gerenciador de Cluster de Failover do Windows. Valide se o cluster foi criado e se a função do SQL Server foi criada e está em execução. 4. Para testar a conectividade e a autenticação com o SQL Server, use uma ferramenta de banco de dados, como o SQL Server Management Studio, para se conectar ao endpoint do SQL Server. (O valor do endpoint é armazenado no Secrets Manager.) Para obter mais detalhes, consulte Connect to Microsoft SQL Server EC2 na Amazon na AWS documentação.	DBA, administrador de sistemas da AWS

Solução de problemas

Problema	Solução
O provisionamento do Terraform foi concluído, mas o Gerenciador de Cluster de Failover do Windows não mostra que um cluster foi criado ou que o cluster está em um estado inoperável.	Toda a instalação dos recursos e a configuração dos clusters podem levar de 45 a 60 minutos. Após a conclusão do Terraform, o script de dados do usuário deve ser executado até a conclusão, o que requer várias reinicializações. Para monitorar o progresso, você pode usar o `Checkpoints` diretório na `C:\` unidade e os logins de instalação do SQL Server`C:\Program Data\Microsoft SQL Server\150\Log`. Ao terminar, a mensagem Instalação concluída estará disponível no `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log` arquivo.
Depois de provisionar um cluster em funcionamento, o uso do Terraform para excluir e recriar o cluster não é bem-sucedido. O Terraform é concluído, mas o cluster não está configurado corretamente.	Parte do processo de provisionamento envolve o registro de máquinas e objetos virtuais no Active Directory e no DNS do Active Directory. Quando existem nomes de computador para os nós do EC2 cluster da Amazon e para o nó do cluster, o FCI não pode inicializar corretamente e falhará no provisionamento. Para corrigir esse problema, execute as seguintes etapas: 1. Exclua os EC2 nós da Amazon, o computador virtual do cluster e o ID do cluster nos usuários e computadores do Active Directory. 2. Exclua a entrada DNS do computador virtual do cluster no DNS do Active Directory.

Problema	Solução
	3. Execute o comando a seguir para excluir o recurso `terragrunt destroy -target=random_string.cluster_id` Terraform, string aleatória, id do cluster. Essa ação excluirá as EC2 instâncias existentes da Amazon. 4. Execute `terraform apply` e espere os três novos recursos a seguir: duas EC2 instâncias FCI da Amazon e 1 ID de cluster de string aleatória.

Recursos relacionados

AWS documentação

- Crie imagens personalizadas com o Image Builder
- Criar uma chave KMS
- Criação de um balde de uso geral
- Criação de uma política chave
- Criando seu AWS Managed Microsoft AD

Mais informações

Informações do módulo Terraform

Este módulo usa uma combinação de configuração de AMI e configuração de dados do usuário para obter uma boa combinação de tempo de provisionamento e estabilidade. Durante o provisionamento, o Windows exige várias reinicializações e esperas. Um método de checkpoints foi implementado para proteger contra loops infinitos durante a reinicialização dos dados persistentes do usuário. Os dados do usuário estão configurados para serem persistentes. Portanto, os scripts de configuração de dados do usuário devem, e devem continuar, sendo desenvolvidos para serem idempotentes. A idempotência simplifica o processo de atualização, permitindo que as instâncias sejam trocadas durante um ciclo de atualização sem configuração manual para reingressar ou recriar clusters FCI.

Cadeias de conexão e cluster de failover do SQL Server

O módulo publicará um segredo contendo o endereço do endpoint que deve ser usado nas cadeias de conexão desse banco de dados. O nome secreto segue o formato`{environment_name}/sqlserver/{cluster_name}/endpoint`. Para instalações em que apenas um nó é usado, você pode esperar que esse seja o endereço IP da interface do SQL Server da EC2 instância Amazon. Para instalações de alta disponibilidade (duas instâncias), você pode esperar que esse seja o nome DNS do Network Load Balancer interno.

O agrupamento virtual de failover IPs não é suportado neste módulo. Um IP virtual deve permanecer na mesma sub-rede para funcionar. Em AWS, uma única sub-rede não pode abranger várias zonas de disponibilidade. Portanto, o uso do virtual IPs eliminaria a capacidade desse módulo ser considerado altamente disponível.

Cada EC2 instância da Amazon recebe três endereços IP privados. Seu uso é o seguinte:

- IP primário para tráfego de rede — O IP de origem para tráfego de saída.
- Comunicações FCI — usadas para manter o estado e a sincronização do cluster de failover.
- SQL Server (porta TCP 1433) — Ouve e também escuta o tráfego de pulsação para determinar qual instância é primária.

Configuração de VPC

Os pré-requisitos listam um conjunto de opções de DHCP configurado para usar o Active Directory para resolução de DNS. No entanto, esse pré-requisito não é um requisito difícil. O requisito básico é que as EC2 instâncias sejam capazes de resolver seu nome de domínio do Active Directory. Atender a esse requisito pode ser feito de outras formas, como usando Amazon Route 53 Resolver endpoints. Para obter mais informações, consulte Integrando a resolução de DNS do seu serviço de diretório com os resolvedores do Amazon Route 53 (AWS postagem no blog).

Configuração da AMI

A AMI usada nesse padrão deve conter os seguintes pré-requisitos de software e configurações:

1. Baixe e expanda os arquivos de instalação do SQL Server 2019 para `C:\SQL_Install_media` o.
2. Instale os seguintes recursos do Windows:
   - `Install-WindowsFeature Failover-Clustering`
   - `Install-WindowsFeature RSAT-AD-PowerShell`
   - `Install-WindowsFeature RSAT-AD-Tools`

- `Install-WindowsFeature RSAT-Clustering-Mgmt`
- `Install-WindowsFeature RSAT-Clustering-PowerShell`
- `Install-WindowsFeature RSAT-Clustering-CmdInterface`

3. Desative o firewall do Windows da seguinte forma:
   - `Get-NetFirewallProfile | Set-NetFirewallProfile -Enabled False`
4. Ative o método de autenticação CredSSP (<domain>substitua pelo nome de domínio Windows da sua organização) da seguinte forma:
   - `Enable-WSManCredSSP -Role "Server" -Force`
   - `Enable-WSManCredSSP -Role "Client" -DelegateComputer *.<domain>.com -Force`
5. Defina as seguintes chaves de registro:
   - Permitir credenciais de autenticação NTLM:
     - `HKLM:\Software\Policies\Microsoft\Windows\CredentialsDelegation`
       - Nome: `AllowFreshCredentialsWhenNTLMOnly`
       - Valor: 1
       - Tipo: `REG_DWORD`
   - Permita que computadores de domínio local usem o NTLM a partir de: PowerShell
     - Caminho: `HKLM:\Software\Policies\Microsoft\Windows\CredentialsDelegation\AllowFreshCredentialsWhenNTLMOnly`
       - Nome: 1
       - Valor: `wsman/*.<domain>.com`
       - Tipo: `REG_SZ`
6. Configure a PowerShell Galeria da seguinte forma:
   - `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`
   - `Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force`
   - `Set-PSRepository -Name PSGallery -InstallationPolicy Trusted`
7. Instale os seguintes PowerShell módulos do Windows*:
   - `Install-Module -Name ComputerManagementDsc`
   - `Install-Module -Name FailOverClusterDsc`
   - `Install-Module -Name PSDscResources`

- `Install-Module -Name xSmbShare`
- `Install-Module -Name xActiveDirectory`
- `Install-Module -Name SqlServer`

Para usar o Image Builder para criar a AMI, siga as instruções em Criar um pipeline de imagem usando o assistente de console do EC2 Image Builder na documentação do Image Builder. Para criar o componente da receita com os pré-requisitos anteriores, use as seguintes etapas:

1. Baixe o arquivo component.yaml da `ami` pasta do repositório. GitHub
2. Copie o conteúdo em um novo componente do Image Builder.
3. Atualize os seguintes espaços reservados com suas informações:
   - `<domain>`— Seu nome de domínio do Active Directory
   - `<bucket_name>`— Nome do bucket Amazon S3 que contém a imagem do SQL Server

Emule workloads do Oracle RAC usando endpoints personalizados no Aurora PostgreSQL

Criado por HariKrishna Boorgadda (AWS)

Resumo

Esse padrão descreve como emular serviços em um workload do Oracle Real Application Clusters (Oracle RAC) usando a edição compatível com o Amazon Aurora Edição Compatível com PostgreSQL com endpoints personalizados que distribuem cargas de trabalho entre instâncias em um único cluster. O padrão mostra como criar endpoints personalizados para bancos de dados Amazon Aurora. Os endpoints personalizados permitem que você distribua e balanceie cargas de trabalho em diferentes conjuntos de instâncias de banco de dados em seu cluster Aurora.

Em um ambiente Oracle RAC, os serviços podem abranger uma ou mais instâncias e facilitar o balanceamento do workload com base no desempenho da transação. Os recursos do serviço incluem recuperação end-to-end autônoma, mudanças contínuas por carga de trabalho e transparência total da localização. Você pode usar esse padrão para emular alguns desses recursos. Por exemplo, você pode emular a capacidade de rotear conexões para aplicativos de relatórios.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um driver JDBC PostgreSQL
- Um banco de dados compatível com o Aurora PostgreSQL
- Um banco de dados Oracle RAC migrado para um banco de dados compatível com o Aurora PostgreSQL

Limitações

- Para as limitações que se aplicam aos endpoints personalizados, consulte Especificação de propriedades para endpoints personalizados na documentação do Amazon RDS.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Oracle RAC de nó triplo

Pilha de tecnologias de destino

- Um banco de dados compatível com o Aurora PostgreSQL com duas réplicas de leitura

Arquitetura de origem

O diagrama seguinte mostra a arquitetura de um banco de dados do Oracle RAC de nó triplo.

Arquitetura de destino

O diagrama a seguir mostra a arquitetura de um banco de dados do Aurora PostgreSQL com duas réplicas de leitura. Três aplicativos/serviços diferentes estão usando endpoints personalizados, que atendem a diferentes usuários de aplicativos e redirecionam o tráfego e a carga entre as réplicas primárias e de leitura.

Ferramentas

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e compatível com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

Épicos

Criar o cluster do Aurora PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Crie um cluster.	Para criar o cluster, consulte Criar um cluster de banco de dados e conectar-se a um banco de dados em um cluster de banco de dados do Aurora PostgreSQL na documentação do Amazon RDS.	Administrador da AWS
Crie um grupo de parâmetros personalizados para o workload.	Para criar um grupo de parâmetros, consulte Criação de um grupo de parâmetros de cluster de banco de dados na documentação do Amazon RDS.	Administrador da AWS
Crie notificações e alarmes de eventos.	Você pode usar notificações de eventos e CloudWatch alarmes da Amazon para notificá-lo quando o cluster muda de estado e para capturar métricas quando um limite predefinido for atingido. Para criar um CloudWatch alarme, consulte Criar um CloudWatch alarme com base em um limite estático na CloudWatch documentação. Para criar uma notificação de evento, consulte Criação de uma regra de CloudWatch	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	eventos que é acionada em um evento na CloudWatch documentação.	

Adicione réplicas ao cluster de banco de dados do Aurora PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Adicione as réplicas de leitura ao cluster.	1. Crie uma réplica de leitura. 2. **Note** Adicione a réplica de leitura à mesma zona de disponibilidade em que seu cluster de banco de dados está. : você pode usar uma zona de disponibilidade diferente se tiver requisitos que precisem ser atendidos para seu nó de failover.	Administrador da AWS
Observe o endpoint de uma réplica de leitura.	Documente seu endpoint de réplica de leitura para uso posterior na criação de endpoints personalizados.	Administrador da AWS

Crie endpoints personalizados

Tarefa	Descrição	Habilidades necessárias
Insira um nome para o endpoint personalizado.	Para cada endpoint que você precisar, crie um nome de endpoint exclusivo relacionado ao seu workload ou aplicativo.	Administrador da AWS
Adicione os membros do endpoint.	Adicione seus endpoints de réplica de leitura a um grupo personalizado. Para obter mais informações, consulte Edição de um endpoint personalizado na documenta ção do Amazon RDS.	Administrador da AWS
(Opcional) Adicione futuras instâncias ao cluster.	Se você quiser adicionar mais réplicas ou endpoints ao grupo personalizado, consulte Adicionar réplicas do Aurora a um cluster de banco de dados na documentação do Amazon RDS.	Administrador da AWS
Crie o endpoint.	Para criar o endpoint, consulte Criação de um endpoint personalizado na documenta ção do Amazon RDS.	Administrador da AWS

Teste as conexões de aplicativos usando endpoints personalizados

Tarefa	Descrição	Habilidades necessárias
Compartilhe os detalhes personalizados do endpoint	Adicione os detalhes do endpoint personalizado aos detalhes da conexão do banco	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
com o aplicativo que aponta para seu workload.	de dados no aplicativo de relatórios que você planeja testar.	
Conecte o workload usando o endpoint personalizado.	Valide os detalhes personalizados do endpoint no aplicativo de relatórios.	Administrador da AWS
Verifique os detalhes da conexão no banco de dados.	1. Teste o nome de usuário e a contagem de conexões do seu aplicativo. 2. Verifique o balanceamento de carga em suas cargas de trabalho para garantir que as conexões sejam distribuídas em diferentes endpoints personalizados (réplicas primárias e de leitura).	Administrador da AWS

Recursos relacionados

- Tipos de endpoints do Aurora
- Regras de associação para endpoints personalizados
- End-to-end Exemplo de AWS CLI para endpoints personalizados
- Amazon Aurora como alternativa ao Oracle RAC
- Desafios ao migrar do Oracle para o PostgreSQL – e como superá-los

Habilite conexões criptografadas para instâncias de banco de dados PostgreSQL no Amazon RDS

Criado por Rohit Kapoor (AWS)

Resumo

O Amazon Relational Database Service (Amazon RDS) é compatível com a criptografia SSL para instâncias de banco de dados PostgreQL. Por meio do SSL, você pode criptografar uma conexão do PostgreSQL entre seus aplicativos e suas instâncias de banco de dados do Amazon RDS para PostgreSQL. Por padrão, o Amazon RDS for PostgreSQL usa criptografia. SSL/TLS and expects all clients to connect by using SSL/TLS O Amazon RDS para PostgreSQL oferece suporte às versões 1.1, e 1.2 do TLS.

Esse padrão descreve como você pode habilitar conexões criptografadas para uma instância de banco de dados do Amazon RDS para PostgreSQL. Você pode usar o mesmo processo para habilitar conexões criptografadas para o Amazon Aurora Edição Compatível com PostgreSQL.

Pré-requisitos e limitações

- Uma conta AWS ativa
- Uma instância de banco de dados Amazon RDS para PostgreSQL
- Um pacote SSL

Arquitetura

Ferramentas

- O pgAdmin é uma plataforma de administração e desenvolvimento de código aberto para o PostgreSQL. Você pode usar o pgAdmin no Linux, Unix, macOS e Windows para gerenciar seus objetos de banco de dados no PostgreSQL 10 e versões posteriores.
- Os editores do PostgreSQL fornecem uma interface mais fácil de usar para ajudá-lo a criar, desenvolver e executar consultas e a editar o código de acordo com seus requisitos.

Práticas recomendadas

- Monitore conexões de banco de dados não seguras.

- Audite direitos de acesso ao banco de dados.
- Garanta que os backups e os instantâneos sejam criptografados em repouso.
- Monitore o acesso ao banco de dados.
- Evite grupos de acesso irrestrito.
- Melhore suas notificações com a Amazon GuardDuty.
- Monitore a adesão à política regularmente.

Épicos

Baixe um certificado confiável e importe-o para sua loja confiável

Tarefa	Descrição	Habilidades necessárias
Carregue um certificado confiável no seu computador.	Para adicionar certificados ao armazenamento das Autoridades de Certificação Raiz Confiáveis do seu computador, siga estas etapas. (Essas instruções usam o Windows Server como exemplo.) 1. No Windows Server, escolha Iniciar, Executar e digite mmc. 2. No console, escolha Arquivo, Adicionar/remover snap-in. 3. Em Snap-ins disponíveis, escolha Certificados e, em seguida, escolha Adicionar. 4. Em Este snap-in sempre gerenciará certificados para, escolha Conta de computador, Avançar.	DevOps engenheiro, engenheiro de migração, DBA

Tarefa	Descrição	Habilidades necessárias
	5. Escolha Computador local, Concluir. 6. Se você não tiver mais snap-ins para adicionar ao console, escolha OK. 7. Na árvore do console, clique duas vezes em Certificados. 8. Clique com o botão direito do mouse em Autoridades de certificação raiz confiáveis. 9. Escolha Todas as tarefas, Importar para importar os certificados baixados. 10. Siga as etapas no Assistente de importação de certificados.	

Forçar conexões SSL

Tarefa	Descrição	Habilidades necessárias
Crie um grupo de parâmetros e defina o parâmetro rds.force_ssl.	Se a instância de banco de dados PostgreSQL tiver um grupo de parâmetros personalizado, edite o grupo de parâmetros e altere `rds.force_ssl` para 1. Se a instância de banco de dados usar o grupo de parâmetros padrão que não tem `rds.force_ssl`	DevOps engenheiro, engenheiro de migração, DBA

Tarefa	Descrição	Habilidades necessárias
	habilitado, crie um novo grupo de parâmetros. Você pode modificar o novo grupo de parâmetros usando a API do Amazon RDS ou manualmente, conforme as instruções a seguir. para criar um novo grupo de parâmetros: 1. Faça login no console de gerenciamento da AWS e abra o console do Amazon RDS para a região da AWS que hospeda a instância de banco de dados. 2. No painel de navegação, escolha Grupos de parâmetros. 3. Escolha Criar grupo de parâmetros e defina os seguintes valores: • Para Parameter group family (Família de grupos de parâmetros), escolha postgres14 ou superior. • Em Nome do grupo, digite pgsql-<database_instance>-ssl. • Em Descrição, insira uma descrição em formato livre para o grupo de	

Tarefa	Descrição	Habilidades necessárias
	parâmetros que você está adicionando. • Escolha Criar. 4. Escolha o grupo de parâmetros que criou anteriormente. 5. Em Parameter group actions (Ações do grupo de parâmetros), escolha Edit (Editar). 6. Encontre rds.force_ssl e altere sua configuração para 1. **Note** Realize testes do lado do cliente antes de alterar esse parâmetro. 7. Escolha Salvar alterações. Para associar o novo grupo de parâmetros de banco de dados à sua instância de banco de dados: 1. No console do Amazon RDS, no painel de navegação, selecione Bancos de dados e escolha a instância de banco de dados PostgreSQL.	

Tarefa	Descrição	Habilidades necessárias
	2. Escolha Modificar. 3. Em Configuração adicional, escolha o novo grupo de parâmetros e, em seguida, escolha Continuar. 4. Em Schedule modifications (Programar modificações), escolha Apply immediately (Aplicar imediatamente). 5. Selecione Modify DB instance (Modificar instância de banco de dados). Para obter mais informações, consulte a documentação do Amazon RDS.	
Força conexões SSL.	Conecte-se à sua instância de banco de dados do Amazon RDS para PostgreSQL de origem. As tentativas de conexão que não usam SSL são rejeitadas com uma mensagem de erro. Para obter mais informações, consulte a documentação do Amazon RDS.	DevOps engenheiro, engenheiro de migração, DBA

Instalar extensão SSL

Tarefa	Descrição	Habilidades necessárias

Instale a extensão SSL.	1. Inicie uma conexão psql ou pgAdmin como DBA.
	2. Chame a função ssl_is_used () para determinar se o SSL está sendo usado.
	`select ssl_is_used();`
	A função retornará `t` se a conexão estiver usando o SSL; caso contrário, retornará `f`.
	3. Instale a extensão SSL.
	`create extension sslinfo;`
	`show ssl;`
	`select ssl_cipher();`
	Para obter mais informações, consulte a documentação do Amazon RDS.
		DevOps engenheiro, engenheiro de migração, DBA

Configure seu cliente PostgreSQL para SSL

Tarefa	Descrição	Habilidades necessárias
Configure um cliente para SSL.	Usando SSL, você pode iniciar o servidor PostgreSQL com suporte para conexões criptografadas que usam protocolos TLS. O servidor	DevOps engenheiro, engenheiro de migração, DBA

Tarefa	Descrição	Habilidades necessárias

	recebe as conexões padrão e SSL na mesma porta TCP e negocia com qualquer cliente conectado se deve usar SSL ou não. Por padrão, essa é uma opção cliente.
	
	Se estiver usando o cliente psql:
	
	1. Garanta que o certifica do Amazon RDS tenha sido carregado em seu computador local.
	2. Inicie uma conexão de cliente SSL adicionando o seguinte:
	
	`psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser sslmode=verify-full sslrootcert=rds-ssl-ca-cert.pem`
	`select ssl_cipher();`
	
	Para outros clientes do PostgreSQL:
	
	• Modifique o respectivo parâmetro da chave pública do aplicativo. Isso pode estar disponível como uma opção ou como uma propriedade na página de	

Tarefa	Descrição	Habilidades necessárias
	conexão nas ferramentas de GUI. Examine as páginas a seguir para esses clientes: • Documentação do pgAdmin • Documentação do JDBC	

Solução de problemas

Problema	Solução
Não é possível baixar o certificado SSL.	Verifique sua conexão com o site e tente baixar novamente o certificado em seu computador local.

Recursos relacionados

- Documentação do Amazon RDS para PostgreSQL
- Usando SSL com uma instância de banco de dados PostgreSQL (documentação do Amazon RDS)
- Conexões TCP/IP seguras com SSL (documentação do PostgreSQL)
- Usando SSL (documentação do JDBC)

Criptografe uma instância de banco de dados Amazon RDS para PostgreSQL existente

Criado por Piyush Goyal (AWS), Shobana Raghu (AWS) e Yaser Raja (AWS)

Resumo

Esse padrão explica como criptografar uma instância de banco de dados existente do Amazon Relational Database Service (Amazon RDS) para PostgreSQL na nuvem da AWS com o mínimo de tempo de inatividade. Esse processo também funciona para instâncias de banco de dados do Amazon RDS para MySQL.

Você só pode habilitar a criptografia para uma instância de banco de dados do Amazon RDS ao criá-la, e não após a sua criação. No entanto, você pode adicionar criptografia a uma instância de banco de dados não criptografada criando um snapshot da instância de banco de dados e depois criando uma cópia criptografada desse snapshot. Em seguida, você pode restaurar uma instância de banco de dados a partir do snapshot criptografado, você terá uma cópia criptografada da sua instância de banco de dados original. Se seu projeto permitir tempo de inatividade (pelo menos para transações de gravação) durante essa atividade, isso é tudo o que você precisa fazer. Quando a nova cópia criptografada da instância de banco de dados estiver disponível, você poderá direcionar seus aplicativos para o novo banco de dados. No entanto, se seu projeto não permitir um tempo de inatividade significativo para essa atividade, você precisará de uma abordagem alternativa que ajude a minimizar o tempo de inatividade. Esse padrão usa o AWS Database Migration Service (AWS DMS) para migrar e replicar continuamente os dados para que a substituição para o novo banco de dados criptografado possa ser feita com o mínimo de tempo de inatividade.

As instâncias de banco de dados criptografadas do Amazon RDS usam o algoritmo de criptografia AES-256 padrão da indústria para criptografar os dados no servidor que hospeda as instâncias do Amazon RDS DB. Após a criptografia dos seus dados, o Amazon RDS lida com a autenticação do acesso e a decodificação dos seus dados de forma transparente com um mínimo impacto sobre o desempenho. Você não precisa modificar suas aplicações cliente de banco de dados para usar a criptografia.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância de banco de dados do Amazon RDS para PostgreSQL

- Experiência em trabalhar com (criar, modificar ou interromper) tarefas do AWS DMS (consulte Trabalho com tarefas do AWS DMS na documentação do AWS DMS)
- Familiaridade com o AWS Key Management Service (AWS KMS) para criptografar bancos de dados (consulte a documentação do AWS KMS)

Limitações

- Você só pode habilitar a criptografia para uma instância de banco de dados do Amazon RDS ao criá-la, e não após a sua criação.
- Os dados em tabelas não registradas não serão restaurados usando instantâneos. Para obter mais informações, consulte Melhores práticas para trabalhar com PostgreSQL.
- Não é possível ter uma réplica de leitura criptografada de uma instância de banco de dados não criptografada nem uma réplica de leitura não criptografada de uma instância de banco de dados criptografada.
- Não é possível restaurar um backup ou um snapshot não criptografado em uma instância de banco de dados criptografada.
- O AWS DMS não transfere automaticamente as sequências, portanto, etapas adicionais são necessárias para lidar com isso.

Para obter mais informações, consulte Limitações das instâncias de banco de dados criptografadas do Amazon RDS na documentação do Amazon RDS.

Arquitetura

Arquitetura de origem

- Instância de banco de dados do RDS não criptografada

Arquitetura de destino

- Instância de banco de dados do RDS criptografada
  - A instância de banco de dados RDS de destino é criada restaurando a cópia do DB snapshot da instância de banco de dados RDS de origem.
  - Uma chave do AWS KMS é usada para criptografia durante a restauração do snapshot.
  - Uma tarefa de replicação do AWS DMS é usada para migrar os dados.

Ferramentas

Ferramentas usadas para habilitar a criptografia:

- Chave do AWS KMS para criptografia: ao criar uma instância de banco de dados criptografada, você pode escolher uma chave gerenciada pelo cliente ou a chave gerenciada pela AWS para que o Amazon RDS criptografe a sua instância de banco de dados. Se você não especificar o identificador de chave para uma chave gerenciada pelo cliente, o Amazon RDS usará a chave gerenciada pela AWS para a sua nova instância de banco de dados. O Amazon RDS cria uma chave gerenciada pela AWS CMK gerenciada para o Amazon RDS para sua conta da . Sua conta da AWS tem uma chave gerenciada pela AWS diferente para Amazon RDS para cada região da AWS. Para obter mais informações sobre o uso de chaves KMS para criptografia do Amazon RDS, consulte Criptografando recursos do Amazon RDS.

Ferramentas usadas para replicação contínua:

- AWS DMS: você pode usar o AWS Database Migration Service (AWS DMS) para replicar as alterações do banco de dados de origem para o banco de dados de destino. É importante manter o banco de dados de origem e de destino sincronizados para reduzir ao mínimo o tempo de inatividade. Para obter informações sobre como configurar o AWS DMS e criar tarefas, consulte a documentação do AWS DMS.

Épicos

Crie um snapshot da instância de banco de dados de origem e criptografe-a

Tarefa	Descrição	Habilidades necessárias
Verificar os detalhes da instância de banco de dados PostgreSQL de origem.	No console do Amazon RDS, escolha a instância de banco de dados PostgreSQL de origem. Na guia Configuração, verifique se a criptografia não está habilitada para a instância. Para ver uma	DBA

Tarefa	Descrição	Habilidades necessárias
	ilustração de tela, consulte a seção Informações adicionais.	
Crie um snapshot de banco de dados.	Crie um snapshot do banco de dados da instância que deseja criptografar. O tempo necessário para criar um snapshot depende do tamanho do seu banco de dados. Para obter instruções, consulte Criação de um DB snapshot na documentação do Amazon RDS.	DBA

Tarefa	Descrição	Habilidades necessárias
Criptografe o instantâneo.	No painel de navegação do console Amazon RDS, escolha Snapshots e selecione o DB snapshot que você criou. Para Actions (Ações), escolha Copy Snapshot (Copiar snapshot). Forneça a região da AWS de destino e o nome da cópia do DB snapshot nos campos correspondentes. Marque a caixa de seleção Ativar criptografia. Em Master Key (Chave mestre), especifique o identificador de chave do KMS a ser usado para criptografar a cópia do snapshot de banco de dados. Escolha Copy Snapshot (Copiar snapshot). Para obter informações, consulte Cópia de um snapshot na documentação do Amazon RDS.	DBA

Prepare a instância de banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Restaure o snapshot de banco de dados.	No console do Amazon RDS, selecione a guia Snapshots. Escolha o instantâneo criptografado que você criou. Em Actions (Ações), escolha Restore Snapshot (Restaura	DBA

Tarefa	Descrição	Habilidades necessárias
	r snapshot). Em Identific ador da instância de banco de dados, insira um nome exclusivo de sua instância de banco de dados. Revise os detalhes da instância e escolha Restaurar instância de banco de dados. Uma nova instância de banco de dados criptografada será criada a partir do seu snapshot. Para obter mais informaçõ es, consulte Restaurar um snapshot de banco de dados na documentação do Amazon RDS.	
Migrar dados usando o AWS DMS	No console do AWS DMS, crie uma tarefa do AWS DMS. Para Migration type escolha Migrate existing data and replication ongoing changes (Migrar dados existentes e replicar alterações contínuas). Em Configurações da tarefa, no modo de preparação da tabela de destino, escolha Truncar. Para obter mais informações consulte Criação de uma tarefa, consulte a documentação do DMS.	DBA

Tarefa	Descrição	Habilidades necessárias
Ativar a validação de dados	Em Configurações da tarefa, escolha Habilitar validação . Isso permite comparar os dados de origem com os dados de destino para verificar se os dados foram migrados com precisão.	DBA
Desabilite as restrições na instância de banco de dados de destino.	Desative quaisquer gatilhos e restrições de chave estrangeira na instância de banco de dados de destino e, em seguida, inicie a tarefa do AWS DMS. Para obter mais informações sobre a desativação de acionadores e restrições de chave estrangeira, consulte a documentação do AWS DMS.	DBA
Verificar os dados.	Depois que o carregamento completo estiver concluído , verifique os dados na instância de banco de dados de destino para ver se eles correspondem aos dados de origem. Para obter mais informações, consulte Validação de dados na documentação do AWS DMS.	DBA

Vá para a instância de banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Interrompa as operações de gravação na instância de banco de dados de origem.	Pare as operações de gravação na instância de banco de dados de origem para que o tempo de inatividade do aplicativo possa começar. Verifique se o AWS DMS concluiu a replicação dos dados no pipeline. Habilite gatilhos e chaves estrangeiras na instância de banco de dados de destino.	DBA
Atualizar sequências do banco de dados	Se o banco de dados de origem contiver números de sequência, verifique e atualize as sequências no banco de dados de destino.	DBA
Configure o endpoint da aplicação.	Configure as conexões do aplicativo para usar os novos endpoints de instância de banco de dados do Amazon RDS. A instância de banco de dados já está criptografada.	DBA, proprietário do aplicativo

Recursos relacionados

- Criar uma tarefa do AWS DMS
- Monitoramento de tarefas de replicação usando a Amazon CloudWatch
- Monitoramento de tarefas do AWS DMS
- Atualização da chave de criptografia do Amazon RDS

Mais informações

Verificar a criptografia da instância de banco de dados PostgreSQL de origem:

Notas adicionais para esse padrão:

- Ative a replicação no PostgreSQL `rds.logical_replication` definindo o parâmetro como 1.

Observação importante: os slots de replicação retêm os arquivos de registro antecipado de gravação (WAL) até que os arquivos sejam consumidos externamente — por exemplo, por`pg_recvlogical`; por trabalhos de extração, transformação e carregamento (ETL); ou pelo AWS DMS. Quando você define o valor do `rds.logical_replication` parâmetro como 1, o AWS DMS define os parâmetros `wal_level`, `max_wal_senders`, `max_replication_slots`, e `max_connections`. Se houver slots de replicação lógica, mas não houver consumidor para os arquivos WAL retidos pelo slot de replicação, você poderá observar um aumento no uso do disco do log de transações e uma diminuição constante no espaço livre de armazenamento. Para obter mais informações e etapas para resolver esse problema, consulte o artigo Como posso identificar o que está causando o erro “Não há espaço restante no dispositivo” ou "DiskFull" no Amazon RDS for PostgreSQL? no Centro de conhecimento do AWS Support.

- Qualquer alteração de esquema que você fizer na instância de banco de dados de origem depois de criar o DB snapshot não estará presente na instância de banco de dados de destino.
- Após criar uma instância de banco de dados criptografada, não será possível alterar a chave do KMS usada por essa instância de banco de dados. Certifique-se de determinar os requisitos da chave do KMS antes de criar a instância de banco de dados criptografada.
- Você deve desativar os gatilhos e as chaves estrangeiras na instância de banco de dados de destino antes de executar a tarefa do AWS DMS. É possível reabilitá-los quando a tarefa for concluída.

Aplique a marcação automática dos bancos de dados do Amazon RDS no lançamento

Criado por Susanne Kangnoh (AWS) e Archit Mathur (AWS)

Resumo

O Amazon Relational Database Service (Amazon RDS) é um serviço Web que facilita a configuração, operação e dimensionamento de um banco de dados relacional na Nuvem do Amazon Web Services (AWS). Ele fornece capacidade econômica e redimensionável para um banco de dados relacional padrão do setor e gerencia tarefas comuns de administração de banco de dados.

As tags permitem categorizar seus recursos da AWS de maneiras diferentes. A marcação de banco de dados relacional é útil quando você tem muitos recursos em sua conta e deseja identificar rapidamente um recurso específico baseado nas tags. Você pode usar tags do Amazon RDS para adicionar metadados personalizados às instâncias de banco de dados do RDS. Cada tag consiste em um valor e em uma chave definida pelo usuário. Recomendamos criar um conjunto consistente de tags para atender às necessidades da sua organização.

Esse padrão fornece um CloudFormation modelo da AWS para ajudá-lo a monitorar e marcar instâncias de banco de dados do RDS. O modelo cria um evento da Amazon CloudWatch Events que acompanha o DBInstance evento AWS CloudTrail Create. (CloudTrail captura chamadas de API para o Amazon RDS como eventos.) Quando detecta esse evento, ela chama uma função do Lambda da AWS que aplica automaticamente as chaves e os valores de tag definidos por você. O modelo também envia uma notificação de que a instância foi marcada, usando o Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do Amazon Simple Storage Service (Amazon S3) para carregar o código Lambda.
- Um endereço de e-mail no qual você deseja receber notificações de marcação.

Limitações

- A solução oferece suporte à CloudTrail criação de DBInstance eventos. Ela não cria notificações para nenhum outro evento.

Arquitetura

Arquitetura de fluxo de trabalho

Automação e escala

- Você pode usar o CloudFormation modelo da AWS várias vezes para diferentes regiões e contas da AWS. Você precisa executar o modelo somente uma vez em cada região ou conta.

Ferramentas

Serviços da AWS

- AWS CloudTrail — CloudTrail A AWS é um serviço da AWS que ajuda você com a governança, a conformidade e a auditoria operacional e de risco da sua conta da AWS. As ações realizadas por um usuário, função ou serviço da AWS são registradas como eventos em CloudTrail.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS. CloudWatch Os eventos ficam cientes das mudanças operacionais à medida que elas ocorrem e tomam medidas corretivas conforme necessário, enviando mensagens para responder ao ambiente, ativando funções, fazendo alterações e capturando informações de estado.
- AWS Lambda: o AWS Lambda é um serviço de computação que oferece suporte à execução de código sem a necessidade de provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço web que permite que aplicativos, usuários finais e dispositivos enviem e recebam notificações da nuvem instantaneamente.

Código

Esse padrão inclui um anexo com dois arquivos:

- `index.zip` é um arquivo compactado que inclui o código do Lambda para esse padrão.
- `rds.yaml`é um CloudFormation modelo que implanta o código Lambda.

Consulte a seção Tópicos para obter informações sobre como usar esses arquivos.

Épicos

Implantar o código do Lambda

Tarefa	Descrição	Habilidades necessárias
Faça upload do código para um bucket do S3.	Crie um novo bucket do S3 ou use um bucket do S3 existente para carregar o arquivo `index.zip` anexado (código do Lambda). Esse bucket deve estar na mesma região da AWS que os recursos (instâncias de banco de dados do RDS) que você deseja monitorar.	Arquiteto de nuvem
Implante o CloudFormation modelo.	Abra o console do Cloudform ation na mesma região da AWS do bucket S3 e implante o arquivo `rds.yaml` fornecido no anexo. No próximo épico, forneça valores para os parâmetros do modelo.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Dar o nome do bucket do S3.	Insira o nome do bucket do S3 que você criou ou selecionou	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	no primeiro épico. Esse bucket do S3 contém o arquivo.zip do código Lambda e deve estar na mesma região da AWS que o CloudFormation modelo e as instâncias de banco de dados do RDS que você deseja monitorar.	
Fornecer a chave do S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `index.zip` ou `controls/index.zip`).	Arquiteto de nuvem
Fornecer um endereço de e-mail.	Forneça um endereço de e-mail ativo no qual você deseja receber notificações de violação.	Arquiteto de nuvem
Especifique um nível de log.	Especifique o nível de registro em log e a verbosidade. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo e deve ser usado somente para depuração. `Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Insira as chaves e os valores das tags para suas instâncias de banco de dados do RDS.	Insira as chaves de tag e os valores necessários que você deseja aplicar automatic amente à instância do RDS. Para obter mais informações, consulte Marcar recursos do Amazon RDS na documenta ção da AWS.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirme a assinatura por e-mail.	Quando o CloudFormation modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail que você forneceu. Para receber notificações quando suas instâncias forem marcadas, você deve confirmar essa assinatura de e-mail.	Arquiteto de nuvem

Recursos relacionados

- Criar um bucket (documentação do Amazon S3)
- Marcação de recursos do Amazon RDS (documentação do Amazon Aurora)
- Carregando objetos (documentação do Amazon S3)
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS (documentação da CloudTrail Amazon CloudWatch)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Expressa o custo de uma tabela do DynamoDB para capacidade sob demanda

Criado por Moinul Al-Mamun (AWS)

Resumo

O Amazon DynamoDB é um banco de dados transacional NoSQL que fornece latência de milissegundos de um dígito, mesmo em escala de petabytes. Essa oferta de tecnologia sem servidor da Amazon Web Services (AWS) está se tornando popular por causa do seu desempenho e escalabilidade consistentes. Não é necessário provisionar a infraestrutura subjacente. Sua única tabela pode crescer para até petabytes.

Com o modo de capacidade sob demanda, você paga por solicitação pelas leituras e gravações de dados que seu aplicativo executa nas tabelas. As cobranças da AWS são baseadas nas unidades de solicitação de leitura (RRUs) e unidades de solicitação de gravação (WRUs) acumuladas em um mês. O DynamoDB monitora continuamente o tamanho da sua tabela durante todo o mês para determinar suas cobranças de armazenamento. Ele suporta backup contínuo com point-in-time-recovery (PITR). O DynamoDB monitora continuamente o tamanho de suas tabelas habilitadas para PITR durante todo o mês para determinar suas cobranças de backup.

Para estimar o custo do DynamoDB para um projeto, é importante calcular quanto RRU, WRU e armazenamento serão consumidos em diferentes estágios do ciclo de vida do produto. Para uma estimativa aproximada de custos, você pode usar a Calculadora de Preços da AWS, mas deve fornecer um número aproximado de RRUs, WRUs, e requisitos de armazenamento para sua tabela. Isso pode ser difícil de estimar no início do projeto. A calculadora de preços da AWS não considera a taxa de crescimento de dados nem o tamanho do item, nem considera o número de leituras e gravações da tabela base e dos índices secundários globais (GSIs) separadamente. Para usar a calculadora de preços da AWS, você deve estimar todos esses aspectos para presumir valores aproximados de WRU, RRU e tamanho de armazenamento para obter sua estimativa de custo.

Esse padrão fornece um mecanismo e um modelo reutilizável do Microsoft Excel para estimar os fatores de custo básicos do DynamoDB, como gravação, leitura, armazenamento, backup e custo de recuperação, para o modo de capacidade sob demanda. Ela é mais granular do que a Calculadora de Preços da AWS e considera a tabela base e GSIs os requisitos de forma independente. Ele também considera a taxa mensal de crescimento dos dados do item e prevê custos por três anos.

Pré-requisitos e limitações

Pré-requisitos

- Conhecimento básico do DynamoDB e do design do modelo de dados do DynamoDB
- Conhecimento básico sobre preços, WRU, RRU, armazenamento, backup e recuperação do DynamoDB (para obter mais informações, consulte Preços da capacidade sob demanda)
- Conhecimento de seus dados, modelo de dados e tamanho do item no DynamoDB
- Conhecimento do DynamoDB GSIs

Limitações

- O modelo fornece um cálculo aproximado, mas não é apropriado para todas as configurações. Para obter uma estimativa mais precisa, você deve medir o tamanho individual do item para cada item na tabela base GSIs e.
- Para uma estimativa mais precisa, você deve considerar o número esperado de gravações (inserir, atualizar e excluir) e leituras para cada item em um mês médio.
- Esse padrão permite estimar somente os custos de gravação, leitura, armazenamento, backup e recuperação para os próximos anos, com base em suposições fixas de crescimento de dados.

Ferramentas

Serviços da AWS

- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.

Outras ferramentas

- A Calculadora de preços da AWS é uma ferramenta de planejamento baseada na web que você pode usar para criar estimativas para seus casos de uso da AWS.

Práticas recomendadas

Para ajudar a manter os custos baixos, considere as seguintes práticas recomendadas de design do DynamoDB.

- Design de chave de partição: use uma chave de partição de alta cardinalidade para distribuir a carga uniformemente.
- Padrão de design da lista de adjacências — Use esse padrão de design para gerenciamento one-to-many e many-to-many relacionamentos.
- Índice esparso — Use um índice esparso para o seu. GSIs Ao criar um GSI, você especifica uma chave de partição e, opcionalmente, uma chave de classificação. Somente itens na tabela base que contêm uma chave de partição GSI correspondente aparecem no índice esparso. Isso ajuda a manter o GSIs tamanho menor.
- Sobrecarga de índice: use o mesmo GSI para indexar vários tipos de itens.
- Fragmentação de gravação de GSI: fragmente de forma inteligente para distribuir dados entre as partições para permitir consultas mais rápidas e eficientes.
- Itens grandes: armazene somente metadados dentro da tabela, salve o blob no Amazon S3 e mantenha a referência no DynamoDB. Divida itens grandes em vários itens e indexe com eficiência usando chaves de classificação.

Para obter mais conhecer mais práticas recomendadas consulte o Guia do desenvolvedor do Amazon DynamoDB.

Épicos

Extraia as informações do item do seu modelo de dados do DynamoDB

Tarefa	Descrição	Habilidades necessárias
Obtenha o tamanho do item.	1. Verifique quantos tipos diferentes de itens você vai armazenar na sua mesa. 2. Para calcular o tamanho de cada item em kilobytes , adicione o tamanho da chave e do valor de cada atributo. 3. Calcule o tamanho do item para uma tabela base e para cada GSI.	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias

Faça uma estimativa do custo de gravação.	Para estimar o custo de gravação no modo de capacidade sob demanda, primeiro você precisa medir quantos WRUs serão consumidos em um mês. Para isso, você precisa considerar os seguintes fatores:
	• Número de operações de criação, atualização e exclusão para cada item em um mês.
	• Número de disponíveis GSIs. Considere cada índice de forma independe nte.
	  • Tamanho médio de um item de índice
	  • Número de tempos de sincronização em um índice
	• Quantas coisas novas (por exemplo, componentes ou produtos) serão adicionad as à tabela a cada mês? O número de itens adicionad os pode ser diferente a cada mês, mas você pode presumir uma taxa média de crescimento com base em seus casos de negócios.
		Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte a seção Informações adicionais.	
Estime o custo de leitura.	Para estimar o custo de leitura no modo sob demanda, primeiro você precisa medir quantos RRUs serão consumidos em um mês. Para isso, você precisa considerar os seguintes fatores: • Número de disponíveis GSIs. Considere cada índice de forma independe nte. • Tamanho médio de um item de índice • Número médio de leituras por produto por mês. • Número total de itens disponíveis (componentes ou produtos) na tabela do DynamoDB.	Engenheiro de dados, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Estime o tamanho e o custo do armazenamento.	Primeiro, estime a necessida de média mensal de armazenamento com base no tamanho do item na tabela. Em seguida, calcule o custo de armazenamento multiplicando o tamanho do armazenamento pelo preço de armazenamento por GB para sua região da AWS. Se você já inseriu dados para estimar o custo de gravação, não precisará inseri-los novamente para calcular o tamanho do armazenamento. Caso contrário, para estimar o tamanho do armazenamento, você precisa considerar os seguintes fatores: • Número de itens de dados em um módulo (produto) com base no design da tabela. • Tamanho médio do item em kilobytes. • Número de disponíveis GSIs. Considere cada índice de forma independe nte. • Tamanho médio de um item de índice	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	• Quantos novos produtos serão adicionados à tabela a cada mês? O número de novos produtos pode ser diferente a cada mês, mas você pode presumir uma taxa média de crescimento com base em seus casos de negócios. Este exemplo usa uma média de 10 milhões de novos produtos por mês.	

Insira as informações do item e do objeto no modelo do Excel

Tarefa	Descrição	Habilidades necessárias
Baixe o modelo do Excel na seção Anexos e ajuste-o para sua tabela de casos de uso.	1. Faça download do modelo do Excel. 2. Ajuste o módulo de negócios e GSIs, com base no design da sua mesa.	Engenheiro de dados
Insira as informações no modelo do Excel.	1. Atualize as informações do item na planilha. Atualize os dados somente nas células laranja. 2. Ajuste os números dos objetos: quanto poderia ser adicionado à tabela a cada mês? 3. Atualize os preços de WRU e RRU por milhão para sua região da AWS.	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	4. Atualize os preços de armazenamento e backup por GB por mês para sua região da AWS. 5. Atualize o preço de recuperação por GB para sua região da AWS. No modelo, há três itens ou entidades: informações, metadados e relacionamento. Há dois GSIs. Para seu caso de uso, se precisar de mais itens, crie novas linhas. Se precisar de mais GSIs, copie um bloco GSI existente e cole para criar quantos blocos GSI você precisar. Em seguida, ajuste os cálculos das colunas SOMA e TOTAL.	

Recursos relacionados

Referências

- Preços do Amazon DynamoDB para capacidade sob demanda
- Calculadora de preços da AWS para DynamoDB
- Práticas recomendadas de design e arquitetura com o DynamoDB
- Conceitos básicos do DynamoDB

Guias e padrões

- Modelagem de dados com Amazon DynamoDB

- Estime os custos de armazenamento de uma tabela do Amazon DynamoDB

Mais informações

Escreva um exemplo de cálculo de custos

O design do modelo de dados do DynamoDB mostra três itens para um produto e um tamanho médio de item de 4 KB. Quando você adiciona um novo produto à tabela base do DynamoDB, ele consome o número de itens * (tamanho do item/unidade de gravação de 1 KB) = 3 * (4/1) = 12 WRU. Neste exemplo, para gravar 1 KB, o produto consome 1 WRU.

Leia o exemplo de cálculo de custos

Para obter a estimativa de RRU, considere a média de quantas vezes cada item será lido em um mês. Por exemplo, o item de informação será lido, em média, 10 vezes em um mês, e o item de metadados será lido duas vezes, e o item de relacionamento será lido cinco vezes. No modelo de exemplo, RRU total para todos os componentes = número de novos componentes criados a cada mês * RRU por componente por mês = 10 milhões * 17 RRU = 170 milhões de RRU por mês.

Todos os meses, novidades (componentes ou produtos serão adicionados, e o número total de produtos aumentará com o tempo. Portanto, os requisitos de RRU também crescerão com o tempo.

- Para o primeiro mês de RRU, o consumo será de 170 milhões.
- No segundo mês, o consumo de RRU será de 2 x 170 milhões = 340 milhões.
- No terceiro mês, o consumo de RRU será de 3 x 170 milhões = 510 milhões.

O gráfico a seguir mostra o consumo mensal de RRU e a previsão de custos.

Observe que os preços no gráfico são apenas para fins ilustrativos. Para criar previsões precisas para seu caso de uso, verifique a página de preços da AWS e use esses preços na planilha do Excel.

Exemplos de cálculo de custos de armazenamento, backup e recuperação

O armazenamento, o backup e a restauração do DynamoDB estão todos conectados entre si. O backup está diretamente conectado ao armazenamento e a recuperação está diretamente conectada ao tamanho do backup. À medida que o tamanho da tabela aumenta, os custos correspondentes de armazenamento, backup e restauração aumentarão proporcionalmente.

Tamanho e custo do armazenamento

O custo de armazenamento aumentará com o tempo com base na sua taxa de crescimento de dados. Por exemplo, suponha que o tamanho médio de um componente ou produto na tabela base GSIs seja de 11 KB e que 10 milhões de novos produtos sejam adicionados todos os meses à tabela do banco de dados. Nesse caso, o tamanho da tabela do DynamoDB aumentou (11 KB * 10 milhões) /1024/1024 = 105 GB por mês. No primeiro mês, o tamanho do armazenamento da tabela será de 105 GB, no segundo mês será de 105 + 105 = 210 GBs e assim por diante.

- No primeiro mês, o custo de armazenamento será de 105 GB* por GB para sua região da AWS.
- No segundo mês, o custo de armazenamento será de 210 GB* por GB para sua região.
- No terceiro mês, o custo de armazenamento será de 315 GB* por GB para sua região.

Para saber o tamanho e o custo do armazenamento para os próximos três anos, consulte a seção Tamanho e previsão do armazenamento.

Custo do backup

O custo do backup aumentará com o tempo, com base na sua taxa de crescimento de dados. Quando você ativa o backup contínuo com point-in-time-recovery (PITR), as cobranças de backup contínuo são baseadas na média de GB de armazenamento por mês. Em um mês civil, o tamanho médio do backup seria igual ao tamanho do armazenamento da tabela, embora o tamanho real pudesse ser um pouco diferente. À medida que novos produtos forem adicionados a cada mês, o tamanho total do armazenamento e o tamanho do backup aumentarão com o tempo. Por exemplo, no primeiro mês, o tamanho médio do backup de 105 GB pode aumentar para 210 GB no segundo mês.

- No primeiro mês, o custo do backup será de 105 GB/mês* preço de backup contínuo por GB para sua região da AWS.
- No segundo mês, o custo do backup será de 210 GB/mês* preço de backup contínuo por GB para sua região.
- No terceiro mês, o custo do backup será de 315 GB/mês* preço de backup contínuo por GB para sua região.
- e assim por diante

O custo do backup está incluído no gráfico na seção Tamanho do armazenamento e previsão de custos.

Custo de recuperação

Quando você está fazendo backup contínuo com a PITR ativada, as cobranças da operação de recuperação são baseadas no tamanho da restauração. Cada vez que você restaura, você paga com base em gigabytes de dados restaurados. Se o tamanho da sua tabela for grande e você realizar a restauração várias vezes em um mês, será caro.

Para estimar o custo da restauração, este exemplo pressupõe que você realize uma recuperação de PITR uma vez por mês no final do mês. O exemplo usa o tamanho médio mensal do backup como o tamanho dos dados de restauração desse mês. No primeiro mês, o tamanho médio do backup é 105 GB e, para a recuperação no final do mês, o tamanho dos dados de restauração seria 105 GB. No segundo mês, seria 210 e GBs assim por diante.

O custo de recuperação aumentará com o tempo com base na taxa de crescimento de seus dados.

- No primeiro mês, o custo de recuperação será de 105 GB* de preço de restauração por GB para sua região da AWS.
- No segundo mês, o custo de recuperação será de 210 GB* de preço de restauração por GB para sua região.
- No terceiro mês, o custo de recuperação será de 315 GB* preço de restauração por GB para sua região.

Para obter mais informações, consulte a guia Armazenamento, backup e recuperação no modelo do Excel e o gráfico na seção a seguir.

Previsão de tamanho e custo de armazenamento

No modelo, o tamanho real do armazenamento faturável é calculado subtraindo o nível gratuito de 25 GB por mês para a classe de tabela Standard. Na planilha, você obterá um gráfico de previsão dividido em valores mensais.

O gráfico de exemplo a seguir prevê o tamanho do armazenamento mensal em GB, o custo de armazenamento faturável, o custo de backup sob demanda e o custo de recuperação para os próximos 36 meses corridos. Todos os custos estão em USD. No gráfico, fica claro que os custos de armazenamento, backup e recuperação aumentam proporcionalmente aos aumentos no tamanho do armazenamento.

Observe que os preços usados no gráfico são apenas para fins ilustrativos. Para criar preços precisos para seu caso de uso, consulte a página de preços da AWS e use esses preços no modelo do Excel.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Estime os custos de armazenamento de uma tabela do Amazon DynamoDB

Criado por Moinul Al-Mamun (AWS)

Resumo

O Amazon DynamoDB é um banco de dados transacional NoSQL que fornece latência de milissegundos de um dígito, mesmo em escala de petabytes. Essa popular oferta sem servidor da AWS fornece desempenho e escalabilidade consistentes. Você não precisa provisionar armazenamento, e sua tabela única pode crescer até petabytes.

O DynamoDB monitora o tamanho da sua tabela continuamente durante todo o mês para determinar suas cobranças de armazenamento. AWS em seguida, cobra pelo tamanho médio do armazenamento em gigabytes. Quanto mais sua mesa crescer com o tempo, mais seu custo de armazenamento aumentará. Para calcular o custo de armazenamento, você pode usar a Calculadora de AWS Preços, mas precisa fornecer o tamanho aproximado da tabela, incluindo índices secundários globais (GSIs), que são muito difíceis de estimar no início do projeto. Além disso, a Calculadora de AWS Preços não considera a taxa de crescimento dos dados.

Esse padrão fornece um mecanismo e um modelo reutilizável do Microsoft Excel para calcular o tamanho e o custo do armazenamento do DynamoDB. Ele considera os requisitos de armazenamento para a tabela base e a GSIs independente. Calcula o tamanho do armazenamento considerando o tamanho de seus itens individuais e a taxa de crescimento de dados ao longo do tempo.

Para obter uma estimativa, insira duas informações no modelo:

- O tamanho do item individual em kilobytes para a tabela base e GSIs
- Quantos novos objetos ou produtos poderiam ser adicionados à tabela, em média, em um mês (por exemplo, 10 milhões)

O modelo gera um gráfico de previsão de armazenamento e custos para os próximos três anos, que é mostrado no exemplo a seguir.

Pré-requisitos e limitações

Pré-requisitos

- Conhecimento básico do DynamoDB, incluindo armazenamento e preços do DynamoDB
- Conhecimento de seus dados, modelo de dados e tamanho do item no DynamoDB
- Conhecimento dos índices secundários globais do DynamoDB () GSIs

Limitações

- O modelo fornece um cálculo aproximado, mas não é apropriado para todas as configurações. Para obter uma estimativa mais precisa, você deve medir o tamanho individual do item para cada item na tabela base GSIs e.
- Esse padrão permite estimar somente o tamanho e o custo do armazenamento para os próximos anos, com base em suposições fixas de crescimento de dados.

Ferramentas

Serviços da AWS

- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.

Outras ferramentas

- AWS A Calculadora de Preços é uma ferramenta de planejamento baseada na web que você pode usar para criar estimativas para seus casos de AWS uso.

Épicos

Extraia as informações do item do seu modelo de dados do DynamoDB

Tarefa	Descrição	Habilidades necessárias
Obtenha o tamanho do item.	1. Determine quantos tipos diferentes de itens você armazenará na sua mesa.	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	2. Para calcular o tamanho de cada item em kilobytes, adicione o `Key` e o `Value` tamanho de cada atributo. 3. Calcule o tamanho do item para uma tabela base e para cada GSI.	
Veja o número de objetos adicionados em um mês.	Estime quantos componentes ou objetos serão adicionados à tabela do DynamoDB, em média, em um mês.	Engenheiro de dados

Insira as informações do item e do objeto no modelo do Excel

Tarefa	Descrição	Habilidades necessárias
Baixe e ajuste a planilha do Excel.	1. Baixe o modelo do Excel do documento anexo. 2. Ajuste o módulo de negócios e GSIs, com base no design da sua mesa.	Engenheiro de dados
Insira as informações no modelo do Excel.	1. Atualize as informações do item na planilha. 2. Ajuste os números dos objetos: quanto poderia ser adicionado à tabela a cada mês? 3. Atualize o preço de armazenamento por GB por mês para seu. Região da AWS	Engenheiro de dados

Recursos relacionados

- Preços da capacidade sob demanda para o Amazon DynamoDB
- AWS Calculadora de preços para DynamoDB

Mais informações

Observe que o modelo em anexo prevê somente o tamanho e o custo do armazenamento para a classe de tabela de armazenamento padrão. Com base na previsão dos custos de armazenamento e considerando o tamanho do item individual e a taxa de crescimento do produto ou do objeto, você pode estimar o seguinte:

- Custo de exportação de dados
- Custo de backup e recuperação
- Requisitos de armazenamento de dados

Custo de armazenamento de dados do Amazon DynamoDB

O DynamoDB monitora continuamente o tamanho de suas tabelas para determinar suas cobranças de armazenamento. O DynamoDB mede o tamanho dos dados faturáveis adicionando o tamanho do byte bruto dos dados mais uma sobrecarga de armazenamento por item que depende dos atributos ativados. Para obter mais informações, consulte o Guia do desenvolvedor do DynamoDB.

O preço do armazenamento de dados depende da classe da sua tabela. Os primeiros 25 GB armazenados por mês são gratuitos se você estiver usando a classe de tabela padrão do DynamoDB. Para obter mais informações sobre os custos de armazenamento das classes de tabela de acesso padrão e padrão de acesso infrequente em diferentes classes Regiões da AWS, consulte Preços da capacidade sob demanda.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Estime o tamanho do mecanismo Amazon RDS para um banco de dados Oracle usando relatórios AWR

Criado por Abhishek Verma (AWS) e Eduardo Valentim (AWS)

Resumo

Quando você migra um banco de dados Oracle para o Amazon Relational Database Service (Amazon RDS) ou Amazon Aurora, computar a CPU, a memória e a E/S de disco para o banco de dados de destino é um requisito fundamental. Você pode estimar a capacidade necessária do banco de dados de destino analisando os relatórios do Oracle Automatic Workload Repository (AWR). Esse padrão explica como usar relatórios AWR para estimar esses valores.

O banco de dados Oracle de origem pode estar no local ou hospedado em uma instância do Amazon Elastic Compute Cloud (Amazon EC2), ou pode ser uma instância de banco de dados Amazon RDS for Oracle. O banco de dados de destino pode ser qualquer banco de dados Amazon RDS ou Aurora.

> **Note**
>
> As estimativas de capacidade serão mais precisas se o mecanismo de banco de dados de destino for o Oracle. Para outros bancos de dados do Amazon RDS, o tamanho do mecanismo pode variar devido às diferenças na arquitetura do banco de dados.

Recomendamos que você execute o teste de desempenho antes de migrar seu banco de dados Oracle.

Pré-requisitos e limitações

Pré-requisitos

- Uma licença do Oracle Database Enterprise Edition e uma licença do Oracle Diagnostics Pack para baixar relatórios AWR.

Versões do produto

- Todas as edições do banco de dados do Oracle para versões 11g (versões 11.2.0.3.v1 e posteriores) e até 12.2 e 18c, 19c
- Esse padrão não abrange o Oracle Engineered Systems ou o Oracle Cloud Infrastructure (OCI).

Arquitetura

Pilha de tecnologia de origem

Um dos seguintes:

- Um banco de dados Oracle on-premises
- Um banco de dados Oracle em uma EC2 instância
- Instância de banco de dados do Amazon RDS para Oracle

Pilha de tecnologias de destino

- Qualquer banco de dados Amazon RDS ou Amazon Aurora

Arquitetura de destino

Para obter informações sobre o processo completo de migração, consulte o padrão Migrar um banco de dados Oracle para o Aurora PostgreSQL usando o AWS DMS e o AWS SCT.

Automação e escala

Se você tiver vários bancos de dados Oracle para migrar e quiser usar métricas de desempenho adicionais, poderá automatizar o processo seguindo as etapas descritas na postagem do blog Instâncias do Amazon RDS do tamanho certo em escala com base nas métricas de desempenho da Oracle.

Ferramentas

- O Oracle Automatic Workload Repository (AWR) é um repositório incorporado aos bancos de dados Oracle. Ele coleta e armazena periodicamente a atividade do sistema e os dados da workload, que são então analisados pelo Automatic Database Diagnostic Monitor (ADDM). O AWR tira snapshots dos dados de desempenho do sistema periodicamente (por padrão, a cada 60 minutos) e armazena as informações (por padrão, até 8 dias). Você pode usar visualizações e relatórios do AWR para analisar esses dados.

Práticas recomendadas

- Para calcular os requisitos de recursos para seu banco de dados de destino, você pode usar um único relatório AWR, vários relatórios AWR ou visualizações dinâmicas do AWR. Recomendamos

que você use vários relatórios AWR durante o período de pico de carga para estimar os recursos necessários para lidar com esses picos de carga. Além disso, as exibições dinâmicas fornecem mais pontos de dados que ajudam a calcular os requisitos de recursos com mais precisão.

- Você deve estimar o IOPS somente para o banco de dados que planeja migrar, não para outros bancos de dados e processos que usam o disco.
- Para calcular quanta E/S está sendo usada pelo banco de dados, não use as informações na seção Perfil de carga do relatório AWR. Em vez disso, use a seção Perfil de E/S, se estiver disponível, ou vá para a seção Estatísticas de atividade da instância e veja os valores totais das operações físicas de leitura e gravação.
- Ao estimar a utilização da CPU, recomendamos que você use o método de métricas do banco de dados em vez das estatísticas do sistema operacional (SO), porque ele se baseia na CPU usada somente pelos bancos de dados. (As estatísticas do SO também incluem o uso da CPU por outros processos.) Você também deve verificar as recomendações relacionadas à CPU no relatório ADDM para melhorar o desempenho após a migração.
- Considere os limites de throughput de E/S – throughput do Amazon Elastic Block Store (Amazon EBS) e throughput de rede – para o tamanho específico da instância ao determinar o tipo certo de instância.
- Execute o teste de desempenho antes da migração para validar o tamanho do mecanismos.

Épicos

Crie um relatório AWR

Tarefa	Descrição	Habilidades necessárias
Ative o relatório AWR.	Para ativar o relatório, siga as instruções na documentação da Oracle.	DBA
Verifique o período de retenção.	Para verificar o período de retenção do relatório do AWR, use a consulta a seguir. `SQL> SELECT snap_interval,retention FROM dba_hist_wr_control;`	DBA

Tarefa	Descrição	Habilidades necessárias
Gere o snapshot.	Se o intervalo do snapshot do AWR não for granular o suficiente para capturar o pico da workload, você poderá gerar o relatório do AWR manualmente. Para gerar o snapshot manual do AWR, use a consulta a seguir. `SQL> EXEC dbms_workload_repository.create_snapshot;`	DBA
Confira os snapshots recentes.	Para verificar snapshots recentes do AWR, use a consulta a seguir. `SQL> SELECT snap_id, to_char(begin_interval_time,'dd/MON/yy hh24:mi') Begin_Interval, to_char(end_interval_time,'dd/MON/yy hh24:mi') End_Interval FROM dba_hist_snapshot ORDER BY 1;`	DBA

Estime os requisitos de E/S de disco

Tarefa	Descrição	Habilidades necessárias
Escolha um método.	O IOPS é a medida padrão das operações de entrada e saída por segundo em um	DBA

Tarefa	Descrição	Habilidades necessárias
	dispositivo de armazenamento e inclui operações de leitura e gravação. Se você estiver migrando um banco de dados on-premis es para o AWS, precisará determinar o pico de E/S de disco usado pelo banco de dados. Você pode usar os seguintes métodos para estimar a E/S do disco para seu banco de dados de destino: • Seção de perfil de carga do relatório AWR • Seção Estatísticas de atividade da instância do relatório AWR (use esta seção para o Oracle Database 12c ou superior) • Seção Perfil de E/S do relatório AWR (use esta seção para versões do banco de dados Oracle anteriores à 12c) • Visualizações do AWR As etapas a seguir descrevem esses quatro métodos.	

Tarefa	Descrição	Habilidades necessárias
Opção 1: use o perfil de carga.	A tabela a seguir mostra um exemplo da seção Perfil de carga do relatório AWR. **Important** Para obter informaçõ es mais precisas, recomendamos que você use a opção 2 (perfis de E/S) ou a opção 3 (estatíst icas de atividade da instância) em vez do perfil de carga. Por Segu / Por Tran / Por Exec / Por Chama Tem de banc de dadc: 26,6 / 0.2 / 0,00 / 0,02 CPU de banc de dadc: 18,0 / 0.1 / 0,00 / 0,01 CPU de fund: 0.2 / 0.0 / 0,00 / 0,00	DBA

Tarefa	Descrição		Habilidades necessárias
	Tam do redo (byte	2.45 ,9	17.0
	Leitu lógic (bloc	3.37 ,5	23.4
	Bloq alter s:	21.6	150,5
	Leitu físic (bloc	13.5	94,4
	Grav físic (bloc	3.46	24,1
	Leia as solic ões de IO:	3.58	24,9
	Solic ões de grav	574,7	4,0
	IO de	106.	0.7

Tarefa	Descrição		Habilidades necessárias
	leitur (MB)		
	Escr IO (MB)	27.1	0.2
	Linha de verifi ão de mens insta eas:	0.0	0.0
	Mens insta ea de leitur lógic da sess		
	Char de usuá	1.24	8.7
	Análi (SQL	4.62	32.2
	Análi física (SQL	8.9	0.1

Tarefa	Descrição	Habilidades necessárias
	Área de traba SQL (MB) 824,9 5.7 Log on: 1,7 0.0 Exec (SQL 136.6 950,4 Reve : 22,9 0.2 Tran s: 143,8 Com base nessas informaçõ es, você pode calcular IOPs e gerar a taxa de transferência da seguinte forma: IOPS = Solicitações de E/S de leitura: + Solicitações de E/S de gravação = 3.586,8 + 574,7 = 4.134,5 Throughput = leitura física (blocos) + Gravação física (blocos) = 13.575,1 + 3.467,3 = 17.042,4 Como o tamanho do bloco no Oracle é de 8 KB, você pode	

Tarefa	Descrição	Habilidades necessárias
	calcular a throughput total da seguinte forma: A throughput total em MB é 17.042,4 * 8 * 1024/1024/1024 = 133,2 MB ⚠ Warning Não use o perfil de carga para estimar o tamanho da instância . Ele não é tão preciso quanto as estatísti cas de atividade da instância ou os perfis de E/S.	

Tarefa	Descrição	Habilidades necessárias
Opção 2: use estatísticas de atividade da instância.	Se você estiver usando uma versão do banco de dados Oracle anterior à 12c, poderá usar a seção Estatísticas de atividade da instância do relatório AWR para estimar o IOPS e a throughput. A tabela a seguir mostra um exemplo dessa seção. Estatística / Total / por Segun / por Trans leitura física total de solicitações de E/S / 2.547.217 / 3.610, / 25.11 total de bytes de leitura física / 80.776.124. / 114.48 26,26 / 796.149 8 gravaç física total de solicitações / 534.19 08 / 757,1 / 5.27	DBA

Tarefa	Descrição	Habilidades necessárias
	de E/S total de bytes de gravaç física 25.517 8.849. 36.16 1,84 251.508 8 Com base nessas informaçõ es, você pode calcular o total de IOPs e a throughput da seguinte forma: IOPS total = 3.610,28 + 757,11 = 4.367 Total de Mbps = 114.482.4 26,26 + 36.165.631,84 = 150.648.058,1/1024/1024 = 143 Mbps	

Tarefa	Descrição	Habilidades necessárias
Opção 3: usar perfis de E/S.	No banco de dados Oracle 12c, o relatório AWR inclui uma seção de Perfis de E/S que apresenta todas as informações em uma única tabela e fornece dados mais precisos sobre o desempenho do banco de dados. A tabela a seguir mostra um exemplo dessa seção. Leitura + gravaç por segun Leitura por Segun Gravaçõ por Segund Total de solicitações: 4.367, 3.610, 757,1 Solicitações de banco de dados 4.161, 3.586, 574,7 Solicitações otimizas: 0.0 0.0 0.0	DBA

Tarefa	Descrição			Habilidades necessárias
	Solicitações para refaze	179,3	2.8	176,6
	Total (MB):	143,7	109.2	34,5
	Banco de dados (MB):	133.1	106.1	27.1
	Total otimiza (MB):	0.0	0.0	0.0
	Refaze (MB):	7.6	2.7	4,9
	Banco de dados (bloco	17.042	13.575	3.467,3
	Por meio do Buffer de Cache (bloco	5.898,	5.360,	537,6
	Direto (bloco	11.143	8.214,	2.929,7

Tarefa	Descrição	Habilidades necessárias
	Essa tabela fornece os seguintes valores de throughput e IOPS total: Throughput = 143 MBPS (da quinta linha, rotulada como Total, segunda coluna) IOPS = 4.367,4 (da primeira linha, chamada Total de solicitações, segunda coluna)	

Opção 4: usar visualizações AWR.	Você pode ver as mesmas informações de IOPS e throughput usando visualizações do AWR. Para obter essas informações, use a seguinte consulta:
	
	`break on report`
	`compute sum of Value on report`
	`select METRIC_NAME,avg(AVERAGE) as "Value"`
	`from dba_hist_sysmetric_summary`
	`where METRIC_NAME in ('Physical Read Total IO Requests Per Sec','Physical Write Total IO Requests Per Sec')`
	`group by metric_name;`
		DBA

Estime os requisitos de CPU

Tarefa	Descrição	Habilidades necessárias
Escolha um método.	Você pode estimar a CPU necessária para o banco de dados de destino de três maneiras: • Usando os núcleos reais disponíveis do processador • Usando os núcleos utilizados com base nas estatísticas do SO • Usando os núcleos utilizados com base nas estatísticas do banco de dados Se você estiver analisando núcleos utilizados, recomendamos usar o método de métricas do banco de dados em vez das estatísticas do SO, pois ele se baseia na CPU usada somente pelos bancos de dados que você planeja migrar. (As estatísticas do SO também incluem o uso da CPU por outros processos.) Você também deve verificar as recomendações relacionadas à CPU no relatório ADDM para melhorar o desempenho após a migração. Você também pode estimar os requisitos com base na	DBA

Tarefa	Descrição	Habilidades necessárias
	geração da CPU. Se você estiver usando diferentes gerações de CPU, poderá estimar a CPU necessária do banco de dados de destino seguindo as instruções no whitepaper Desmistificando o número de v CPUs para um desempenho ideal da carga de trabalho.	

Tarefa	Descrição	Habilidades necessárias
Opção 1: estimar os requisitos com base nos núcleos disponíveis.	Nos relatórios do AWR: • CPUs referem-se ao lógico e ao virtual CPUs. • Os núcleos são o número de processadores em um chipset físico de CPU. • Um soquete é um dispositivo físico que conecta um chip a uma placa. Os processadores de vários núcleos têm soquetes com vários núcleos de CPU. Você pode estimar os núcleos disponíveis de duas maneiras: • Usando os comandos de OS • Usando o relatório AWR Para estimar os núcleos disponíveis usando comandos do sistema operacional Use o comando a seguir para contar os núcleos no processador. `$ cat /proc/cpuinfo | grep "cpu cores"|uniq cpu cores : 4 cat /proc/cpuinfo | egrep "core id|physical id" | tr -d "\n" |`	DBA

Tarefa	Descrição	Habilidades necessárias

	`sed s/physical/\\nphysical/g | grep -v ^$ | sort | uniq | wc -l`
	
	Use o comando a seguir para contar os soquetes no processador.
	
	`grep "physical id" /proc/cpuinfo | sort -u`
	`physical id : 0`
	`physical id : 1`
	
	Note
	Não recomendamos o uso de comandos do sistema operacional, como nmon e sar, para extrair a utilização da CPU. Isso ocorre porque esses cálculos incluem a utilização da CPU por outros processos e podem não refletir a CPU real usada pelo banco de dados.
	
	Para estimar os núcleos disponíveis usando o relatório AWR
	
	Você também pode derivar a utilização da CPU na primeira	

Tarefa	Descrição	Habilidades necessárias
	seção do relatório AWR. Veja um trecho do relatório. N ID Inst Insi Hor Ver: R/ d do um de b ban núm iníci d de d dad X <DE XX) 1 05 12.1 Nã de 0 sete de 202 23:(Nor Plat CPU Núc Soq Mem do a (GB) hos <ho Linu 80 80 2 441,7 e> x86 de 64 bits Neste exemplo, a CPUs contagem é 80, o que indica que elas são lógicas (virtuais) CPUs. Você também pode ver que essa configura ção tem dois soquetes, um processador físico em cada soquete (para um total de dois processadores físicos) e 40	

Tarefa	Descrição	Habilidades necessárias
	núcleos para cada processad or ou soquete físico.	

Tarefa	Descrição	Habilidades necessárias
Opção 2: estimar a utilização da CPU usando estatísticas do sistema operacional.	Você pode verificar as estatísticas de uso da CPU do sistema operacional diretamente no sistema operacional (usando sar ou outro utilitário do SO host) ou revisando os valores de IDLE/ (IDLE +BUSY) na seção Estatísticas do sistema operacional do relatório AWR. Você pode ver os segundos de CPU consumidos diretamente de v$osstat. Os relatórios AWR e Statspack também mostram esses dados na seção Estatísticas do sistema operacional. Se houver vários bancos de dados na mesma caixa, todos eles terão os mesmos valores de v$osstat para BUSY_TIME. Estatística / Valor / Valor final FREE_MEMORY_BYT / 6.810.67.248 / 12.280.799.232 INACTIVE_MEMORY_BYTES / 175.627.33.632 / 160.380.653.568 SWAP_FREE_BYTES / 17.145.64.336 / 17.145.872.384	DBA

Tarefa	Descrição		Habilidades necessárias
	BUSY_T	1.305.56 .937	
	IDLE_TI	4.312.71 .839	
	IOWAIT_ ME	53.417.1 4	
	NICE_TI	29.815	
	SYS_TIM	148.567. 70	
	USER_T	1.146.91 .783	
	LOAD	25	29
	VM_EM_ ES	593.920	
	VM_OUT TES	327.680	
	PHYSIC/ MEMOR TES	474.362. 17.152	
	NUM_CF	80	
	NUM_CF ÚCLEOS	80	
	NUM_CF OCKETS	2	

Tarefa	Descrição	Habilidades necessárias
	GLOBAL_SEND_SIZE_MAX 4.194.304 GLOBAL_RECEIVE_SIZE_MAX 2.097.152 TCP_RECEIVE_SIZE_DEFAULT 87.380 TCP_RECEIVE_SIZE_MAX 6.291.456 TCP_RECEIVE_SIZE_MIN 4.096 TCP_SEND_SIZE_DEFAULT 16.384 TCP_SEND_SIZE_MAX 4.194.304 TCP_SEND_SIZE_MIN 4.096	
	Se não houver outros grandes consumidores de CPU no sistema, use a fórmula a seguir para calcular a porcentagem de utilização da CPU:	

Tarefa	Descrição	Habilidades necessárias
	Utilização = Tempo de ocupação/Tempo total Tempo ocupado = requisitos = v$OSStat.BUSY_TIME C = Tempo total (ocupado + ocioso) C = capacidade = v$ostat.BUSY_TIME + v$ostat.IDLE_TIME Utilização = BUSY_TIME/(BUSY_TIME + IDLE_TIME) = -1.305.569.937/(1.305.569.937 + 4.312.718.839) = 23% utilizados	

Tarefa	Descrição	Habilidades necessárias
Opção 3: estimar a utilização da CPU usando métricas de banco de dados.	Se vários bancos de dados estiverem em execução no sistema, você poderá usar as métricas do banco de dados que aparecem no início do relatório. Snap Id / Tem do snap / Sess / Curso Sessã Com o Snap 1846 28-Set-2 09:0(1226 35,8 Fim do Snap 1854 06-Out-2 13:0(1876 41.1 Decc : 11.7! (minu Tem de banc de dadc 312.(0 (minu Para obter métricas de utilização da CPU, use esta fórmula: Uso da CPU do banco de dados (porcentagem da energia da CPU disponível) =	DBA

Tarefa	Descrição	Habilidades necessárias
	tempo de CPU/NUM_CPUS/ tempo decorrido onde o uso da CPU é descrito pelo tempo da CPU e representa o tempo gasto na CPU, não o tempo de espera pela CPU. Esse cálculo resulta em: = 312.625,40/11.759,64/80 = 33% da CPU está sendo usada Número de núcleos (33%) * 80 = 26,4 núcleos Total de núcleos = 26,4 * (120%) = 31,68 núcleos Você pode usar o maior desses dois valores para calcular a utilização da CPU da instância de banco de dados Amazon RDS ou Aurora. **Note** No IBM AIX, a utilização calculada não corresponde aos valores do sistema operacional ou do banco de dados. Esses valores	

Tarefa	Descrição	Habilidades necessárias
	coincidem em outros sistemas operacionais.	

Estime os requisitos de memória

Tarefa	Descrição	Habilidades necessárias
Estime os requisitos de memória usando estatísticas de memória.	Você pode usar o relatório AWR para calcular a memória do banco de dados de origem e combiná-la com o banco de dados de destino. Você também deve verificar o desempenho do banco de dados existente e reduzir seus requisitos de memória para economizar custos ou aumentar seus requisitos para melhorar o desempenho. Isso requer uma análise detalhada do tempo de resposta do AWR e do Acordo de Serviço (SLA) (SLA) do aplicativo. Use a soma do uso da área global do sistema Oracle (SGA) e da área global do programa (PGA) como a utilização de memória estimada para o Oracle. Adicione 20% a mais para o sistema operacional para determinar um requisito de tamanho de memória alvo. Para o Oracle RAC, use a soma da utilização estimada	DBA

Tarefa	Descrição	Habilidades necessárias
	da memória em todos os nós do RAC e reduza a memória total, pois ela está armazenada em blocos comuns. 1. Verifique as métricas na tabela de porcentagem de eficiência da instância. A tabela usa os seguintes termos: • A porcentagem de acertos no buffer é a porcentagem de vezes que um determinado bloco foi encontrado no cache do buffer em vez de realizar uma E/S física. Para um melhor desempenho, almeje 100 por cento. • A porcentagem do buffer sem espera deve estar próxima de 100 por cento. • A porcentagem de Latch Hit deve estar próxima de 100 por cento. • A porcentagem de CPU sem análise é a porcentagem do tempo de CPU gasto em atividades sem análise. Esse valor deve estar	

Tarefa	Descrição	Habilidades necessárias
	próximo de 100 por cento. Porcentagens de eficiência da instância (meta de 100%) Porce 99,99 NoWa 100,00 em % de de buffer refaze sem esper % 99,84 Porce 100,00 de em impac de no classi buffer ação na memó Porce 748,7 Porce 99,81 em em de de acerto anális na flexíve biblio as Porce 96,61 Porce 100,00 em em de de execu latch para hit:	

Tarefa	Descrição	Habilidades necessárias
	analis Porce 72,73 Porce 99,21 em em de de anális CPU de sem CPU anális para anális decor : Porce 0,00 em de acerto de flash cache Neste exemplo, todas as métricas parecem boas, então você pode usar a SGA e a PGA para o banco de dados existente como requisito de planejamento de capacidade. 2. Verifique a seção de estatísticas de memória e calcule o SGA/PGA. Início Fim	

Tarefa	Descrição	Habilidades necessárias
	Memória do host (MB): 452.387 452.387,3 Uso da SGA (MB): 220.544 220.544,0 Uso do PGA (MB): 36.874,9 45.270,0 Memória total da instância em uso = SGA + PGA = 220 GB + 45 GB = 265 GB Adicionar 20% do buffer: Memória total da instância = 1,2 * 265 GB = 318 GB Como a SGA e a PGA representam 70% da memória do host, o requisito total de memória é: Memória total do host = 318/0,7 = 464 GB **Note** Quando você migra para o Amazon RDS	

Tarefa	Descrição	Habilidades necessárias
	for Oracle, a PGA e a SGA são pré-calculadas com base em uma fórmula predefinida. Certifique-se de que os valores pré-calculados estejam próximos às suas estimativas.	

Determine o tipo de instância de banco de dados do banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Determine o tipo de instância de banco de dados com base nas estimativas de E/S de disco, CPU e memória.	Com base nas estimativas das etapas anteriores, a capacidade do banco de dados Amazon RDS ou Aurora de destino deve ser: • 68 núcleos de CPU • 143 MBPS de throughput • 4367 IOPS para E/S de disco • 464 GB de memória No banco de dados Amazon RDS ou Aurora de destino, você pode mapear esses valores para o tipo de instância db.r5.16xlarge, que tem uma capacidade de 32 núcleos, 512 GB de RAM e	DBA

Tarefa	Descrição	Habilidades necessárias
	13.600 Mbps de throughput. Para obter mais informações, consulte a postagem no blog da AWS. Use o tamanho certo de instâncias do Amazon RDS em uma escala com base nas métricas de desempenho da Oracle.	

Recursos relacionados

- Classe de instância de banco de dados Aurora (documentação do Amazon Aurora)
- armazenamento de instância de banco de dados do Amazon RDS (documentação do Amazon RDS)
- Ferramenta AWS Miner (GitHub repositório)

Exporter tabelas do Amazon RDS para SQL Server para um bucket do S3 usando o AWS DMS

Criado por Subhani Shaik (AWS)

Resumo

O Amazon Relational Database Service (Amazon RDS) para SQL Server não oferece suporte ao carregamento de dados em outros servidores vinculados a mecanismos de banco de dados na nuvem da Amazon Web Services (AWS). Em vez disso, você pode usar o AWS Database Migration Service (AWS DMS) para exportar tabelas do Amazon RDS para SQL Server para um bucket do Amazon Simple Storage Service (Amazon S3), onde os dados estão disponíveis para outros mecanismos de banco de dados.

O AWS DMS ajuda a migrar bancos de dados para a AWS com facilidade e segurança. O banco de dados de origem permanece totalmente operacional durante a migração, o que minimiza o tempo de inatividade de aplicativos que dependem do banco de dados. O AWS DMS pode migrar seus dados dos/para os bancos de dados comerciais e de código aberto mais usados no mercado.

Esse padrão usa o AWS Secrets Manager ao configurar os endpoints do AWS DMS. O Secrets Manager ajuda você a proteger os segredos necessários para acessar aplicativos, serviços e recursos de TI. Você pode usar o serviço para alternar, gerenciar e recuperar credenciais de banco de dados, chaves de API e outros segredos durante seu ciclo de vida. Usuários e aplicativos recuperam segredos com uma chamada para o Secrets Manager, reduzindo a necessidade de codificar informações confidenciais. O Secrets Manager oferece alternância secreta com integração embutida para o Amazon RDS, o Amazon Redshift e o Amazon DocumentDB. Além disso, o serviço é extensível a outros tipos de segredos, incluindo chaves e OAuth tokens de API. Com o Secrets Manager, você pode controlar o acesso a segredos ao usar permissões refinadas e auditar a rotação de segredos centralmente para recursos na Nuvem AWS, serviços de terceiros e ambientes on-premises.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do S3
- Uma nuvem privada virtual (VPC)

- Uma sub-rede de banco de dados
- Amazon RDS para SQL Server
- Um perfil do AWS Identity and Access Management (IAM) com acesso (listar, obter e colocar objetos) ao bucket do S3 em nome da instância do Amazon RDS.
- Secrets Manager para armazenar as credenciais da instância RDS.

Arquitetura

Pilha de tecnologia

- Amazon RDS para SQL Server
- AWS DMS
- Amazon S3
- AWS Secrets Manager

Arquitetura de destino

O diagrama a seguir mostra a arquitetura para importar dados da instância do Amazon RDS para o bucket do S3 com a ajuda do AWS DMS.

1. A tarefa de migração do AWS DMS que se conecta à instância de origem do Amazon RDS por meio do endpoint de origem
2. Copiar dados da instância de origem do Amazon RDS
3. A tarefa de migração do AWS DMS que se conecta ao bucket do S3 de destino por meio do endpoint de destino
4. Exportar dados copiados para o bucket do S3 no formato de valores separados por vírgula (CSV)

Ferramentas

Serviços da AWS

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente.

Outros serviços

- O Microsoft SQL Server Management Studio (SSMS) é uma ferramenta para gerenciar o SQL Server, incluindo acesso, configuração e administração de componentes do SQL Server.

Épicos

Configurar a instância do Amazon RDS para SQL Server

Tarefa	Descrição	Habilidades necessárias
Criar a instância do Amazon RDS para SQL Server.	1. Abra o Console de Gerenciamento da AWS, escolha RDS e use a opção Criação padrão para criar uma instância do Amazon RDS com a edição necessária, como SQL Server Express Edition, SQL Server Standard Edition ou SQL Server Enterprise Edition. Para a versão, escolha 2016 ou superior. 2. Em Modelos, escolha Dev/Test.	DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
Configurar as credenciais para a instância.	1. Insira um nome para a instância. 2. Forneça um nome de usuário e senha para a instância do Amazon RDS.	DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
Configurar a classe, o armazenamento, o ajuste de escala automático e a disponibilidade da instância.	1. Selecione a classe da instância de banco de dados na lista: classes Padrão, Memória otimizada e Intermitente. Escolha o tipo de instância de banco de dados que aloca a capacidade computacional, de rede e de memória exigida pelas workloads planejadas para essa instância de banco de dados. Para obter mais informações, consulte a documentação da AWS. 2. Selecione o tipo de armazenamento na lista: SSD de uso geral, SSD de IOPS provisionadas ou Magnético.. Aloque o tamanho de armazenamento padrão conforme necessário. 3. Escolha Habilitar escalabilidade automática de armazenamento para aumentar o armazenamento do Amazon RDS com base no seu planejamento de capacidade. 4. Uma implantação Multi-AZ com uma instância de replicação é compatível com o AWS DMS. No	DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
	caso de uma interrupção na zona de disponibilidade, no hardware interno ou na rede, o AWS DMS criará uma instância em espera e fornecerá alta disponibilidade (HA) por meio de failover automático para as réplicas em espera. Dependendo do tamanho da importação, selecione a opção apropriada.	
Especificar a VPC, o grupo de sub-rede, o acesso público e o grupo de segurança.	Selecione a VPC, os grupos de sub-redes de banco de dados e o grupo de segurança da VPC conforme necessário para criar a instância do Amazon RDS. Siga as práticas recomendadas, por exemplo: • Não habilite o acesso público à instância de banco de dados do RDS. • Não use o CIDR 0.0.0.0/0 nos grupos de segurança. • Use somente o endereço IP e os detalhes da porta necessários para acessar a instância do RDS.	DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
Configurar o monitoramento, o backup e a manutenção.	1. Especifique as opções de backup que você deseja. Por padrão, os backups automáticos são habilitados com um período de retenção de sete dias. 2. Escolha as configurações apropriadas de atualização automática da versão secundária e da janela de manutenção para aplicar as modificações ou a manutenção pendente ao banco de dados pelo Amazon RDS. 3. Selecione Criar banco de dados.	DBA, engenheiro DevOps

Configurar o banco de dados e os dados de exemplo

Tarefa	Descrição	Habilidades necessárias
Criar uma tabela e carregar os dados de exemplo.	No novo banco de dados, crie uma tabela. Use o código de exemplo na seção Informações adicionais para carregar dados na tabela.	DBA, engenheiro DevOps

Configurar credenciais

Tarefa	Descrição	Habilidades necessárias
Crie o segredo.	1. No console, selecione Secrets Manager e escolha Armazenar um novo segredo. 2. Insira um nome de usuário e senha para o banco de dados do Amazon RDS para SQL Server. Esse segredo será usado para o endpoint de origem do AWS DMS.	DBA, engenheiro DevOps

Configurar o acesso entre o banco de dados e o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM para acessar o Amazon RDS.	1. No console, escolha IAM e crie um perfil do IAM que dê acesso de leitura/gravação a um bucket do S3 ao Amazon RDS. 2. Em Atributo, selecione Integração do S3.	DBA, engenheiro DevOps

Criar um bucket do S3.

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Para salvar os dados do Amazon RDS para SQL	DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
	Server, no console, escolha S3 e, em seguida, escolha Criar bucket. Certifique-se que o bucket do S3 não está disponível ao público.	

Configurar o acesso entre o AWS DMS e o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM para o AWS DMS acessar o Amazon S3.	Crie um perfil do IAM que permita ao AWS DMS listar, obter e colocar objetos do bucket do S3.	DBA, engenheiro DevOps

Configurar o AWS DMS.

Tarefa	Descrição	Habilidades necessárias
Criar um endpoint do AWS DMS para a origem.	1. No console, escolha Serviço de migração de banco de dados e escolha Endpoints. Crie o endpoint de origem, marcando a caixa de seleção Selecionar instância de banco de dados do RDS. 2. Para o mecanismo de origem, selecione Microsoft SQL Server. 3. Em Acesso ao banco de dados do endpoint, escolha AWS Secrets Manager e	DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
	insira o segredo e o perfil do IAM que você criou anteriormente e o nome do banco de dados. 4. Teste o endpoint de origem.	
Criar um endpoint do AWS DMS para o destino.	Crie o Endpoint de destino, selecionando Amazon S3 como Mecanismo de destino. Forneça o nome do bucket do S3 e o nome da pasta para o perfil do IAM criada anteriormente.	DBA, engenheiro DevOps
Criar uma instância de replicação do AWS DMS.	Na mesma VPC, sub-rede e grupo de segurança, crie a instância de replicação do AWS DMS. Para obter mais informações sobre como escolher classe de instância, consulte a documentação da AWS.	DBA, engenheiro DevOps
Criar a tarefa de migração do AWS DMS.	Para exportar os dados do Amazon RDS para SQL Server para o bucket do S3, crie uma tarefa de migração de banco de dados. Para tipo de migração, selecione Migrar dados existentes. Selecione os endpoints e a instância de replicação do AWS DMS que você criou.	DBA, engenheiro DevOps

Exportar os dados para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Executar a tarefa de migração do banco de dados.	Para exportar os dados da tabela do SQL Server, inicie a tarefa de migração do banco de dados. A tarefa exportará os dados do Amazon RDS para SQL Server para o bucket do S3 no formato CSV.	DBA, engenheiro DevOps

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Excluir os recursos.	Para evitar custos extras, use o console para excluir os recursos na seguinte ordem: 1. Tarefa de migração 2. Instância da replicação 3. Endpoints 4. Bucket do S3 5. Instância do banco de dados	DBA, engenheiro DevOps

Recursos relacionados

- AWS DMS
- Amazon S3
- Amazon RDS para SQL Server
- Integração do Amazon S3

Mais informações

Para criar o banco de dados e a tabela e carregar os dados de exemplo, use o código a seguir.

```
--Step1: Database creation in RDS SQL Server
CREATE DATABASE [Test_DB]
 ON  PRIMARY
( NAME = N'Test_DB', FILENAME = N'D:\rdsdbdata\DATA\Test_DB.mdf' , SIZE = 5120KB ,
 FILEGROWTH = 10%)
 LOG ON
( NAME = N'Test_DB_log', FILENAME = N'D:\rdsdbdata\DATA\Test_DB_log.ldf' , SIZE =
 1024KB , FILEGROWTH = 10%)
GO

--Step2: Create Table
USE Test_DB
GO
Create Table Test_Table(ID int, Company Varchar(30), Location Varchar(20))

--Step3: Load sample data.
USE Test_DB
GO
Insert into Test_Table values(1,'AnyCompany','India')
Insert into Test_Table values(2,'AnyCompany','USA')
Insert into Test_Table values(3,'AnyCompany','UK')
Insert into Test_Table values(4,'AnyCompany','Hyderabad')
Insert into Test_Table values(5,'AnyCompany','Banglore')
```

Manipule blocos anônimos em instruções de SQL dinâmico no Aurora PostgreSQL

Criado por anuradha chintha (AWS)

Resumo

Esse padrão mostra como evitar o erro que você recebe ao manipular blocos anônimos em instruções de SQL dinâmico. Você recebe uma mensagem de erro ao usar o AWS Schema Conversion Tool para converter um banco de dados Oracle em um banco de dados Aurora compatível com PostgreSQL. Para evitar o erro, você deve saber o valor de uma variável de ligação OUT, mas não pode saber o valor de uma variável de ligação OUT até depois de executar a instrução SQL. O erro resulta do fato de a AWS Schema Conversion Tool (AWS SCT) não entender a lógica dentro da instrução Dynamic SQL. A AWS SCT não pode converter a instrução de SQL dinâmico em código PL/SQL (ou seja, funções, procedimentos e pacotes).

Pré-requisitos e limitações

Pré-requisitos

- Conta da AWS ativa
- Instância de banco de dados (DB) Aurora PostgreSQL
- Amazon Relational Database Service (Amazon RDS) para instância de banco de dados Oracle
- Terminal interativo PostgreSQL (psql)
- SQL *Plus
- Esquema `AWS_ORACLE_EXT` (parte do pacote de extensão AWS SCT) em seu banco de dados de destino
- Versão mais recente da AWS Schema Conversion Tool (AWS SCT) e seus drivers necessários

Arquitetura

Pilha de tecnologia de origem

- Oracle Database on-premises 10g e versão posterior

Pilha de tecnologias de destino

- Amazon Aurora PostgreSQL
- Amazon RDS para PostgreSQL
- AWS Schema Conversion Tool (AWS SCT)

Arquitetura de migração

O diagrama a seguir mostra como usar as variáveis de ligação 0UT AWS SCT e Oracle para escanear o código do seu aplicativo em busca de instruções SQL incorporadas e converter o código em um formato compatível que um banco de dados Aurora possa usar.

O diagrama mostra o seguinte fluxo de trabalho:

1. Gere um relatório da AWS SCT para o banco de dados de origem usando o Aurora PostgreSQL como banco de dados de destino.
2. Identifique o bloco anônimo no bloco de código SQL dinâmico (para o qual a AWS SCT gerou o erro).
3. Converta o bloco de código manualmente e implante o código em um banco de dados de destino.

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL.
- O Amazon Relational Database Service (Amazon RDS) para Oracle ajuda você a configurar, operar e escalar um banco de dados relacional Oracle na Nuvem AWS.
- O AWS Schema Conversion Tool (AWS SCT) ajuda você a tornar previsíveis migrações heterogêneas de bancos de dados ao converter automaticamente o esquema do banco de dados de origem e a maioria dos objetos de código do banco de dados em um formato compatível com o banco de dados de destino.

Outras ferramentas

- O pgAdmin permite que você se conecte e interaja com seu servidor de banco de dados.

- O Oracle SQL Developer é um ambiente de desenvolvimento integrado que você pode usar para desenvolver e gerenciar bancos de dados no Oracle Database. Você pode usar o SQL *Plus ou o Oracle SQL Developer para esse padrão.

Épicos

Configurar o banco de dados de origem do Oracle

Tarefa	Descrição	Habilidades necessárias
Crie uma instância Oracle no Amazon RDS ou na Amazon EC2.	Para criar uma instância de banco de dados Oracle no Amazon RDS, consulte Criar uma instância de banco de dados Oracle e conectar-se a um banco de dados em uma instância Oracle na documentação do Amazon RDS. Para criar uma instância de banco de dados Oracle no Amazon Elastic Compute Cloud (Amazon EC2), consulte Amazon EC2 for Oracle na documentação do AWS Prescriptive Guidance.	DBA
Crie um esquema de banco de dados e objetos para migração.	É possível usar o Amazon Cloud Directory para criar um esquema de banco de dados. Para obter mais informações, consulte Criar um esquema na documentação do Cloud Directory.	DBA
Configurar grupos de segurança de entrada e saída.	Para criar e configurar grupos de segurança, consulte	DBA

Tarefa	Descrição	Habilidades necessárias
	Controle de acesso com grupos de segurança na documentação do Amazon RDS.	
Confirme se o banco de dados está em execução.	Para verificar o status do seu banco de dados, consulte Visualização de eventos do Amazon RDS na documentação do Amazon RDS.	DBA

Configurar o banco de dados Aurora PostgreSQL de destino

Tarefa	Descrição	Habilidades necessárias
Crie uma instância do Aurora PostgreSQL no Amazon RDS.	Para criar uma instância do Aurora PostgreSQL, consulte Criar um cluster de banco de dados e conectar-se a um banco de dados em um cluster de banco de dados do Aurora PostgreSQL, na documentação do Amazon RDS.	DBA
Configure um grupo de segurança de entrada e saída.	Para criar e configurar grupos de segurança, consulte Fornecer acesso ao cluster de banco de dados na VPC criando um grupo de segurança na documentação do Aurora.	DBA
Confirme se o banco de dados do Aurora PostgreSQL está em execução.	Para verificar o status do seu banco de dados, consulte Visualização de eventos do	DBA

Tarefa	Descrição	Habilidades necessárias
	Amazon RDS na documentação do Aurora.	

Configurar a AWS SCT

Tarefa	Descrição	Habilidades necessárias
Conecte a AWS SCT ao banco de dados de origem.	Para conectar a AWS SCT ao seu banco de dados de origem, consulte Conectar ao PostgreSQL como origem na documentação da AWS SCT.	DBA
Conecte a AWS SCT ao seu banco de dados de destino.	Para conectar a AWS SCT ao seu banco de dados de destino, consulte O que é a AWS Schema Conversion Tool? no Guia do usuário da AWS Schema Conversion Tool.	DBA
Converta o esquema do banco de dados na AWS SCT e salve o código convertido automatizado como um arquivo SQL.	Para salvar arquivos convertidos da AWS SCT, consulte Salvar e aplicar seu esquema convertido na AWS SCT no Guia do usuário da AWS Schema Conversion Tool.	DBA

Migrar o código

Tarefa	Descrição	Habilidades necessárias
Obtenha o arquivo SQL para conversão manual.	No arquivo convertido da AWS SCT, extraia o arquivo SQL que requer conversão manual.	DBA
Atualize o script.	Atualize manualmente o arquivo SQL.	DBA

Recursos relacionados

- Amazon RDS
- Atributos do Amazon Aurora

Mais informações

O código do exemplo a seguir mostra como configurar o banco de dados de origem do Oracle:

```
CREATE or replace PROCEDURE calc_stats_new1 (
  a NUMBER,
  b NUMBER,
  result out NUMBER)
IS
BEGIN
result:=a+b;
END;
/
```

```
set serveroutput on ;

DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN calc_stats_new1(:a, :b,:output); END;';
```

```
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;
  DBMS_OUTPUT.PUT_LINE('output:'||output);

END;
```

O código do exemplo a seguir mostra como configurar o banco de dados de destino do Aurora PostgreSQL:

```
 w integer,
 x integer)
RETURNS integer
AS
$BODY$
DECLARE
begin
return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized
      ('test_pg' ) then
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );

PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;


DO $$
declare
v_sql text;
```

```
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$
```

Lide com funções sobrecarregadas do Oracle no Aurora compatível com PostgreSQL

Criado por Sumana Yanamandra (AWS)

Resumo

O código que você migra de um banco de dados Oracle on-premises para Amazon Aurora Edição Compatível com PostgreSQL pode incluir funções sobrecarregadas. Essas funções têm a mesma definição, ou seja, o mesmo nome da função e o mesmo número e tipo de dados dos parâmetros de entrada (`IN`), mas o tipo de dados ou o número de parâmetros de saída (`OUT`) podem ser diferentes.

Essas incompatibilidades de parâmetros podem causar problemas no PostgreSQL, porque é difícil determinar qual função executar. Esse padrão ilustra como lidar com funções sobrecarregadas ao migrar o código do banco de dados para o Aurora compatível com PostgreSQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma instância de banco de dados Oracle como seu banco de dados de origem
- Uma instância de banco de dados compatível com o Aurora PostgreSQL como seu banco de dados de destino (consulte as instruções na documentação do Aurora)

Versões do produto

- Oracle Database 9i ou superior
- Oracle SQL Developer versão 18.4.0.376
- Cliente pgAdmin 4
- Aurora compatível com PostgreSQL versão 11 ou superior (consulte Identificação de versões do Amazon Aurora PostgreSQL na documentação do Aurora)

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL.

Outras ferramentas

- O Oracle SQL Developer é um ambiente de desenvolvimento gratuito e integrado para trabalhar com SQL em bancos de dados Oracle em implantações tradicionais e em nuvem.
- O pgAdmin é uma ferramenta de gerenciamento de software livre para o PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.

Épicos

Criar uma função simples

Tarefa	Descrição	Habilidades necessárias
Crie uma função no PostgreSQL que tenha um parâmetro de entrada e um parâmetro de saída.	O exemplo a seguir ilustra uma função nomeada `test_overloading` no Aurora compatível com PostgreSQL. Essa função tem dois parâmetros: um parâmetro de texto de entrada e um parâmetro de texto de saída. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE BEGIN`	Engenheiro de dados, Aurora compatível com PostgreSQL

Tarefa	Descrição	Habilidades necessárias
	str2 := 'Success'; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;	

Execute a função no PostgreSQL.	Execute a função que você criou na etapa anterior.
	`select public.test_overloading('Test');`
	Isso deve mostrar a seguinte saída.
	`Success`
		Engenheiro de dados, Aurora compatível com PostgreSQL

Sobrecarregar a função

Tarefa	Descrição	Habilidades necessárias
Use o mesmo nome de função para criar uma função sobrecarregada no PostgreSQL.	Crie uma função sobrecarregada no Aurora compatível com PostgreSQL que use o mesmo nome da função anterior. O exemplo a seguir também é nomeado `test_overloading` , mas tem três parâmetros: um parâmetro de texto de entrada, um parâmetro de	Engenheiro de dados, Aurora compatível com PostgreSQL

Tarefa	Descrição	Habilidades necessárias
	texto de saída e um parâmetro inteiro de saída. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text, OUT num1 integer) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE str3 text; BEGIN str2 := 'Success'; num1 := 100; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	

Tarefa	Descrição	Habilidades necessárias

Execute a função no PostgreSQL.	Quando você executa essa função, ela falha com a seguinte mensagem de erro.
	
	`ERROR: cannot change return type of existing function`
	`HINT: Use DROP FUNCTION test_overloading(text) first.`
	
	Isso acontece porque o Aurora compatível com PostgreSQL não oferece suporte direto à sobrecarga de funções. Ele não consegue identificar qual função executar, porque o número de parâmetros de saída é diferente na segunda versão da função, embora os parâmetros de entrada sejam os mesmos.
		Engenheiro de dados, Aurora compatível com PostgreSQL

Aplicar a solução alternativa

Tarefa	Descrição	Habilidades necessárias
Adicione INOUT ao primeiro parâmetro de saída.	Como solução alternativa, modifique o código da função representando o primeiro parâmetro de saída como `INOUT`.	Engenheiro de dados, Aurora compatível com PostgreSQL

Tarefa	Descrição	Habilidades necessárias
	`CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, INOUT str2 text, OUT num1 integer) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE str3 text; BEGIN str2 := 'Success'; num1 := 100; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	

Tarefa	Descrição	Habilidades necessárias

Execute a função revisada.	Execute a função que você atualizou usando a consulta a seguir. Você passa um valor nulo como segundo argumento dessa função, porque declarou esse parâmetro como `INOUT` para evitar o erro.
	`select public.test_overloading('Test', null);`
	A função agora foi criada com sucesso.
	`Success, 100`
		Engenheiro de dados, Aurora compatível com PostgreSQL

Validação dos resultados.	Verifique se o código com a função sobrecarregada foi convertido com êxito.	Engenheiro de dados, Aurora compatível com PostgreSQL

Recursos relacionados

- Trabalhar com Amazon Aurora PostgreSQL (documentação do Aurora)
- Sobrecarga de funções no Oracle (documentação do Oracle)
- Sobrecarga de funções no PostgreSQL (documentação do PostgreSQL)

Ajude a aplicar a marcação no DynamoDB

Criado por Mansi Suratwala (AWS)

Resumo

Esse padrão configura notificações automáticas quando uma tag predefinida do Amazon DynamoDB está ausente ou removida de um recurso do DynamoDB na nuvem da Amazon Web Services (AWS).

O DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que proporciona uma performance rápida e previsível com escalabilidade. O DynamoDB permite que você alivie a carga administrativa de operar e escalar um banco de dados distribuído. Ao usar o DynamoDB, você não precisa se preocupar com provisionamento, instalação e configuração de hardware, replicação, correção de software nem escalabilidade de cluster.

O padrão usa um CloudFormation modelo da AWS, que cria um evento Amazon CloudWatch Events e uma função do AWS Lambda. O evento observa qualquer informação de marcação nova ou existente do DynamoDB usando a AWS. CloudTrail Se uma tag predefinida estiver ausente ou removida, CloudWatch aciona uma função Lambda, que envia uma notificação do Amazon Simple Notification Service (Amazon SNS) informando sobre a violação.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do Amazon Simple Storage Service (Amazon S3) para o arquivo .zip do Lambda que contém o script do Python para execução da função do Lambda

Limitações

- A solução funciona somente quando os `UntagResource` CloudTrail eventos `TagResource` ou ocorrem. Ela não cria notificações para nenhum outro evento.

Arquitetura

Pilha de tecnologias de destino

- Amazon DynamoDB
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Arquitetura de destino

Automação e escala

Você pode usar o CloudFormation modelo da AWS várias vezes para diferentes regiões e contas da AWS. Você precisa executar o modelo somente uma vez em cada região ou conta.

Ferramentas

Ferramentas

- Amazon DynamoDB: o DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade.
- AWS CloudTrail — CloudTrail é um serviço da AWS que ajuda você com governança, conformidade e auditoria operacional e de risco da sua conta da AWS. As ações realizadas por um usuário, função ou serviço da AWS são registradas como eventos em CloudTrail.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- AWS Lambda: o Lambda é um serviço de computação que oferece suporte à execução de código sem a necessidade de provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço web que permite que aplicativos, usuários finais e dispositivos enviem e recebam notificações da nuvem instantaneamente.

Código

- Um arquivo .zip do projeto está disponível como anexo.

Épicos

Definir o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	No console do Amazon S3, escolha ou crie um bucket do S3 com um nome exclusivo que não contenha barras iniciais. Esse bucket do S3 hospedará o arquivo .zip do código do Lambda. Seu bucket do S3 deve estar na mesma região da AWS do recurso do DynamoDB que está sendo monitorado.	Arquiteto de nuvem

Carregar o código do Lambda para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Carregue o código do Lambda para o bucket do S3.	Carregar o arquivo .zip do código do Lambda fornecido na seção Anexos no bucket do S3. O bucket do S3 deve estar na mesma região que o recurso do DynamoDB que está sendo monitorado.	Arquiteto de nuvem

Implemente o CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo da AWS.	No CloudFormation console da AWS, implante o CloudFormation modelo da AWS fornecido na seção Anexos. No próximo épico, forneça valores dos parâmetros.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Dê um nome ao bucket do S3.	Insira o nome do bucket do S3 que você criou ou escolheu no primeiro épico.	Arquiteto de nuvem
Forneça a chave do Amazon S3.	Forneça a localização do arquivo .zip do código do Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `<folder>/<file-name>.zip`).	Arquiteto de nuvem
Fornecer um endereço de e-mail	Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS.	Arquiteto de nuvem
Defina o nível de registro em log.	Defina o nível de registro em log e a frequência da sua função do Lambda. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	
Insira as chaves de tag necessárias do DynamoDB.	Certifique-se de que as tags estejam separadas por vírgulas, sem espaços entre elas (por exemplo,`ApplicationId,CreatedBy,Environment,Organization`). O evento CloudWatch Eventos pesquisa essas tags e envia uma notificação se elas não forem encontradas.	Arquiteto de nuvem

Confirmar a assinatura.

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o modelo é implantado com sucesso, ele envia um e-mail de assinatura para o endereço de e-mail que você forneceu. Para receber notificações de violação, você deve confirmar essa assinatura de e-mail.	Arquiteto de nuvem

Recursos relacionados

- Criar um bucket do S3

- Carregar os arquivos em um bucket do S3
- Marcar recursos no DynamoDB
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS CloudTrail

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Implemente a recuperação de desastres entre regiões com o AWS DMS e o Amazon Aurora

Criado por Mark Hudson (AWS)

Resumo

Desastres naturais ou induzidos pelo homem podem ocorrer a qualquer momento e podem afetar a disponibilidade de serviços e cargas de trabalho em execução em uma determinada região da AWS. Para mitigar os riscos, você deve desenvolver um plano de recuperação de desastres (DR) que incorpore os recursos integrados entre regiões dos serviços da AWS. Para serviços da AWS que não fornecem inerentemente funcionalidade entre regiões, o plano de DR também deve fornecer uma solução para lidar com seu failover em todas as regiões da AWS.

Esse padrão orienta você em uma configuração de recuperação de desastres envolvendo dois clusters de banco de dados da Amazon Aurora edição compatível com MySQL em uma única região. Para atender aos requisitos de DR, os clusters de banco de dados são configurados para usar o atributo do Amazon Aurora Global Database, com um único banco de dados abrangendo várias regiões da AWS. Uma tarefa do AWS Database Migration Service (AWS DMS) replica dados entre os clusters na região local. No entanto, o AWS DMS atualmente não oferece suporte ao failover de tarefas entre regiões. Esse padrão inclui as etapas necessárias para contornar essa limitação e configurar de forma independente o AWS DMS em ambas as regiões.

Pré-requisitos e limitações

Pré-requisitos

- Regiões da AWS primárias e secundárias selecionadas que oferecem suporte aos bancos de dados globais Amazon Aurora.
- Dois clusters de banco de dados independentes da Amazon Aurora MySQL Edition em uma única conta na região principal.
- Classe de instância de banco de dados db.r5 ou superior (recomendado).
- Uma tarefa do AWS DMS na região principal executando a replicação contínua entre os clusters de banco de dados existentes.
- Recursos da região de DR disponíveis para atender aos requisitos de criação de instâncias de banco de dados. Para obter mais informações, consulte Trabalhar com uma instância de banco de dados em uma VPC.

Limitações

- Para ver a lista completa das limitações do banco de dados global Amazon Aurora, consulte Limitações dos bancos de dados globais Amazon Aurora.

Versões do produto

- Amazon Aurora Edição 5.7 ou 8.0 Compatível com MySQL. Para obter mais informações, consulte Versões do Amazon Aurora.

Arquitetura

Pilha de tecnologias de destino

- Cluster do banco de dados global Amazon Aurora edição compatível com MySQL
- AWS DMS

Arquitetura de destino

O diagrama a seguir mostra um banco de dados global para duas regiões da AWS, uma com os bancos de dados principal e de relatórios e a replicação do AWS DMS, e outra com os bancos de dados secundários principais e relatores.

Automação e escala

Você pode usar CloudFormation a AWS para criar a infraestrutura pré-requisito na região secundária, como a nuvem privada virtual (VPC), sub-redes e grupos de parâmetros. Você também pode usar CloudFormation a AWS para criar clusters secundários na região de DR e adicioná-los ao banco de dados global. Se você usou CloudFormation modelos para criar os clusters de banco de dados na região primária, poderá atualizá-los ou aumentá-los com um modelo adicional para criar o recurso de banco de dados global. Para obter mais informações, consulte Criação de um cluster de banco de dados Amazon Aurora com duas instâncias de banco de dados e Criação de um cluster de banco de dados global para o Aurora MySQL.

Por fim, você pode criar as tarefas do AWS DMS nas regiões primária e secundária usando CloudFormation após a ocorrência de eventos de failover e failback. Para obter mais informações, consulte AWS::DMS::ReplicationTask.

Ferramentas

- O Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado que é compatível com MySQL e PostgreSQL. Esse padrão usa Amazon Aurora Edição compatível com MySQL.
- Os bancos de dados globais do Amazon Aurora são projetados para aplicativos distribuídos globalmente. Um único banco de dados global Amazon Aurora pode abranger várias regiões da AWS. Ele replica seus dados sem afetar o desempenho do banco de dados. Ele também permite leituras locais rápidas com baixa latência em cada região e fornece recuperação de desastres de interrupções em toda a região.
- O AWS DMS fornece migração única ou replicação contínua. Uma tarefa de replicação contínua mantém seus bancos de dados de origem e destino sincronizados. Depois de configurada, a tarefa de replicação contínua aplica continuamente as alterações de origem ao destino com latência mínima. Todos os recursos do AWS DMS, como validação e transformações de dados, estão disponíveis para qualquer tarefa de replicação.

Épicos

Preparar os clusters de banco de dados existentes na região primária

Tarefa	Descrição	Habilidades necessárias
Modifique o grupo de parâmetros do cluster de banco de dados.	No grupo de parâmetro s do cluster de banco de dados existente, ative o registro binário em nível de linha definindo o parâmetro `binlog_format` como um valor de linha. O AWS DMS exige registro binário em nível de linha para bancos de dados compatíve is com MySQL ao realizar replicação contínua ou captura de dados de alteração (CDC). Para obter mais informações,	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	consulte Como usar um banco de dados compatível com o MySQL gerenciado pela AWS como fonte para o AWS DMS.	

Tarefa	Descrição	Habilidades necessárias

Atualize o período de retenção do log binário do banco de dados.	Usando um cliente MySQL instalado em seu dispositivo de usuário final ou uma instância do Amazon Elastic Compute Cloud (EC2Amazon), execute o seguinte procedimento armazenado fornecido pelo Amazon Relational Database Service (Amazon RDS) no nó gravador do cluster de banco de dados principalXX, onde é o número de horas para reter os registros.
	`call mysql.rds_set_configuration('binlog retention hours', XX)`
	Confirme a configuração executando o seguinte comando.
	`call mysql.rds_show_configuration;`
	Bancos de dados compatíveis com MySQL gerenciados pela AWS eliminam os logs binários o mais rápido possível. Portanto, o período de retenção deve ser longo o suficiente para garantir que os logs não sejam eliminados antes que a tarefa do AWS
		DBA

Tarefa	Descrição	Habilidades necessárias
	DMS seja executada. Um valor de 24 horas geralment e é suficiente, mas o valor deve ser baseado no tempo necessário para configurar a tarefa do AWS DMS na região de DR.	

Atualize a tarefa existente do AWS DMS na região principal

Tarefa	Descrição	Habilidades necessárias

Registre o ARN da tarefa do AWS DMS.	Use o nome do recurso da Amazon (ARN) para obter o nome da tarefa do AWS DMS para uso posterior. Para recuperar o ARN da tarefa do AWS DMS, visualize a tarefa no console ou execute o comando a seguir.
	`aws dms describe-replication-tasks`
	Um ARN se parece com o seguinte.
	`arn:aws:dms:us-east-1:<accountid>:task:AN6HFFMPM246XOZVEUHCNSOVF7MQCLTOZUIRAMY`
	Os caracteres após os dois últimos pontos correspondem
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	ao nome da tarefa usado em uma etapa posterior.	
Modifique a tarefa existente do AWS DMS para registrar o ponto de verificação.	O AWS DMS cria pontos de verificação que contêm informações para que o mecanismo de replicação conheça o ponto de recuperação para o fluxo de alterações. Para registrar as informações do ponto de verificação, execute as seguintes etapas no console: 1. Interrompa a tarefa do AWS DMS. 2. Use o editor JSON na tarefa para definir o TaskRecoveryTableEnabled parâmetro como verdadeiro. 3. Inicie a tarefax do AWS DMS.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Valide as informações do ponto de verificação.	Usando um cliente MySQL conectado ao endpoint do gravador do cluster, consulte a nova tabela de metadados no cluster do banco de dados do relator para verificar se ela existe e contém as informaçõ es do estado de replicação. Execute o seguinte comando: `select * from awsdms_co ntrol.awsdms_txn_s tate;` O nome da tarefa do ARN deve ser encontrado nessa tabela na coluna `Task_Name` .	DBA

Expanda os dois clusters do Amazon Aurora para uma região de DR

Tarefa	Descrição	Habilidades necessárias
Crie uma infraestrutura básica na região de DR.	Crie os componentes básicos necessários para a criação e o acesso aos clusters do Amazon Aurora: • Nuvem privada virtual (VPC) • Sub-redes • Grupo de segurança • Listas de controle de acesso à rede • Grupo de sub-redes	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	• DB parameter group (grupo de parâmetros de banco de dados) • Grupo de parâmetros do cluster de banco de dados Certifique-se de que a configuração de ambos os grupos de parâmetros corresponda à configuração na região primária.	
Adicione a região de DR aos dois clusters do Amazon Aurora.	Adicione uma região secundária (a região de DR) aos clusters principal e relator do Amazon Aurora. Para obter mais informações, consulte Adicionar uma região da AWS a um banco de dados global do Amazon Aurora.	Administrador da AWS

Execute o failover

Tarefa	Descrição	Habilidades necessárias
Interrompa a tarefa do AWS DMS.	A tarefa do AWS DMS na região principal não funcionará adequadamente após a ocorrência do failover e deverá ser interrompida para evitar erros.	Administrador da AWS
Execute um failover gerenciado.	Execute um failover gerenciado do cluster de banco de	Administrador da AWS, DBA

Tarefa	Descrição	Habilidades necessárias
	dados principal para a região de DR. Para ver as instruções, consulte Failover planejado gerenciado para Amazon Aurora Global Databases. Após a conclusão do failover no cluster de banco de dados principal, execute a mesma atividade no cluster de banco de dados do relator.	
Carregue dados no banco de dados principal.	Insira dados de teste no nó gravador do banco de dados principal no cluster de banco de dados DR. Esses dados serão usados para validar se a replicação está funcionando adequadamente.	DBA
Crie a instância de replicação do AWS DMS.	Para criar a instância de replicação do AWS DMS na região de DR, consulte Criação de uma instância de replicação.	Administrador da AWS, DBA

Tarefa	Descrição	Habilidades necessárias
Criação de endpoints do AWS DMS de origem e de destino.	Para criar os endpoints de origem e destino do AWS DMS na região de DR, consulte Criação de endpoints de origem e destino. A origem deve apontar para a instância do gravador do cluster de banco de dados principal. O destino deve apontar para a instância do gravador do cluster de banco de dados do relator.	Administrador da AWS, DBA
Obtenha o ponto de verificação de replicação.	Para obter o ponto de verificação de replicação, use um cliente MySQL para consultar a tabela de metadados executando o seguinte no nó gravador no cluster de banco de dados repórter na região DR. `select * from awsdms_control.awsdms_txn_state;` Na tabela, encontre o valor task_name que corresponde ao ARN da tarefa do AWS DMS que existe na região principal que você obteve no segundo épico.	DBA

Tarefa	Descrição	Habilidades necessárias
Crie uma tarefa do AWS DMS.	Usando o console, crie uma tarefa do AWS DMS na região DR. Na tarefa, especifique um método de migração de Replicar somente alterações de dados. Para obter mais informações, consulte Criar uma tarefa. 1. Nas configurações da tarefa, use o assistente para especificar o seguinte: • Modo de início CDC para transações de origem: ative o modo de início CDC personalizado • Ponto inicial personalizado do CDC para transações de origem: especifique um ponto de verificação de recuperação 2. Na caixa Ponto de verificação de recuperação, insira o valor do ponto de verificação de replicação obtido anteriormente por meio da consulta ao banco de dados na tabela `awsdms_txn_state` . 3. Na seção de configurações da tarefa, selecione o editor JSON e defina o TaskRecoveryTableE	Administrador da AWS, DBA

Tarefa	Descrição	Habilidades necessárias
	nabledparâmetro como verdadeiro. Defina a configuração da tarefa do AWS DMS Iniciar a tarefa de migração como Automaticamente ao criar.	
Registre o ARN da tarefa do AWS DMS.	Use o ARN para obter o nome da tarefa do AWS DMS para uso posterior. Para recuperar o ARN da tarefa do AWS DMS, execute o comando a seguir. `aws dms describe-replication-tasks`	Administrador da AWS, DBA
Valide os dados replicados.	Consulte o cluster de banco de dados do relator na região de DR para confirmar se os dados de teste que você carregou no cluster de banco de dados principal foram replicados.	DBA

Execute o failback

Tarefa	Descrição	Habilidades necessárias
Interrompa a tarefa do AWS DMS.	A tarefa do AWS DMS na região DR não funcionar á adequadamente após a ocorrência do failback e	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	deverá ser interrompida para evitar erros.	
Execute um failback gerenciado.	Faça o failback do cluster de banco de dados principal para a região primária. Para ver as instruções, consulte Failover planejado gerenciado para Amazon Aurora Global Databases. Após a conclusão do failback no cluster de banco de dados principal, execute a mesma atividade no cluster de banco de dados do relator.	Administrador da AWS, DBA
Obtenha o ponto de verificação de replicação.	Para obter o ponto de verificação de replicação, use um cliente MySQL para consultar a tabela de metadados executando o seguinte no nó gravador no cluster de banco de dados repórter na região DR. `select * from awsdms_control.awsdms_txn_state;` Na tabela, encontre o valor `task_name` que corresponde ao ARN da tarefa do AWS DMS que existe na região de DR que você obteve no quarto épico.	DBA

Tarefa	Descrição	Habilidades necessárias
Atualização de endpoints do AWS DMS de origem e de destino.	Depois que os clusters do banco de dados falharem, verifique os clusters na região primária para determinar quais nós são as instância s do gravador. Em seguida, verifique se os endpoints existentes de origem e destino do AWS DMS na região primária estão apontando para as instâncias do gravador. Caso contrário, atualize os endpoints com os nomes do Sistema de Nomes de Domínio (DNS) da instância do gravador.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Crie uma tarefa do AWS DMS.	Usando o console, crie uma tarefa do AWS DMS na região primária. Na tarefa, especifiq ue um método de migração de Replicar somente alteraçõe s de dados. Para obter mais informações, consulte Criar uma tarefa. 1. Nas configurações da tarefa, use o assistente e especifique o seguinte: • Modo de início CDC para transações de origem: ative o modo de início CDC personalizado • Ponto inicial personali zado do CDC para transações de origem: especifique um ponto de verificação de recuperaç ão 2. Na caixa Ponto de verificaç ão de recuperação, insira o valor do ponto de verificaç ão de replicação obtido anteriormente por meio da consulta ao banco de dados na tabela `awsdms_tx n_state` . 3. Também na seção de configurações da tarefa, selecione o editor JSON e defina o TaskRecov	Administrador da AWS, DBA

Tarefa	Descrição	Habilidades necessárias
	eryTableEnabledparâmetro como verdadeiro. 4. Por fim, defina a configura ção da tarefa do AWS DMS Iniciar a tarefa de migração como Automaticamente ao criar.	
Registre o nome do recurso da Amazon (ARN) da tarefa do AWS DMS.	Use o ARN para obter o nome da tarefa do AWS DMS para uso posterior. Para recuperar o ARN da tarefa do AWS DMS, execute o comando a seguir: `aws dms describe-replication-tasks` O nome da tarefa será necessário ao realizar outro failover gerenciado ou durante um cenário de DR.	Administrador da AWS, DBA
Exclua as tarefas do AWS DMS.	Exclua a tarefa original (atualmente interrompida) do AWS DMS na região principal e a tarefa existente do AWS DMS (atualmente interromp ida) na região secundária.	Administrador da AWS

Recursos relacionados

- Configuração do cluster de banco de dados do Amazon Aurora
- Usar bancos de dados globais do Amazon Aurora

- Como trabalhar com o Amazon Aurora MySQL
- Trabalhando com instância de replicação do AWS DMS
- Trabalhando com endpoints do AWS DMS
- Trabalhando com tarefas do AWS DMS
- O que é a AWS CloudFormation?

Mais informações

Os bancos de dados globais Amazon Aurora são usados neste exemplo para DR porque fornecem um objetivo de tempo de recuperação (RTO) efetivo de 1 segundo e um objetivo de ponto de recuperação (RPO) de menos de 1 minuto, ambos inferiores às soluções replicadas tradicionais e ideais para cenários de DR.

Os bancos de dados globais Amazon Aurora oferecem muitas outras vantagens, incluindo as seguintes:

- Leituras globais com latência local: consumidores globais podem acessar informações em uma região local, com latência local.
- Clusters de banco de dados secundários escaláveis do Amazon Aurora: os clusters secundários podem ser escalados de forma independente, adicionando até 16 réplicas somente para leitura.
- Replicação rápida de clusters de banco de dados do Amazon Aurora primários para secundários: a replicação tem pouco impacto na performance no cluster primário. Isso ocorre na camada de armazenamento, com latências de replicação entre regiões típicas de menos de 1 segundo.

Esse padrão também usa o AWS DMS para replicação. Os bancos de dados Amazon Aurora oferecem a capacidade de criar réplicas de leitura, o que pode simplificar o processo de replicação e a configuração de DR. No entanto, o AWS DMS geralmente é usado para replicar quando são necessárias transformações de dados ou quando o banco de dados de destino exige índices adicionais que o banco de dados de origem não tem.

Migre funções e procedimentos do Oracle que tenham mais de 100 argumentos para o PostgreSQL

Criado por Srinivas Potlachervoo (AWS)

Resumo

Este padrão mostra como migrar funções e procedimentos do Oracle que tenham mais de 100 argumentos para o PostgreSQL. Por exemplo, você pode usar esse padrão para migrar funções e procedimentos Oracle para um dos seguintes serviços de banco de dados da AWS compatíveis com PostgreSQL:

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL
- Amazon Aurora Edição Compatível com PostgreSQL

O PostgreSQL não suporta funções ou procedimentos que tenham mais de 100 argumentos. Como solução alternativa, você pode definir um novo tipo de dados que tenha campos de tipo que correspondam aos argumentos da função de origem. Em seguida, você pode criar e executar uma função PL/pgSQL que usa o tipo de dados personalizado como argumento.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância de banco de dados Oracle do Amazon RDS
- Uma instância de banco de dados Amazon RDS para PostgreSQL ou uma instância de banco de dados Aurora compatível com PostgreSQL

Versões do produto

- Instância de banco de dados Oracle do Amazon RDS, versões 10.2 e posteriores
- Instância de banco de dados PostgreSQL do Amazon RDS, versões 9.4 e posteriores, ou instâncias de banco de dados compatíveis com o Aurora PostgreSQL, versões 9.4 e posteriores
- Oracle SQL Developer versão 18 e posteriores
- pgAdmin versão 4 e posterior

Arquitetura

Pilha de tecnologia de origem

- Instância de banco de dados Oracle do Amazon RDS, versões 10.2 e posteriores

Pilha de tecnologias de destino

- Instância de banco de dados PostgreSQL do Amazon RDS, versões 9.4 e posteriores, ou instâncias de banco de dados compatíveis com o Aurora PostgreSQL, versões 9.4 e posteriores

Ferramentas

Serviços da AWS

- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.
- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.

Outros serviços

- O Oracle SQL Developer é um ambiente de desenvolvimento integrado que simplifica o desenvolvimento e o gerenciamento de bancos de dados Oracle em implantações tradicionais e baseadas em nuvem.
- O pgAdmin é uma ferramenta de gerenciamento de software livre para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.

Práticas recomendadas

Certifique-se de que o tipo de dados criado corresponda aos campos de tipo incluídos na função ou procedimento de origem do Oracle.

Épicos

Execute uma função ou procedimento Oracle que tenha mais de 100 argumentos

Tarefa	Descrição	Habilidades necessárias
Crie ou identifique uma função ou procedimento existente do Oracle/PLSQL que tenha mais de 100 argumentos.	Crie uma função ou procedimento Oracle/PLSQL que tenha mais de 100 argumentos. - ou - Identifique uma função ou procedimento existente do Oracle/PLSQL que tenha mais de 100 argumentos. Para obter mais informações, consulte as seções 14.7 Instrução CREATE FUNCTION e 14.11 CREATE PROCEDURE na documentação do Oracle Database.	Conhecimento em Oracle/PLSQL
Compile a função ou o procedimento Oracle/PLSQL.	Compile a função ou o procedimento Oracle/PLSQL. Para ter mais informações, consulte Compilar uma função na documentação do Oracle Database.	Conhecimento em Oracle/PLSQL
Execute a função Oracle/PLSQL.	Execute a função ou o procedimento Oracle/PLSQL. Em seguida, salve a saída.	Conhecimento em Oracle/PLSQL

Defina um novo tipo de dados que corresponda aos argumentos da função de origem ou do procedimento

Tarefa	Descrição	Habilidades necessárias
Defina um novo tipo de dados no PostgreSQL.	Defina um novo tipo de dados no PostgreSQL que inclua todos os mesmos campos que aparecem nos argumentos da função ou do procedimento Oracle de origem. Para ter mais informações, consulte CREATE TYPE na documentação do PostgreSQL.	Conhecimento sobre PostgreSQL PL/pgSQL

Crie uma função PostgreSQL que inclua o novo argumento TYPE

Tarefa	Descrição	Habilidades necessárias
Crie uma função do PostgreSQL que inclua o novo tipo de dados.	Crie uma função do PostgreSQL que inclua o novo argumento `TYPE`. Para analisar um exemplo de função, consulte a seção Informações adicionais desse padrão.	Conhecimento sobre PostgreSQL PL/pgSQL
Compile a função PostgreSQL.	Compile a função no PostgreSQL. Se os novos campos de tipo de dados corresponderem aos argumentos da função de origem ou do procedimento,	Conhecimento sobre PostgreSQL PL/pgSQL

Tarefa	Descrição	Habilidades necessárias
	a função será compilada com êxito.	
Execute a função PostgreSQL.	Execute a função PostgreSQL.	Conhecimento sobre PostgreSQL PL/pgSQL

Solução de problemas

Problema	Solução
A função retorna o seguinte erro: ERRO: erro de sintaxe próximo a “<statement>”	Certifique-se de que todas as declarações da função terminem com ponto e vírgula (`;`).
A função retorna o seguinte erro: ERRO: “<variable>” não é uma variável conhecida	Certifique-se de que a variável usada no corpo da função esteja listada na seção `DECLARE` da função.

Recursos relacionados

- Trabalho com o Amazon Aurora PostgreSQL (Guia do usuário do Amazon Aurora para Aurora)
- CREATE TYPE (documentação do PostgreSQL)

Mais informações

Exemplo de função PostgreSQL que inclui um argumento TYPE

```
CREATE OR REPLACE FUNCTION test_proc_new
(
    IN p_rec type_test_proc_args
)
RETURNS void
AS
$BODY$
```

```
BEGIN

    /*
    **************
    The body would contain code to process the input values.
    For our testing, we will display couple of values.
    ***************
    */
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_acct_id: ', p_rec.p_acct_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_id: ', p_rec.p_ord_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_date: ', p_rec.p_ord_date);

END;
$BODY$
LANGUAGE plpgsql
COST 100;
```

Migre instâncias do banco de dados Amazon RDS para Oracle para outras contas que usam AMS

Criado por Pinesh Singal (AWS)

Resumo

Este padrão mostra como migrar uma instância do banco de dados Amazon Relational Database Service (Amazon RDS) para Oracle de uma conta da AWS para outra conta da AWS. O padrão se aplica a cenários em que a conta de origem da AWS não usa o AWS Managed Services (AMS), mas a conta de destino, sim. Você pode concluir a migração usando uma solicitação de alteração (RFC) na AMS em vez de usar o Console de Gerenciamento da AWS para realizar operações de banco de dados. Essa abordagem assegura tempo de inatividade mínimo para um banco de dados de origem Oracle de vários terabytes com um grande número de transações. Por exemplo, o tempo de inatividade de um banco de dados de 400 a 900 GB pode durar aproximadamente duas ou três horas. O tempo de migração do banco de dados é diretamente proporcional ao tamanho da instância do banco de dados Amazon RDS para Oracle.

> **Important**
>
> Esse padrão exige que você faça um snapshot do banco de dados da instância de banco de dados Amazon RDS for Oracle em uma conta de origem, copie o snapshot para uma conta de destino que esteja usando o AMS e, em seguida, crie uma nova instância de banco de dados a partir desse snapshot levantando. RFCs

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da AWS para a conta de origem
- Uma conta ativa da AWS que usa a AMS para a conta de destino
- Instância de banco de dados do Amazon RDS para Oracle, em funcionamento

Limitações

- As mesmas propriedades ou configurações das instâncias do banco de dados na conta de origem são copiadas para uma nova instância do banco de dados de destino na AMS.

- O método RFC usado nessa abordagem de migração tem recursos limitados para oferecer suporte ao Amazon RDS para Oracle. Você pode acessar todos os recursos do Amazon RDS for Oracle usando um modelo da CloudFormation AWS para realizar a migração do banco de dados.
- Poderá ocorrer uma interrupção do aplicativo por várias horas porque a migração deve ser concluída durante o tempo de inatividade programado. Durante o tempo de inatividade, você interrompe a instância do banco de dados na conta de origem e, em seguida, acessa uma nova instância do banco de dados na conta de destino.
- Essa abordagem de migração não se aplica à migração de uma instância do banco de dados de uma região da AWS para outra região dentro da mesma conta da AWS.

Versões do produto

- Instância Oracle Database Standard Edition 2 (SE2) 12.1.0.2.v2 e posterior no Amazon RDS for Oracle
- O Amazon RDS para Oracle 11g não é mais compatível (para obter mais informações, consulte Amazon RDS para Oracle na documentação do Amazon RDS.)

Arquitetura

Pilha de tecnologia de origem

- Instância do Oracle Database SE2 12.1.0.2.v2 no Amazon RDS for Oracle
- Grupo de sub-rede do Amazon RDS
- Grupo de opções do Amazon RDS (se necessário)
- Grupo de parâmetros do Amazon RDS (se necessário)
- Grupo de segurança da Amazon Virtual Private Cloud (Amazon VPC)
- AWS Key Management Service (AWS KMS) com chaves gerenciadas pela AWS ou chaves gerenciadas pelo cliente
- Perfil do AWS Identity and Access Management (IAM) (se necessário)

Pilha de tecnologias de destino

- Instância do Oracle Database SE2 12.1.0.2.v2 no Amazon RDS for Oracle
- Grupo de sub-rede do Amazon RDS
- Grupo de opções do Amazon RDS (se necessário)

- Grupo de parâmetros do Amazon RDS (se necessário)
- Grupo de segurança da Amazon VPC
- AWS Managed Services (AMS)
- AWS KMS com chaves gerenciadas pela AWS e chaves gerenciadas pelo cliente
- Perfil do IAM (se necessário)

Arquitetura de migração de origem e de destino

O diagrama a seguir mostra a migração de uma instância do banco de dados Amazon RDS para Oracle em uma conta da AWS para uma instância do banco de dados Amazon RDS para Oracle em outra conta da AWS que usa AMS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Faça um snapshot da instância do banco de dados do Amazon RDS para Oracle na conta de origem.
2. Copie o snapshot para a AMS na conta de destino.
3. Crie uma nova instância do banco de dados Amazon RDS para Oracle a partir do snapshot na conta de destino.

Automação e escala

Você pode automatizar e escalar a migração usando CloudFormation modelos e criando RFCs no AMS. CloudFormation permite que você use todos os recursos do Amazon RDS for Oracle, incluindo a capacidade de configurar e restaurar a instância de banco de dados ao criar uma instância de banco de dados Amazon RDS for Oracle a partir de um snapshot.

Ferramentas

- O Amazon Relational Database Service (Amazon RDS) para Oracle ajuda você a configurar, operar e escalar um banco de dados relacional Oracle na Nuvem AWS.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O AWS Managed Services (AMS) ajuda você a operar sua infraestrutura da AWS com mais eficiência e segurança.

Épicos

Prepare-se para a substituição na conta de destino

Tarefa	Descrição	Habilidades necessárias
Como criar uma chave do AWS KMS.	1. Crie uma RFC automatizada, chamada Criar chave KMS, para criar uma chave KMS personalizada a partir da sua conta de destino. 2. **Note** Compartilhe sua chave KMS personalizada com a conta de origem. : Você não pode compartilhar instâncias de banco de dados Amazon RDS for Oracle que usam a chave gerenciada padrão da AWS para Amazon RDS (). `aws/rds` Em vez disso, compartilhe a instância do banco de dados criptografando-a novamente a partir da sua chave KMS.	AWS, AMS
Crie um grupo de segurança.	Crie uma RFC automatizada chamada Criar grupo de	AWS, AMS

Tarefa	Descrição	Habilidades necessárias
	segurança para criar um grupo de segurança para sua VPC a partir da sua conta de destino. Certifique-se de especificar o seguinte: • Novo nome do grupo de segurança • Regras de entrada e saída TCP e UDP • Tags padrão	

Tarefa	Descrição	Habilidades necessárias
(Opcional) Revise seus recursos do Amazon RDS.	Os seguintes recursos são criados quando uma instância do banco de dados Amazon RDS para Oracle é criada: • Grupo de sub-redes do Amazon RDS (com base no ID da sub-rede) • Grupo de opções do Amazon RDS (com base no snapshot da instância do banco de dados de origem) • Grupo de parâmetros do Amazon RDS (com base no snapshot da instância do banco de dados) Se você quiser analisar os recursos do Amazon RDS que foram criados com sua instância do banco de dados, pode se conectar à sua instância do banco de dados Oracle e encontrar seu grupo de sub-redes, grupo de opções e grupo de parâmetros no console do Amazon RDS.	AWS

Substituir a conta de origem

Tarefa	Descrição	Habilidades necessárias
Interromper o aplicativo.	Interrompa o aplicativo e seus serviços dependentes.	Proprietário do App

Tarefa	Descrição	Habilidades necessárias
	Você deve interromper todo o tráfego para o banco de dados na conta de origem.	
Tire um snapshot do manual.	Crie manualmente um snapshot do banco de dados da instância do banco de dados Amazon RDS para Oracle na conta de origem.	AWS
Interrompa a instância de banco de dados.	Interrompa a instância do banco de dados Amazon RDS para Oracle.	AWS
Copie o snapshot.	Copie o snapshot do banco de dados para a mesma conta de origem e, em seguida, use a chave KMS personalizada compartilhada da conta de destino para criptografar novamente o arquivo copiado do snapshot do banco de dados.	AWS
Compartilhar o snapshot.	Compartilhe o novo snapshot (copiado com a chave KMS personalizada) com a conta de destino.	AWS

Substituir a conta de origem

Tarefa	Descrição	Habilidades necessárias
Copie o snapshot.	Crie uma RFC automatizada chamada Copiar snapshot do	AWS, AMS

Tarefa	Descrição	Habilidades necessárias
	RDS para copiar o snapshot do banco de dados para a mesma conta de destino e use a chave KMS padrão gerenciada pela AWS criada para recriptografia. Isso é necessário para tornar a conta de destino proprietária do novo snapshot e permitir que a instância do banco de dados Amazon RDS para Oracle criada a partir do snapshot seja associada ao grupo de opções, se necessári o.	
Crie uma instância do banco de dados a partir do snapshot.	Crie uma RFC automatiz ada chamada Criar banco de dados do snapshot para criar uma instância do banco de dados Amazon RDS para Oracle a partir do snapshot. Certifique-se de especificar o seguinte: • Novo ID do snapshot criado na etapa anterior • ID da VPC • ID da sub-rede • ID da instância de banco de dados do RDS • Tags padrão	AWS, AMS

Tarefa	Descrição	Habilidades necessárias
Anexe a instância ao grupo de segurança e faça atualizações de configuração.	1. Crie uma RFC manual chamada Atualizar outro para anexar a instância do banco de dados Amazon RDS para Oracle que você criou anteriormente com o grupo de segurança da VPC. 2. Faça quaisquer alterações adicionais na configuração da instância do banco de dados Amazon RDS para Oracle.	AWS, AMS

Tarefa	Descrição	Habilidades necessárias
Teste a instância de banco de dados.	Teste a nova conectividade do endpoint da instância do banco de dados Amazon RDS para Oracle fazendo login em qualquer instância ou servidor de aplicativos hospedado no mesmo grupo de segurança e usando telnet para se conectar à porta 1521. Para obter mais informaçõ es, consulte Conectar a uma instância de banco de dados do Amazon RDS na documentação do Amazon RDS. **Note** Se as credenciais de login do usuário principal estiverem disponíveis, você poderá testar a instância de banco de dados Amazon RDS for Oracle fazendo login em qualquer cliente SQL (como o Oracle SQL Developer).	AWS, DBA

Recursos relacionados

- AWS Managed Services (documentação da AWS)

- Como RFCs trabalhar (documentação do AWS Managed Services)
- Compartilhamento de snapshots criptografados (Guia do usuário do Amazon RDS)
- Como posso compartilhar um snapshot criptografado do banco de dados do Amazon RDS com outra conta? (Centro de Conhecimentos da AWS)
- O que é o Amazon Relational Database Service (Amazon RDS)? (Guia do usuário do Amazon RDS)
- Amazon RDS para Oracle (Guia do usuário do Amazon RDS)
- Uso dos consoles da AMS (documentação do AWS Managed Services)

Mais informações

Para reverter a migração

Se desejar reverter a migração, conclua as seguintes etapas:

1. Crie uma RFC manual (Atualizar outro) a partir da conta de destino para excluir a pilha do banco de dados criada na própria conta de destino.
2. Atualize a configuração do aplicativo para apontar para a instância do banco de dados Amazon RDS para Oracle na conta de origem.
3. Inicie a instância do banco de dados Amazon RDS para Oracle na conta de origem.

Migrar variáveis de ligação Oracle OUT para um banco de dados PostgreSQL

Criado por Bikash Chandra Rout (AWS) e Vinay Paladi (AWS)

Resumo

Esse padrão mostra como migrar variáveis de ligação do Oracle Database 0UT para qualquer um dos seguintes serviços de banco de dados da AWS compatíveis com PostgreSQL:

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL
- Amazon Aurora Edição Compatível com PostgreSQL

O PostgreSQL não é compatível com variáveis de ligação 0UT. Para obter a mesma funcionalidade em suas instruções do Python, você pode criar uma função PL/pgSQL personalizada que usa as variáveis do pacote `GET` e `SET` em vez disso. Para aplicar essas variáveis, o exemplo de script de função wrapper fornecido nesse padrão usa um pacote de extensão da AWS Schema Conversion Tool (AWS SCT).

> **Note**
>
> Se a `EXECUTE IMMEDIATE` instrução Oracle for uma `SELECT` instrução que possa retornar uma linha no máximo, é uma prática recomendada fazer o seguinte:

- Coloque variáveis de ligação `0UT` (define) na cláusula `INT0`
- Coloque variáveis de ligação `IN` na cláusula `USING`

Para obter mais informações, consulte a instrução EXECUTE IMMEDIATE na documentação da Oracle.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem do Oracle Database 10g (ou mais recente) em um datacenter on-premises

- Uma instância de banco de dados Amazon RDS para PostgreSQL ou uma instância de banco de dados Aurora compatível com PostgreSQL

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Oracle Database 10g (ou mais recente) on-premises

Pilha de tecnologias de destino

- Uma instância de banco de dados Amazon RDS para PostgreSQL ou uma instância de banco de dados Aurora compatível com PostgreSQL

Arquitetura de destino

O diagrama a seguir mostra um exemplo de fluxo de trabalho para migrar variáveis de 0UT vinculação do banco de dados Oracle para um banco de dados AWS compatível com PostgreSQL.

O diagrama mostra o seguinte fluxo de trabalho:

1. O AWS SCT converte o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino AWS compatível com PostgreSQL.
2. Qualquer objeto de banco de dados que não possa ser convertido automaticamente é sinalizado pela função PL/pgSQL. Os objetos marcados são então convertidos manualmente para concluir a migração.

Ferramentas

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID, que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.
- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.

- O AWS Schema Conversion Tool (AWS SCT) é compatível com as migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maioria do código personalizado em um formato compatível com o banco de dados de destino.
- O pgAdmin é uma ferramenta de gerenciamento de software livre para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.

Épicos

Migre variáveis de ligação Oracle OUT usando uma função PL/pgSQL personalizada e o AWS SCT

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao seu banco de dados AWS compatível com PostgreSQL.	Depois que você criou uma instância de banco de dados, pode usar qualquer aplicativo cliente SQL padrão para se conectar à um banco de dados no seu cluster de banco de dados. Por exemplo, você pode usar o pgAgmin para se conectar à sua instância de banco de dados. Para obter mais informações, consulte os procedimentos a seguir: • Conectando-se a uma instância de banco de dados Amazon RDS no Guia do usuário do Amazon RDS • Conectando-se a um cluster de banco de dados Amazon Aurora no Guia do usuário do Amazon Aurora	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Adicione o exemplo de script de função wrapper desse padrão ao esquema principal do banco de dados de destino.	Copie o exemplo do script da função wrapper PL/pgSQL da seção Informações adicionais deste padrão. Em seguida, adicione a função ao esquema principal do banco de dados de destino. Para obter mais informações, consulte CREATE FUNCTION na documentação do PostgreSQL.	Engenheiro de migração
(Opcional) Atualize o caminho de pesquisa no esquema principal do banco de dados de destino para que ele inclua o esquema Test_PG.	Para melhorar o desempenho, você pode atualizar a variável search_path do PostgreSQL para que ela inclua o nome do esquema Test_pg. Se você incluir o nome do esquema no caminho de pesquisa, não precisará especificar o nome sempre que chamar a função PL/pgSQL. Para obter mais informações, consulte a seção 5.9.3 O caminho de pesquisa do esquema na documentação do PostgreSQL.	Engenheiro de migração

Recursos relacionados

- AWS Schema Conversion Tool
- Variáveis de ligação OUT (documentação da Oracle)

- Melhore o desempenho da consulta SQL usando variáveis de ligação (Oracle Blog)

Mais informações

Exemplo de função PL/pgSQL

```
/* Oracle */

CREATE or replace PROCEDURE test_pg.calc_stats_new1 (
                                                      a NUMBER,
                                                      b NUMBER,
                                                      result out NUMBER
                                                    )

IS
BEGIN
result:=a+b;
END;
/
/* Testing */
set serveroutput on
DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN test_pg.calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;  -- calc_stats(a, a, b, a)
  DBMS_OUTPUT.PUT_LINE('output:'||output);
END;

output:11


PL/SQL procedure successfully completed.

--Postgres--

/* Example : 1 */
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new1(
                                                        w integer,
                                                        x integer
```

```
                                                    )
RETURNS integer
AS
$BODY$
begin
      return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION aws_oracle_ext.set_package_variable(
                                                                  package_name name,
                                                                  variable_name name,
                                                                  variable_value
 anyelement
                                                                )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
begin
    perform set_config
      ( format( '%s.%s',package_name, variable_name )
      , variable_value::text
      , false );
  end;
$BODY$;

CREATE OR REPLACE FUNCTION aws_oracle_ext.get_package_variable_record(
                                                                    package_name
 name,
                                                                    record_name name
                                                                  )
RETURNS text
LANGUAGE 'plpgsql'
    COST 100
    VOLATILE
AS $BODY$
begin
    execute 'select ' || package_name || '$Init()';
```

```
    return aws_oracle_ext.get_package_variable
        (
         package_name := package_name
        , variable_name := record_name || '$REC' );
end;
$BODY$;

--init()--
CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized('test_pg' ) then
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;

/* callable for 1st Example */

DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$
```

```
/*In above Postgres example we have set the value of v_output using v_output_l in the
 dynamic anonymous block to mimic the
  behaviour of oracle out-bind variable .*/

--Postgres Example : 2 --
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new2(
 w integer,
 x integer,
inout status text,
 out result integer)
AS
$BODY$
DECLARE
begin
result :=  w + x ;
status := 'ok';
end;
$BODY$
LANGUAGE  plpgsql;

/* callable for 2nd Example */
DO $$
declare
v_sql text;
v_output_loc int;
v_staus text:= 'no';
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
execute 'do $a$ declare v_output_l int; v_status_l text; begin select * from
 test_pg.calc_stats_new2('||a||','||b||','''||v_staus||''') into v_status_l,v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_status'', v_status_l) ;
end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
v_staus := aws_oracle_ext.get_package_variable('test_pg', 'v_status');
raise notice 'v_output_loc %',v_output_loc;
raise notice 'v_staus %',v_staus;
END ;
$$
```

Migre o SAP HANA para a AWS usando o SAP HSR com o mesmo nome de host

Criado por Pradeep Puliyampatta (AWS)

Resumo

As migrações do SAP HANA para a Amazon Web Services (AWS) podem ser realizadas usando várias opções, incluindo backup e restauração, exportação e importação e replicação do sistema SAP HANA (HSR). A seleção de uma opção específica depende da conectividade de rede entre os bancos de dados SAP HANA de origem e de destino, do tamanho do banco de dados de origem, das considerações sobre o tempo de inatividade e de outros fatores.

A opção SAP HSR para migrar workloads do SAP HANA para a AWS funciona bem quando há uma rede estável entre os sistemas de origem e de destino e todo o banco de dados (snapshot de replicação do banco de dados SAP HANA) pode ser completamente replicado em 1 dia, conforme estipulado pela SAP para requisitos de throughput de rede para SAP HSR. Os requisitos de tempo de inatividade com essa abordagem são limitados à execução da aquisição no AWS ambiente de destino, ao backup do banco de dados SAP HANA e às tarefas de pós-migração.

O SAP HSR suporta o uso de nomes de host diferentes (nomes de host mapeados para endereços IP diferentes) para tráfego de replicação entre os sistemas primário ou de origem e secundário ou de destino. Você pode fazer isso definindo esses conjuntos específicos de nomes de host na seção `[system_replication_hostname_resolution]` em `global.ini`. Nesta seção, todos os hosts dos sites primário e secundário devem ser definidos em cada host. Para obter etapas detalhadas de configuração, consulte a documentação do SAP.

Uma das principais conclusões dessa configuração é que os nomes de host no sistema primário devem ser diferentes dos nomes de host no sistema secundário. Caso contrário, os seguintes erros podem ser observados.

- `"each site must have a unique set of logical hostnames"`
- `"remoteHost does not match with any host of the source site. All hosts of source and target site must be able to resolve all hostnames of both sites correctly"`

No entanto, o número de etapas pós-migração pode ser reduzido usando o mesmo nome de host do banco de dados SAP HANA no ambiente de destino. AWS

Esse padrão fornece uma solução alternativa para usar o mesmo nome de host nos ambientes de origem e destino ao usar a opção SAP HSR. Com esse padrão, você pode usar a opção SAP HANA Hostname Rename. Você atribui um nome de host temporário ao banco de dados SAP HANA de destino para facilitar a exclusividade do nome de host para o SAP HSR. Depois que a migração concluir a etapa de aquisição no ambiente SAP HANA de destino, você poderá reverter o nome do host do sistema de destino para o nome do host do sistema de origem.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Uma nuvem privada virtual (VPC) com um endpoint de rede privada virtual (VPN) ou um roteador.
- AWS Client VPN ou AWS Direct Connect configurado para transferir arquivos da origem para o destino.
- Bancos de dados SAP HANA no ambiente de origem e de destino. O nível de patch de destino do banco de dados SAP HANA deve ser igual ou superior ao nível do patch de origem do banco de dados SAP HANA, dentro da mesma edição da plataforma SAP HANA. Por exemplo, a replicação não pode ser configurada entre os sistemas HANA 1.0 e HANA 2.0. Para obter mais informações, consulte a pergunta 15 na nota do SAP nº 1999880 – Perguntas frequentes: replicação do sistema SAP HANA.
- Servidores de aplicativos SAP no ambiente de destino.
- Volumes do Amazon Elastic Block Store (Amazon EBS) no ambiente de destino.

Limitações

A lista de documentos SAP a seguir abrange problemas conhecidos relacionados a essa solução alternativa, incluindo restrições relacionadas à hierarquização dinâmica e às migrações escaláveis do SAP HANA:

- 2956397 – Falha na renomeação do sistema de banco de dados SAP HANA
- 2222694 – Ao tentar renomear o sistema HANA, aparece o seguinte erro “Os arquivos de origem não são de propriedade do usuário sidadm original (uid = xxxx)”
- 2607227 – hdblcm: register_rename_system: Falha ao renomear a instância do SAP HANA
- 2630562 – A renomeação do nome do host HANA falhou e o HANA não inicializa

- 2935639 – sr_register não está usando o nome do host especificado em system_replication_hostname_resolution na seção global.ini
- 2710211 – Erro: o sistema de origem e o sistema de destino têm nomes de host lógicos sobrepostos
- 2693441 – Falha ao renomear um sistema SAP HANA devido a um erro
- 2519672 – O HANA primário e o secundário têm sistemas diferentes (PKI, SSFS), dados e chaves, ou não é possível verificar
- 2457129 – A renomeação do host do sistema SAP HANA não é permitida quando a classificação dinâmica em camadas faz parte do cenário
- 2473002 – Usando a replicação do sistema HANA para migrar o sistema de aumento de escala (não há restrições fornecidas pela SAP ao usar essa abordagem de renomeação de nome de host para sistemas SAP HANA de aumento de escala). No entanto, o procedimento deve ser repetido em cada hospedeiro individual. Outras limitações de migração de aumento de escala também se aplicam a essa abordagem.)

Versões do produto

- Essa solução se aplica às edições 1.0 e 2.0 da plataforma SAP HANA DB.

Arquitetura

Configuração da origem

Um banco de dados SAP HANA é instalado no ambiente de origem. Todas as conexões do servidor de aplicativos SAP e interfaces de banco de dados usam o mesmo nome de host para conexões de clientes. O diagrama a seguir mostra o exemplo do nome do host de origem `hdbhost` e seu endereço IP correspondente.

Configuração do destino

O ambiente de Nuvem AWS destino usa o mesmo nome de host para executar um banco de dados SAP HANA. O ambiente de destino na AWS inclui o seguinte:

- Banco de dados SAP HANA
- Servidores de aplicativos SAP
- Volumes do EBS

Configuração intermediária

No diagrama a seguir, o nome do host no ambiente de AWS destino é temporariamente renomeado `temp-host` para que os nomes de host na origem e no destino sejam exclusivos. Depois que a migração concluir a etapa de aquisição no ambiente de destino, o nome do host virtual do sistema de destino será renomeado usando o nome original, `hdbhost`.

A configuração intermediária inclui uma das seguintes opções:

- AWS Client VPN com um endpoint Client VPN
- AWS Direct Connect conectando-se a um roteador

Os servidores de aplicativos SAP no ambiente de AWS destino podem ser instalados antes da configuração da replicação ou após a aquisição. No entanto, instalar os servidores de aplicativos antes da configuração da replicação pode ajudar na redução do tempo de inatividade durante a instalação, configuração de alta disponibilidade e backups.

Ferramentas

Serviços da AWS

- AWS Client VPNé um serviço VPN gerenciado baseado em cliente que permite acessar com segurança AWS recursos e recursos em sua rede local.
- AWS Direct Connectconecta sua rede interna a um AWS Direct Connect local por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para o público Serviços da AWS, ignorando os provedores de serviços de Internet em seu caminho de rede.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (EC2Amazon). Os volumes do EBS se comportam como dispositivos de bloco brutos e não formatados. É possível montar esses volumes como dispositivos em suas instâncias.

Outras ferramentas

- Servidores de aplicativos SAP: os servidores de aplicativos SAP fornecem aos programadores uma forma de expressar a lógica de negócios. O servidor de aplicativos SAP executa o processamento de dados com base na lógica de negócios. Os dados reais são armazenados em um banco de dados, que é um componente separado.
- SAP HANA cockpit e SAP HANA Studio: tanto o SAP HANA cockpit quanto o SAP HANA Studio fornecem uma interface administrativa para o banco de dados SAP HANA. No SAP HANA Studio, o console de administração do SAP HANA é a visualização do sistema que fornece conteúdo relevante para a administração do banco de dados SAP HANA.
- SAP HANA System Replication: a replicação do sistema SAP HANA (SAP HSR) é o procedimento padrão fornecido pela SAP para replicar bancos de dados SAP HANA. Os executáveis necessários para o SAP HSR fazem parte do próprio kernel do servidor SAP HANA.

Épicos

Preparar os ambientes de origem e de destino

Tarefa	Descrição	Habilidades necessárias
Instale e configure os bancos de dados SAP HANA.	Nos ambientes de origem e destino, garanta que o banco de dados SAP HANA esteja instalado e configurado de acordo com as melhores práticas do SAP HANA. Para obter mais informações, consulte SAP HANA on. AWS	Administração do SAP Basis
Mapeie o endereço IP.	No ambiente de destino, certifique-se de que o nome do host temporário esteja atribuído a um endereço IP interno. 1. Atribua um IPv4 endereço secundário à EC2 instância no AWS Management Console navegando até	Administração da AWS

Tarefa	Descrição	Habilidades necessárias
	Instância EC2, Ações, Rede, Gerenciar endereço IP, Atribuir novo endereço IP. 2. Para atribuir o mesmo endereço ao adaptador de EC2 rede (NIC), do sistema operacional, como usuário root, execute o comando`ip addr add <IP>/32 dev eth0`, `<IP>` substituindo-o pelo endereço IP da etapa 1.	
Resolva os nomes de host de destino.	No banco de dados SAP HANA secundário, confirme se os dois nomes de host (`hdbhost` e `temp-host`) foram resolvidos para as redes de replicação do SAP HANA atualizando os nomes de host relevantes no arquivo `/etc/hosts` .	Administração do Linux
Faça backup dos bancos de dados SAP HANA de origem e de destino.	Use o SAP HANA Studio ou o cockpit do SAP HANA para realizar backups nos bancos de dados do SAP HANA.	Administração do SAP Basis

Tarefa	Descrição	Habilidades necessárias
Trocar certificados PKI do sistema.	(Aplica-se somente ao SAP HANA 2.0 e versões posteriores) Troque certificados no armazenamento seguro da infraestrutura de chave pública (PKI) do sistema no armazenamento do sistema de arquivos (SSFS) entre os bancos de dados primários e secundários. Para obter mais informações, consulte a nota do SAP nº 2369981 – Etapas de configuração necessárias para autenticação com a replicação do sistema SAP HANA.	Administração do SAP Basis

Renomeie o banco de dados SAP HANA de destino

Tarefa	Descrição	Habilidades necessárias
Interrompa as conexões do cliente-destino.	No ambiente de destino, desligue os servidores de aplicativos SAP e outras conexões de clientes.	Administração do SAP Basis
Renomeie o banco de dados SAP HANA de destino para o nome do host temporário.	1. Como usuário raiz, renomeie o nome de host do banco de dados SAP HANA de destino para o nome de host temporário usando `hdblcm` residente. `root $> cd /hana/shared/<SID/hdblcm`	Administração do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	`root $> ./hdblcm` 2. Escolha a opção 9 | `rename_system` | `Rename the SAP HANA Database System`. 3. Forneça o novo nome: `temp-host` . 4. Você pode validar outras opções conforme necessário. No entanto, certifique-se de não misturar a renomeação do host com uma alteração de SID (nota do SAP nº 2598814 – hdblcm: falha na renomeação do SID). A parada e o início do banco de dados SAP HANA serão controlados por `hdblcm`.	
Atribua redes de replicação.	No arquivo `global.ini` do sistema de origem, abaixo do cabeçalho `[system_replication_hostname_resolution]` , forneça os detalhes da rede de replicação de origem e destino. Em seguida, copie as entradas para o arquivo `global.ini` no sistema de destino.	Administração do SAP Basis

Tarefa	Descrição	Habilidades necessárias
Habilite a replicação no primário.	Para habilitar a replicação no SAP HANA DB, execute o comando a seguir. `hdbnsutil -sr_enable --name=siteA`	Administração do SAP Basis

Registre o banco de dados SAP HANA de destino como um sistema secundário.	Para registrar o banco de dados SAP HANA de destino como um sistema secundário de origem para o SAP HSR, escolha a replicação assíncrona.
	`(sid)adm $> HDB stop`
	`(sid)adm $> hdbnsutil -sr_register –name=siteB –remotehost=hdbhost /`
	`--remoteInstance=00 –replicationMode=async –operationMode=logreplay`
	`(sid)adm $> HDB start`
	Como alternativa, você pode escolher a opção `–online` de se registrar. Nesse caso, você não precisa parar e iniciar o banco de dados SAP HANA.
		Administração do SAP Basis

Tarefa	Descrição	Habilidades necessárias

Valide a sincronização.	No banco de dados SAP HANA de origem, verifique se todos os logs estão aplicados no sistema de destino (porque é uma replicação assíncrona).
	
	Para verificar a replicação, na origem, execute os comandos a seguir.
	
	`(sid)adm $> cdpy`
	`(sidadm $> python systemReplicationStatus.py`
		Administração do SAP Basis

Encerre o aplicativo SAP de origem e o banco de dados SAP HANA.	Durante a substituição da migração, desligue o sistema de origem (o aplicativo SAP e o banco de dados SAP HANA).	Administração do SAP Basis
Execute uma aquisição no destino.	Para realizar uma aquisição no alvo na AWS, execute o comando `hdbnsutil -sr_takeover` .	Administração do SAP Basis

Tarefa	Descrição	Habilidades necessárias
No banco de dados SAP HANA de destino, desative a replicação.	Para limpar os metadados de replicação, interromp a a replicação no sistema de destino executando o comando `hdbnsutil -sr_disable` . **Note** Isso está de acordo com a Nota SAP 2693441 — Falha ao renomear um sistema SAP HANA devido a um erro.	Administração do SAP Basis
Faça backup do banco de dados SAP HANA de destino.	Depois que a aquisição for bem-sucedida, recomenda mos realizar um backup completo do banco de dados SAP HANA.	Administração do SAP Basis

Reverta para o nome do host original no sistema de destino

Tarefa	Descrição	Habilidades necessárias
Reverta o nome do host de destino do banco de dados SAP HANA para o original.	1. Para reverter o nome de host do banco de dados SAP HANA de destino para o nome de host virtual original, use o `hdblcm` residente.	Administração do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	``` root $> cd /hana/shared/<SID>/hdblcm root $> ./hdblcm ``` 2. Escolha a opção `9 | rename_system | Rename the SAP HANA Database System`. 3. Forneça o novo nome: `hdbhost`. Você pode validar outras opções conforme necessário. No entanto, certifique-se de não misturar a renomeação do host com uma alteração de SID (nota do SAP nº 2598814 – hdblcm: falha na renomeação do SID).	
Ajuste hdbuserstore.	Adapte os detalhes `hdbuserstore` apontando para os detalhes `schema/user` da origem. Para obter etapas detalhadas, consulte a Documentação do SAP. Para validar essa etapa, execute o comando `R3trans -d`. O resultado deve refletir uma conexão bem-sucedida com o banco de dados SAP HANA.	Administração do SAP Basis

Tarefa	Descrição	Habilidades necessárias
Inicie as conexões do cliente.	No ambiente de destino, ligue os servidores de aplicativos SAP e outras conexões de clientes.	Administração do SAP Basis

Recursos relacionados

Referências do SAP

As referências da documentação do SAP são frequentemente atualizadas pela SAP. Para se manter atualizado, consulte a nota do SAP nº 2407186 – Guias de instruções e documentos técnicos sobre a alta disponibilidade do SAP HANA.

Notas adicionais do SAP

- 2550327 – Como renomear um sistema SAP HANA
- 1999880 – Perguntas frequentes: Replicação do sistema SAP HANA
- 2078425 – Nota de solução de problemas para a ferramenta de gerenciamento do ciclo de vida da plataforma SAP HANA hdblcm
- 2592227 – Alteração do sufixo FQDN em sistemas HANA
- 2048681 – Executando tarefas de administração do gerenciamento do ciclo de vida da plataforma SAP HANA em sistemas de vários hosts sem SSH ou credenciais raiz

Documentos SAP

- Conexão de rede de replicação do sistema
- Resolução de nome de host para replicação do sistema

AWS referências

- Migrando o SAP HANA de outras plataformas para AWS

Mais informações

As alterações realizadas por `hdblcm` como parte da atividade de renomeação do nome do host são consolidadas no seguinte log detalhado.

Migre o SQL Server para a AWS usando grupos de disponibilidade distribuídos

Criado por Praveen Marthala (AWS)

Resumo

Os grupos de disponibilidade do Microsoft SQL Server Always On fornecem uma solução de alta disponibilidade (HA) e recuperação de desastres (DR) para o SQL Server. Um grupo de disponibilidade consiste em uma réplica primária que aceita tráfego de leitura/gravação e até oito réplicas secundárias que aceitam tráfego de leitura. Um grupo de disponibilidade é configurado em um cluster de failover do Windows Server (WSFC) com dois ou mais nós.

Os grupos de disponibilidade distribuídos do Microsoft SQL Server Always On fornecem uma solução para configurar dois grupos de disponibilidade separados entre dois grupos independentes WFSCs. Os grupos de disponibilidade que fazem parte do grupo de disponibilidade distribuída não precisam estar no mesmo datacenter. Um grupo de disponibilidade pode estar no local e o outro grupo de disponibilidade pode estar na nuvem da Amazon Web Services (AWS) em instâncias da Amazon Elastic Compute Cloud (Amazon EC2) em um domínio diferente.

Esse padrão descreve as etapas para usar um grupo de disponibilidade distribuído para migrar bancos de dados SQL Server locais que fazem parte de um grupo de disponibilidade existente para o SQL Server com grupos de disponibilidade configurados na Amazon. EC2 Seguindo esse padrão, você pode migrar os bancos de dados para a Nuvem AWS com o mínimo de tempo de inatividade durante a substituição. Os bancos de dados estão altamente disponíveis na AWS imediatamente após a substituição. Você também pode usar esse padrão para alterar o sistema operacional subjacente on-premises para a AWS, mantendo a mesma versão do SQL Server.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Direct Connect ou AWS Site-to-Site VPN
- A mesma versão do SQL Server instalada on-premises e nos dois nós da AWS

Versões do produto

- SQL Server versão 2016 e posterior
- SQL Server Enterprise Edition

Arquitetura

Pilha de tecnologia de origem

- Banco de dados do Microsoft SQL Server com grupos de disponibilidade Always On on-premises

Pilha de tecnologias de destino

- Banco de dados Microsoft SQL Server com grupos de disponibilidade Always On na Amazon EC2 na nuvem da AWS

Arquitetura de migração

Terminologia

- WSFC 1 – WSFC on-premises
- WSFC 2 – WSFC na Nuvem AWS
- AG 1 – Primeiro grupo de disponibilidade, que está no WSFC 1
- AG 2 – Segundo grupo de disponibilidade, que está no WSFC 2
- Réplica primária do SQL Server – nó no AG 1 que é considerado o principal global para todas as gravações
- Encaminhador do SQL Server – nó no AG 2 que recebe dados de forma assíncrona da réplica primária do SQL Server
- Réplica secundária do SQL Server – nós no AG 1 ou AG 2 que recebem dados de forma síncrona da réplica primária ou do encaminhador

Ferramentas

- AWS Direct Connect: o AWS Direct Connect vincula sua rede interna a um local do AWS Direct Connect por meio de um cabo de fibra óptica de Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para serviços públicos da AWS, ignorando provedores de serviço da internet no caminho da sua rede.

- Amazon EC2 — A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode usar EC2 a Amazon para lançar quantos servidores virtuais precisar e pode expandir ou aumentar a escala.
- AWS Site-to-Site VPN — O AWS Site-to-Site VPN oferece suporte à criação de uma rede privada site-to-site virtual (VPN). Você pode configurar o VPN para transmitir tráfego entre instâncias que você executa na AWS e sua própria rede remota.
- Microsoft SQL Server Management Studio: o Microsoft SQL Server Management Studio (SSMS) é um ambiente integrado para o gerenciamento de uma infraestrutura do SQL Server. Ele fornece uma interface de usuário e um grupo de ferramentas com editores de scripts avançados que interagem com o SQL Server.

Épicos

Configure um segundo grupo de disponibilidade na AWS

Tarefa	Descrição	Habilidades necessárias
Crie um WSFC na AWS.	Crie o WSFC 2 em EC2 instâncias da Amazon com dois nós para HA. Você usará esse cluster de failover para criar o segundo grupo de disponibilidade (AG 2) na AWS.	Administrador de sistemas, SysOps administrador
Crie o segundo grupo de disponibilidade no WSFC 2.	Usando o SSMS, crie o AG 2 em dois nós no WSFC 2. O primeiro nó no WSFC 2 atuará como encaminhador. O segundo nó no WSFC 2 atuará como a réplica secundária do AG 2. Neste estágio, nenhum banco de dados está disponíve l no AG 2. Esse é o ponto de partida para configurar	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	o grupo de disponibilidade distribuído.	
Crie bancos de dados sem opção de recuperação no AG 2.	Faça backup dos bancos de dados no grupo de disponibilidade on-premises (AG 1). Restaure os bancos de dados tanto para o encaminhador quanto para a réplica secundária do AG 2 sem opção de recuperação. Ao restaurar os bancos de dados, especifique um local com espaço em disco suficiente para os arquivos de dados do banco de dados e os arquivos de log. Nesse estágio, os bancos de dados estão em estado de restauração. Eles não fazem parte do AG 2 ou do grupo de disponibilidade distribuída e não estão sincronizando.	DBA, Desenvolvedor

Configurar o grupo de disponibilidade distribuído

Tarefa	Descrição	Habilidades necessárias
Crie o grupo de disponibilidade distribuída no AG 1.	Para criar o grupo de disponibilidade distribuído no AG 1, use o `CREATE AVAILABILITY GROUP` com a opção `DISTRIBUTED`.	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	1. Use endereços de endpoint `LISTENER_URL` para o AG 1 e o AG 2. 2. Para `AVAILABILITY-MODE`, use `ASYNCHRONOUS_COMMIT` para evitar a latência da rede, se houver. Isso não afetará o desempenho do banco de dados. 3. Para `FAILOVER_MODE`, use `MANUAL`. É o único modo de disponibilidade que funciona com grupos de disponibilidade distribuídos. 4. Para restaurar os bancos de dados manualmente no AG 2 e ter mais controle sobre bancos de dados maiores, use `MANUAL` for `SEEDING_MODE`.	

Tarefa	Descrição	Habilidades necessárias
Crie o grupo de disponibilidade distribuída no AG 2.	Para criar o grupo de disponibilidade distribuído no AG 2, use o `ALTER AVAILABILITY GROUP` com a opção `DISTRIBUTED`. 1. Use endereços de endpoint `LISTENER_URL` para o AG 1 e o AG 2. 2. Para `AVAILABILITY-MODE`, use `ASYNCHRONOUS_COMMIT` para evitar a latência da rede, se houver. Isso não afetará o desempenho do banco de dados. 3. Para `FAILOVER_MODE`, use `MANUAL`. É o único modo de disponibilidade que funciona com grupos de disponibilidade distribuídos. 4. Para restaurar os bancos de dados manualmente no AG 2 e ter mais controle sobre bancos de dados maiores, use `MANUAL` for `SEEDING_MODE`. O grupo de disponibilidade distribuída é criado entre o AG 1 e o AG 2.	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Os bancos de dados no AG 2 ainda não estão configura dos para participar do fluxo de dados do AG 1 para o AG 2.	
Adicione bancos de dados ao encaminhador e à réplica secundária no AG 2.	Adicione os bancos de dados ao grupo de disponibilidade distribuído usando `ALTER DATABASE` com a opção `SET HADR AVAILABILITY GROUP` no encaminhador e na réplica secundária no AG 2. Isso inicia o fluxo de dados assíncrono entre bancos de dados no AG 1 e no AG 2. O primário global faz gravações, envia dados de forma síncrona para a réplica secundária no AG 1 e envia os dados de forma assíncrona para o encaminha dor no AG 2. O encaminha dor no AG 2 envia dados de forma síncrona para a réplica secundária no AG 2.	DBA, Desenvolvedor

Monitore o fluxo de dados assíncrono entre o AG 1 e o AG 2

Tarefa	Descrição	Habilidades necessárias
Registros de uso DMVs e do SQL Server.	Monitore o status do fluxo de dados entre dois grupos de disponibilidade usando	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	exibições de gerenciamento dinâmico (DMVs) e registros do SQL Server. DMVs que são de interesse para monitoramento incluem `sys.dm_hadr_availability_replica_states` `sys.dm_hadr_automatic_seeding` e. Para saber o status da sincronização do encaminhador, monitore o estado sincronizado no log do SQL Server no encaminhador.	

Execute atividades de substituição para a migração final

Tarefa	Descrição	Habilidades necessárias
Interrompa todo o tráfego para a réplica primária.	Interrompa o tráfego de entrada para a réplica primária no AG 1 para que nenhuma atividade de gravação ocorra nos bancos de dados e os bancos de dados estejam prontos para a migração.	Proprietário do aplicativo, desenvolvedor
Altere o modo de disponibilidade do grupo de disponibilidade distribuída no AG 1.	Na réplica primária, defina o modo de disponibilidade do grupo de disponibilidade distribuído como síncrono.	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Depois de alterar o modo de disponibilidade para síncrono, os dados são enviados de forma síncrona da réplica primária no AG 1 para o encaminhador no AG 2.	
Verifique LSNs em ambos os grupos de disponibilidade.	Verifique os últimos números de sequência de log (LSNs) no AG 1 e no AG 2. Como nenhuma gravação está acontecendo na réplica primária no AG 1, os dados são sincronizados e os últimos LSNs para os dois grupos de disponibilidade devem corresponder.	DBA, Desenvolvedor
Atualize o AG 1 para a função secundária.	Quando você atualiza o AG 1 para a função secundári a, o AG 1 perde a função de réplica principal e não aceita gravações, e o fluxo de dados entre dois grupos de disponibi lidade é interrompido.	DBA, Desenvolvedor

Faça o failover para o segundo grupo de disponibilidade

Tarefa	Descrição	Habilidades necessárias
Faça o failover manual para o AG 2.	No encaminhador no AG 2, altere o grupo de disponibi lidade distribuído para permitir a perda de dados. Como você já verificou e confirmou que	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	os últimos LSNs no AG 1 e no AG 2 coincidem, a perda de dados não é uma preocupaç ão. Quando você permite a perda de dados no encaminhador no AG 2, as funções do AG 1 e do AG 2 mudam: • O AG 2 se torna o grupo de disponibilidade com a réplica primária e a réplica secundária. • O AG 1 se torna o grupo de disponibilidade com o encaminhador e a réplica secundária.	
Altere o modo de disponibi lidade do grupo de disponibi lidade distribuída no AG 2.	Na réplica primária no AG 2, altere o modo de disponibi lidade para assíncrono. Isso altera a movimentação de dados do AG 2 para o AG 1, de síncrono para assíncrono. Essa etapa é necessária para evitar a latência de rede entre o AG 2 e o AG 1, se houver, e não afetará o desempenho do banco de dados.	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Comece a enviar tráfego para a nova réplica primária.	Atualize a cadeia de conexão para usar o endpoint de URL do receptor no AG 2 para enviar tráfego para os bancos de dados. O AG 2 agora aceita gravações e envia dados para o encaminhador no AG 1, além de enviar dados para sua própria réplica secundári a no AG 2. Os dados são movidos de forma assíncrona do AG 2 para o AG 1.	Proprietário do aplicativo, desenvolvedor

Realizar atividades pós-substituição

Tarefa	Descrição	Habilidades necessárias
Descarte o grupo de disponibi lidade distribuída no AG 2.	Monitore a migração pelo período de tempo planejado. Em seguida, descarte o grupo de disponibilidade distribuí da no AG 2 para remover a configuração do grupo de disponibilidade distribuí da entre o AG 2 e o AG 1. Isso remove a configura ção do grupo de disponibi lidade distribuído e o fluxo de dados do AG 2 para o AG 1 é interrompido. Neste momento, o AG 2 está altamente disponível na AWS,	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	com uma réplica primária que recebe gravações e uma réplica secundária no mesmo grupo de disponibilidade.	
Desative os servidores on-premises.	Desative os servidores on-premises no WSFC 1 que fazem parte do AG 1.	Administrador de sistemas, SysOps administrador

Recursos relacionados

- Grupos de disponibilidade distribuídos
- SQL Docs: grupos de disponibilidade distribuídos
- SQL Docs: grupos de disponibilidade Always On: uma solução de alta disponibilidade e recuperação de desastres

Migre do Oracle 8i ou 9i para o Amazon RDS for Oracle usando o AWS DMS SharePlex

Criado por Ramu Jagini (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados Oracle 8i ou 9i on-premises para um banco de dados do Amazon Relational Database Service (Amazon RDS) para Oracle. Você pode usar esse padrão para concluir sua migração com tempo de inatividade reduzido usando o Quest SharePlex para replicação síncrona.

Você deve usar uma instância de banco de dados do Oracle intermediária para sua migração porque o AWS Database Migration Service (AWS DMS) não oferece suporte ao Oracle 8i ou 9i como ambiente de origem. Você pode usar a SharePlex versão 7.6.3 para replicar de versões anteriores do banco de dados Oracle para versões posteriores do banco de dados Oracle. A instância intermediária do banco de dados Oracle é compatível como destino para a SharePlex versão 7.6.3 e suportada como fonte para o AWS DMS ou versões mais recentes do. SharePlex Esse suporte permite a replicação contínua de dados para o ambiente de destino do Amazon RDS para Oracle.

Considere que vários tipos de dados e atributos obsoletos podem afetar a migração do Oracle 8i ou 9i para a versão mais recente do Oracle Database. Para mitigar esse impacto, esse padrão usa o Oracle 11.2.0.4 como uma versão intermediária do banco de dados para ajudar a otimizar o código do esquema antes da migração para o ambiente de destino do Amazon RDS para Oracle.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem do Oracle 8i ou 9i em um ambiente on-premises
- Oracle Database 12c versão 2 (12CR2) para armazenamento temporário no Amazon Elastic Compute Cloud (Amazon) EC2
- Quest SharePlex 7.6.3 (nível comercial)

Limitações

- Limitações do RDS for Oracle

Versões do produto

- Oracle 8i ou 9i para o banco de dados de origem
- Oracle 12 CR2 para o banco de dados de teste (deve corresponder à versão do Amazon RDS for Oracle)
- Oracle 12 CR2 ou posterior para o banco de dados de destino (Amazon RDS for Oracle)

Arquitetura

Pilha de tecnologia de origem

- Banco de dados do Oracle 8i ou 9i
- SharePlex

Pilha de tecnologias de destino

- Amazon RDS para Oracle

Arquitetura de migração

O diagrama a seguir mostra como migrar um banco de dados Oracle 8i ou 9i de um ambiente on-premises para uma instância de banco de dados do Amazon RDS para Oracle na Nuvem AWS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Ative o banco de dados de origem Oracle com o modo de registro de arquivamento, registro forçado e registro suplementar.
2. Restaure o banco de dados intermediário Oracle a partir do banco de dados de origem Oracle usando a recuperação do Recovery Manager (RMAN) e o point-in-time FLASHBACK_SCN.
3. Configure SharePlex para ler redo logs do banco de dados de origem Oracle usando `FLASHBACK_SCN` (usado no RMAN).
4. Inicie a SharePlex replicação para sincronizar dados do banco de dados de origem Oracle com o banco de dados intermediário Oracle.

5. Restaure o banco de dados de destino do Amazon RDS para Oracle usando EXPDP e IMPDP com `FLASHBACK_SCN`.
6. Configure o AWS DMS e suas tarefas de origem como o banco de dados intermediário Oracle e o Amazon RDS para Oracle como o banco de dados de destino usando `FLASHBACK_SCN` (usado no EXPDP).
7. Inicie tarefas do AWS DMS para sincronizar dados do banco de dados intermediário da Oracle com o banco de dados de destino da Oracle.

Ferramentas

- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- SharePlexA Quest é uma ferramenta Oracle-to-Oracle de replicação de dados para mover dados com o mínimo de tempo de inatividade e sem perda de dados.
- O Recovery Manager (RMAN) é um cliente de banco de dados do Oracle que executa tarefas de backup e recuperação em seus bancos de dados. Isso simplifica imensamente o backup, a restauração e a recuperação de arquivos de banco de dados.
- O Data Pump Export ajuda você a carregar dados e metadados em um conjunto de arquivos do sistema operacional chamado conjunto de arquivos de despejo. O conjunto de arquivos de despejo só pode ser importado pelo utilitário Data Pump Import (Importação do Data Pump) ou pelo pacote DBMS_DATAPUMP.

Épicos

Configuração SharePlex e o banco de dados de teste da Oracle na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Crie uma EC2 instância.	1. Crie uma EC2 instância. 2. Instale o Oracle 12 CR2 na EC2 instância para servir como banco de dados intermediário Oracle.	Administração do Oracle

Tarefa	Descrição	Habilidades necessárias
Prepare o banco de dados de preparação.	Prepare o banco de dados intermediário Oracle para restauração como um upgrade no Oracle 12 CR2 usando o backup RMAN do ambiente de origem do banco de dados Oracle 8i ou 9i. Para obter mais informações, consulte o Guia do usuário do Oracle 9i Recovery Manager e o Guia do usuário de backup e recuperação do banco de dados na documentação do Oracle.	Administração do Oracle
Configurar SharePlex.	Configure a SharePlex origem como um banco de dados Oracle 8i ou 9i local e configure o destino como o banco de dados intermediário Oracle 12 CR2 hospedado na Amazon. EC2	SharePlex, administração da Oracle

Configure o Amazon RDS para Oracle como seu ambiente de destino

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de banco de dados Oracle.	Crie um banco de dados Amazon RDS for Oracle e, em seguida, conecte o Oracle CR2 12 ao banco de dados. Para obter mais informações, consulte Criar uma instância	DBA

Tarefa	Descrição	Habilidades necessárias
	de banco de dados Oracle e conectar-se a um banco de dados em uma instância de banco de dados Oracle na documentação do Amazon RDS.	
Restaure o Amazon RDS para Oracle a partir do banco de dados de teste.	1. Faça um backup EXPDP do servidor de banco de dados intermediário do Oracle usando `FLASHBACK_SCN` . 2. Restaure o Amazon RDS para Oracle a partir do banco de dados de teste. Para obter mais informaçõ es, consulte 54 DBMS_DATA PUMP na documentação da Oracle.	DBA

Configurar o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Crie endpoints para os bancos de dados.	Crie um endpoint de origem para o banco de dados intermediário Oracle e um endpoint de destino para o banco de dados do Amazon RDS para Oracle. Para obter mais informações, consulte Como criar endpoints de origem ou de destino	DBA

Tarefa	Descrição	Habilidades necessárias
	usando o AWS DMS? no Centro de Conhecimentos da AWS.	
Criação de uma instância de replicação.	Use o AWS DMS para iniciar uma instância de replicação do banco de dados intermediário Oracle para o banco de dados do Amazon RDS para Oracle. Para obter mais informações, consulte Como criar uma instância de replicação do AWS DMS? no Centro de Conhecimentos da AWS.	DBA
Crie e inicie tarefas de replicação.	Crie tarefas de replicação do AWS DMS para captura de dados de alterações (CDC) usando o EXPDP (já que a carga total de `FLASHBACK_SCN` já aconteceu por meio do EXPDP). Para obter mais informações, consulte Criar uma tarefa na documentação do AWS DMS.	DBA

Substituição para o Amazon RDS para Oracle

Tarefa	Descrição	Habilidades necessárias
Interrompa o workload do aplicativo.	Interrompa os servidores de aplicativos e seus aplicativos	Desenvolvedor de aplicativos, DBA

Tarefa	Descrição	Habilidades necessárias
	durante a janela de substituição planejada.	
Valide a sincronização do banco de dados temporário local da Oracle com a instância. EC2	Confirme se todas as mensagens foram publicadas para tarefas de replicação da instância de SharePlex replicação no banco de dados de teste Oracle na Amazon EC2 executando algumas mudanças de log no banco de dados de origem local. Para obter mais informações, consulte 6.4.2 Alternar um arquivo de log na documentação do Oracle.	DBA
Valide a sincronização do banco de dados intermediário do Oracle com o banco de dados do Amazon RDS para Oracle.	Confirme se todas as suas tarefas do AWS DMS não têm atrasos nem erros e, em seguida, verifique o estado de validação das tarefas.	DBA
Pare a replicação do SharePlex Amazon RDS.	Se as replicações do AWS DMS SharePlex e do AWS não estiverem mostrando nenhum erro, interrompa as duas replicações.	DBA

Tarefa	Descrição	Habilidades necessárias
Remapeie o aplicativo para o Amazon RDS.	Compartilhe os detalhes do endpoint do Amazon RDS para Oracle com o servidor de aplicativos e seus aplicativos e, em seguida, inicie o aplicativo para retomar as operações comerciais.	Desenvolvedor de aplicativos, DBA

Teste o ambiente de destino da AWS

Tarefa	Descrição	Habilidades necessárias
Teste o ambiente de banco de dados de teste da Oracle na AWS.	1. Teste a SharePlex replicação e verifique se não há lacunas de sincronização ou erros de replicação no banco de dados intermediário Oracle. 2. Verifique se o aplicativo se comporta conforme o esperado por meio de benchmarks definidos no ambiente on-premises.	SharePlex, administração da Oracle
Teste o ambiente do Amazon RDS.	1. Verifique se todos os dados propagados para o Amazon RDS após a replicação estão livres de erros. 2. Aponte outro aplicativo para a instância de banco de dados do Amazon RDS e, em seguida, execute testes de desempenho para	Administração do Oracle

Tarefa	Descrição	Habilidades necessárias
	verificar o comportamento esperado. Para obter mais informações, consulte o Amazon RDS para Oracle na documentação do Amazon RDS.	

Recursos relacionados

- Migre com confiança
- Amazon EC2
- Amazon RDS para Oracle
- AWS Database Migration Service
- Como depurar suas migrações do AWS DMS: o que fazer quando as coisas dão errado (Parte 1)
- Como depurar suas migrações do AWS DMS: o que fazer quando as coisas dão errado (Parte 2)
- Como depurar suas migrações do AWS DMS: o que fazer quando as coisas dão errado? (Parte 3)
- SharePlex para replicação de banco de dados
- SharePlex: replicação de banco de dados para qualquer ambiente

Monitore o Amazon Aurora em busca de instâncias sem criptografia

Criado por Mansi Suratwala (AWS)

Resumo

Esse padrão fornece um CloudFormation modelo da Amazon Web Services (AWS) que você pode implantar para configurar notificações automáticas quando uma instância do Amazon Aurora é criada sem a criptografia ativada.

O Aurora é um mecanismo de banco de dados relacional gerenciado compatível com o MySQL e o PostgreSQL. Com algumas cargas de trabalho, o Aurora pode oferecer até cinco vezes a taxa de processamento do MySQL e até três vezes a taxa de processamento do PostgreSQL, sem exigir alterações na maioria das aplicações existentes.

O CloudFormation modelo cria um evento Amazon CloudWatch Events e uma função do AWS Lambda. O evento usa CloudTrail a AWS para monitorar qualquer criação de instância do Aurora ou uma restauração pontual de uma instância existente. O evento Cloudwatch Events inicia a função do Lambda, que verifica se a criptografia está ativada. Se a criptografia não estiver ativada, a função do Lambda enviará uma notificação do Amazon Simple Notification Service (Amazon SNS) informando você sobre a violação.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa

Limitações

- Esse controle de serviço funciona somente com instâncias do Amazon Aurora. Ele não é compatível com outras instâncias do Amazon Relational Database Service (Amazon RDS).
- O CloudFormation modelo deve ser implantado somente para `CreateDBInstance` **`RestoreDBClusterToPointInTim`**e.

Versões do produto

- Versões do PostgreSQL que são compatíveis no Amazon Aurora
- Versões do MySQL que são compatíveis com o Amazon Aurora

Arquitetura

Pilha de tecnologias de destino

- Amazon Aurora
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Arquitetura de destino

Automação e escala

Você pode usar o CloudFormation modelo várias vezes para diferentes regiões e contas. Você precisa executá-lo apenas uma vez em cada região ou conta.

Ferramentas

Ferramentas

- Amazon Aurora: o Amazon Aurora é um mecanismo de banco de dados relacional gerenciado compatível com o MySQL e o PostgreSQL.
- AWS CloudTrail — CloudTrail A AWS ajuda você a gerenciar a governança, a conformidade e a auditoria operacional e de risco da sua conta da AWS. As ações realizadas por um usuário, uma função ou um serviço da AWS são registradas como eventos em CloudTrail.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um near-real-time fluxo de eventos do sistema que descrevem as mudanças nos recursos da AWS.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que você pode usar para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.

- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens usando Lambda, HTTP, e-mail, notificações push móveis e mensagens de texto móveis (SMS).

Código

Um arquivo .zip do projeto está disponível como anexo.

Épicos

Crie o bucket do S3 para o script do Lambda

Tarefa	Descrição	Habilidades necessárias
Defina o bucket do S3.	Abra o console do Amazon S3, escolha ou crie um bucket do S3. Esse bucket do S3 hospedará o arquivo.zip do código Lambda. Seu bucket do S3 precisa estar na mesma região da que o Aurora. O nome do bucket do S3 não pode conter barras iniciais.	Arquiteto de nuvem

Carregar o código do Lambda para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Faça o upload do código do Lambda.	Faça upload do arquivo .zip do código Lambda fornecido na seção Anexos para o bucket do S3 que você definiu.	Arquiteto de nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	No CloudFormation console, implante o `RDS_Aurora_Encryption_At_Rest.yml` CloudFormation modelo fornecido como anexo a esse padrão. No próximo épico, forneça valores para os parâmetros do modelo.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Dê o nome do bucket do S3.	Insira o nome do bucket do S3 que você criou ou escolheu no primeiro épico.	Arquiteto de nuvem
Forneça a chave do S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `<directory>/<file-name>.zip`).	Arquiteto de nuvem
Forneça um endereço de e-mail.	Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS.	Arquiteto de nuvem
Defina o nível de registro em log.	Defina o nível de registro em log e a frequência da sua função do Lambda. `Info` designa mensagens informativas detalhadas sobre	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	o progresso do aplicativo. `Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail fornecido. Você precisa confirmar sua assinatura para começar a receber as notificações.	Arquiteto de nuvem

Recursos relacionados

- Criar um bucket do S3
- Fazer upload de arquivos em um bucket do S3
- Criar um cluster de banco de dados do Amazon Aurora
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS CloudTrail

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Monitore GoldenGate os logs do Oracle usando a Amazon CloudWatch

Criado por Chithra Krishnamurthy (AWS)

Resumo

GoldenGate A Oracle fornece replicação em tempo real entre o Amazon Relational Database Service (Amazon RDS) para bancos de dados Oracle ou entre bancos de dados Oracle hospedados no Amazon Elastic Compute Cloud (Amazon). EC2 Ele oferece suporte à replicação unidirecional e bidirecional.

Quando você usa GoldenGate para replicação, o monitoramento é fundamental para verificar se o GoldenGate processo está ativo e em execução, para garantir que os bancos de dados de origem e de destino estejam sincronizados.

Esse padrão explica as etapas para implementar o CloudWatch monitoramento da Amazon para um registro de GoldenGate erros e como definir alarmes para enviar notificações para eventos específicos, como`STOP`, por exemplo, para que você `ABEND` possa tomar as medidas apropriadas para retomar a replicação rapidamente.

Pré-requisitos e limitações

Pré-requisitos

- GoldenGate instalado e configurado em uma EC2 instância, para que você possa configurar o CloudWatch monitoramento dessas EC2 instâncias. Se você quiser monitorar a replicação bidirecional GoldenGate em todas as regiões da AWS, você deve instalar o CloudWatch agente em cada EC2 instância em que o GoldenGate processo está sendo executado.

Limitações

- Esse padrão explica como monitorar o GoldenGate processo usando CloudWatch o. CloudWatch não monitora atrasos na replicação ou problemas de sincronização de dados durante a replicação. Você deve executar consultas SQL separadas para monitorar o atraso na replicação ou os erros relacionados aos dados, conforme explicado na documentação. GoldenGate

Versões do produto

- Este documento é baseado na implementação do Oracle GoldenGate 19.1.0.0.4 para Oracle no Linux x86-64. No entanto, essa solução é aplicável a todas as versões principais do GoldenGate.

Arquitetura

Pilha de tecnologias de destino

- GoldenGate binários para Oracle instalados em uma instância EC2
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)

Arquitetura de destino

Ferramentas

Serviços da AWS

- A Amazon CloudWatch é um serviço de monitoramento usado nesse padrão para monitorar registros GoldenGate de erros.
- O Amazon SNS é um serviço de notificação de mensagens usado nesse padrão para enviar notificações por e-mail.

Outras ferramentas

- GoldenGate O Oracle é uma ferramenta de replicação de dados que você pode usar para o Amazon RDS for Oracle ou bancos de dados Oracle hospedados na Amazon. EC2

Etapas de implementação de alto nível

1. Crie uma função do AWS Identity and Access Management (IAM) para o CloudWatch agente.
2. Anexe a função do IAM à EC2 instância em que os registros GoldenGate de erros são gerados.
3. Instale o CloudWatch agente na EC2 instância.
4. Configure os arquivos de configuração do CloudWatch agente: `awscli.conf` `awslogs.conf` e.
5. Inicie o CloudWatch agente.
6. Crie filtros métricos no grupo de logs.

7. Configuração do Amazon SNS.
8. Criar um alarme para o filtro de métricas. O Amazon SNS envia alertas por e-mail quando esses filtros capturam eventos.

Para obter instruções detalhadas, consulte a próxima seção.

Épicos

Etapa 1. Crie uma função do IAM para o CloudWatch agente

Tarefa	Descrição	Habilidades necessárias
Crie o perfil do IAM.	O acesso aos recursos da AWS exige permissões, então você cria funções do IAM para incluir as permissões necessárias para que cada servidor execute o CloudWatch agente. Para criar um perfil do IAM: 1. Faça login no Console de Gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/. 2. No painel de navegação, escolha Perfis e Criar perfil. 3. Em Tipo de entidade confiável, escolha Serviços da AWS. 4. Para Casos de uso comuns, escolha e EC2, em seguida, escolha Avançar. 5. Na lista de políticas, marque a caixa de seleção	AWS geral

Tarefa	Descrição	Habilidades necessárias
	ao lado de CloudWatc hAgentServerPolicy. Se necessário, use a caixa de pesquisa para encontrar a política. 6. Escolha Próximo. 7. Em Role name (Nome da função), insira um nome para a nova função, como `goldengate-cw-moni toring-role` ou outro nome que você preferir. 8. (Opcional) Em Role description (Descrição da função), insira uma descrição. 9. Confirme se isso CloudWatchAgentSer verPolicyaparece em Nome da política. 10. (Opcional) Adicione um ou mais (pares chave-valor) de tag para organizar, rastrear ou controlar o acesso a essa função e, em seguida, escolha Criar perfil.	

Etapa 2. Anexe a função do IAM à GoldenGate EC2 instância

Tarefa	Descrição	Habilidades necessárias
Anexe a função do IAM à EC2 instância em que os registros	Os registros de erro gerados por GoldenGate precisam	AWS geral

Tarefa	Descrição	Habilidades necessárias
GoldenGate de erros são gerados.	ser preenchidos CloudWatch e monitorados, então você precisa anexar a função do IAM que você criou na etapa 1 à EC2 instância em que GoldenGate está sendo executada. Como anexar um perfil do IAM a uma instância: 1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/. 2. No painel de navegação, escolha Instâncias e encontre a instância em que GoldenGate está sendo executada. 3. Selecione a instância, em seguida escolha Ações, Segurança, Modificar perfil do IAM. 4. Selecione o perfil do IAM a ser anexado à instância e selecione Salvar.	

Etapas 3-5. Instale e configure o CloudWatch agente na instância Goldengate EC2

Tarefa	Descrição	Habilidades necessárias
Instale o CloudWatch agente na GoldenGate EC2 instância.	Para instalar o agente, execute o comando:	AWS geral

Tarefa	Descrição	Habilidades necessárias
	`sudo yum install -y awslogs`	

Tarefa	Descrição	Habilidades necessárias

Edite os arquivos de configuração do agente.	1. Execute o seguinte comando:
	`sudo su -`
	2. Edite esse arquivo para atualizar a região da AWS conforme necessário.
	`cat /etc/awslogs/conf`
	`[plugins]`
	`cwlogs = cwlogs`
	`[default]`
	`region = us-east-1`
	3. Edite o `/etc/awslogs/awslogs.conf` arquivo para atualizar o nome do arquivo, o nome do grupo de registros e o date/time format. You must specify the date/time para que corresponda ao formato da data`ggserror.log` ; caso contrário, o fluxo de registros não fluirá para dentro CloudWatch. Por exemplo:
	`datetime_format = %Y-`
	`%m-%dT%H:%M:%S%z`
	`file = /u03/oracle/`
	`oragg/ggserr.log`
	`log_group_name =`
	` goldengate_monitor`
		AWS geral

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudWatch agente.	Para iniciar o agente, use o seguinte comando. `$ sudo service awslogsd start` Depois de iniciar o agente, você pode visualizar o grupo de registros no CloudWatch console. O fluxo de logs terá o conteúdo do arquivo.	AWS geral

Etapa 6. Crie filtros métricos para o grupo de logs

Tarefa	Descrição	Habilidades necessárias
Crie filtros de métricas para as palavras-chave ABEND e STOPPED.	Quando você cria filtros métricos para o grupo de logs, sempre que os filtros são identificados no registro de erros, ele inicia um alarme e envia uma notificação por e-mail com base na configuração do Amazon SNS. Para criar um filtro de métricas: 1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/. 2. Escolha o nome do grupo de logs.	CloudWatch

Tarefa	Descrição	Habilidades necessárias
	3. Escolha Actions (Ações) e Create metric filter (Criar filtro de métrica). 4. Para o padrão de filtro, especifique um padrão comoABEND. 5. Escolha Next (Próximo) e digite um nome para o filtro de métrica. 6. Em Detalhes da métrica, em Namespace métrica, insira um nome para o CloudWatch namespace em que a métrica será publicada. Se esse namespace ainda não existir, certifique-se de que a opção Create new (Criar novo) esteja selecionada. 7. Em Valor da métrica, digite 1 se o filtro de métrica estiver contando ocorrênci as das palavras-chave no filtro. 8. Defina a unidade como Nenhuma. 9. Escolha Criar filtro de métrica. Você pode encontrar o filtro de métrica que criou no painel de navegação. 10. Crie outro filtro métrico para o STOPPED padrão. Em um	

Tarefa	Descrição	Habilidades necessárias
	grupo de logs, você pode criar vários filtros métricos e definir alarmes individua lmente.	

Etapa 7. Configuração do Amazon SNS

Tarefa	Descrição	Habilidades necessárias
Criar um tópico do SNS.	Nesta etapa, você configura o Amazon SNS para criar alarmes para os filtros métricos. Para criar um tópico do SNS: 1. Faça login no console do Amazon SNS em casahttps://console.aws.amazon.com/sns/. 2. Em Criar tópico, insira o nome do tópico, por exemplo, `goldengate-alert` e então escolha Próximas etapas. 3. Em Tipo, escolha Padrão. 4. Role até o final do formulário e escolha Create topic (Criar tópico). O console abrirá a página Details (Detalhes) do tópico.	Amazon SNS
Crie uma assinatura.	Crie uma assinatura para o tópico:	Amazon SNS

Tarefa	Descrição	Habilidades necessárias
	1. No painel de navegação à esquerda, escolha Assinaturas. 2. Na página Assinaturas, escolha Criar assinatura. 3. Na página Criar assinatura, escolha o campo TARN do tópico para ver uma lista dos tópicos em sua conta AWS. 4. Escolha o tópico que você criou na etapa anterior. 5. Em Protocolo, escolha E-mail. 6. Em Endpoint, insira um endereço de e-mail que possa receber notificações. 7. Escolha Criar a assinatura. O console abre a página de Detalhes da nova assinatura. 8. Verifique sua caixa de entrada de e-mail da AWS Notifications e escolha Confirmar a assinatura no e-mail. O Amazon SNS abre seu navegador da Web e exibe uma confirmação de assinatura com seu ID de assinatura.	

Etapa 8. Crie um alarme para enviar notificações para os filtros métricos

Tarefa	Descrição	Habilidades necessárias
Crie um alarme para o tópico do SNS.	Para criar um alarme com base em um filtro de métrica de grupo de logs: 1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/. 2. No painel de navegação, escolha Logs e escolha Log groups (Grupos de logs). 3. Escolha o grupo de logs que contém seu filtro de métrica. 4. Escolha Metric filters (Filtros de métrica). 5. Na guia de Filtros de métrica, selecione a caixa do filtro de métrica no qual deseja basear seu alarme. 6. Selecione Criar alarme. 7. Para as Condições, é necessário especificar o seguinte em cada seção: • Em Tipo de limite, escolha Estático. • Para Quando a métrica <metric-name> for . . ., escolha Maior. • Para que... , especifique 0.	CloudWatch

Tarefa	Descrição	Habilidades necessárias
	8. Escolha Próximo. 9. Em Notificação: • Em Alarm state trigger (Gatilho do estado do alarme), escolha In alarm (Em alarme). • Em Envie notificação para o seguinte tópico do SNS, escolha Selecione um tópico existente. • Na caixa de e-mail, selecione o tópico do Amazon SNS que você criou na etapa anterior. 10. Escolha Próximo. 11. Em Name e Description (Nome e Descrição), insira um nome e uma descrição para o seu alarme. **Note** Para a descrição, você pode especificar o nome da instância para que o e-mail de notificação seja descritivo. 12. Em Pré-visualizar e criar, verifique se sua configuração está correta e em seguida escolha Criar alarme.	

Tarefa	Descrição	Habilidades necessárias
	Após essas etapas, sempre que esses padrões forem detectados no arquivo de log de GoldenGate erros (`ggserr.log`) que você está monitorando, você receberá uma notificação por e-mail.	

Solução de problemas

Problema	Solução
O fluxo de log do registro GoldenGate de erros não flui para dentro CloudWatch.	Verifique o `/etc/awslogs/awslogs.conf` arquivo para verificar o nome do arquivo, o nome do grupo de registros e date/time format. You must specify the date/time a correspondência com o formato de data em`ggserror.log` . Caso contrário, o fluxo de log não fluirá para dentro CloudWatch.

Recursos relacionados

- CloudWatch Documentação da Amazon
- Coleta de métricas e registros com o CloudWatch agente
- Documentação do Amazon SNS

Redefinir a plataforma do Oracle Database Enterprise Edition para o Standard Edition 2 no Amazon RDS para Oracle

Criado por Lanre (Lan-Ray) showunmi (AWS) e Tarun Chawla (AWS)

Resumo

O Oracle Database Enterprise Edition (EE) é uma escolha popular em muitas empresas para executar aplicativos. Em alguns casos, no entanto, os aplicativos usam poucos ou nenhum atributo do Oracle Database EE, portanto, não há justificativa para incorrer em enormes custos de licenciamento. Você pode obter economia de custos fazendo o downgrade desses bancos de dados para o Oracle Database Standard Edition 2 (SE2) ao migrar para o Amazon RDS.

Esse padrão descreve como fazer o downgrade do Oracle Database EE para o Oracle Database SE2 ao migrar do local para o Amazon RDS for Oracle. As etapas apresentadas nesse padrão também se aplicam se seu banco de dados EE Oracle já estiver em execução no Amazon RDS ou em uma instância do Amazon Elastic Compute Cloud EC2 (Amazon).

Para obter mais informações, consulte o guia Recomendações da AWS sobre como avaliar o downgrade de bancos de dados Oracle para a Standard Edition 2 na AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Oracle Database Enterprise Edition
- Uma ferramenta cliente, como Oracle SQL Developer ou SQL*Plus, para conectar e executar comandos SQL no banco de dados Oracle
- Usuário do banco de dados para realizar a avaliação; por exemplo, um dos seguintes:
  - Usuário com privilégios suficientes para executar a avaliação do AWS Schema Conversion Tool (AWS SCT)
  - Usuário com privilégios suficientes para executar consultas SQL nas tabelas do dicionário do banco de dados Oracle
- Usuário do banco de dados para realizar a migração do banco de dados; por exemplo, um dos seguintes:
  - Usuário com privilégios suficientes para executar o AWS Database Migration Service (AWS DMS)

- Usuário com privilégios suficientes para realizar a exportação e importação do Oracle Data Pump
- Usuário com privilégios suficientes para executar o Oracle GoldenGate

Limitações

- O Amazon RDS para Oracle tem um tamanho máximo para banco de dados. Para obter mais informações, consulte Armazenamento de instâncias de banco de dados do Amazon RDS.

Versões do produto

A lógica geral descrita nesse documento se aplica às versões do Oracle a partir da 9i. Para ver as versões compatíveis dos bancos de dados autogerenciados e do Amazon RDS para Oracle, consulte a documentação do AWS DMS.

Para identificar o uso de atributo nos casos em que não há suporte ao AWS SCT , execute consultas SQL no banco de dados de origem. Para migrar de versões anteriores do Oracle em que o AWS DMS e o Oracle Data Pump não são compatíveis, use os utilitários de exportação e importação da Oracle.

Para obter uma lista atual das versões e edições compatíveis, consulte Oracle no Amazon RDS na documentação da AWS. Para obter detalhes sobre preços e classes de instâncias compatíveis, consulte Amazon RDS para Oracle Edition Enterprise Edition.

Arquitetura

Pilha de tecnologia de origem

- Oracle Database Enterprise Edition em execução no local ou na Amazon EC2

Pilha de tecnologias de destino usando ferramentas nativas da Oracle

- Amazon RDS for Oracle executando o Oracle Database SE2

1. Exporte dados usando o Oracle Data Pump.
2. Copie arquivos de despejo para o Amazon RDS por meio de um link de banco de dados.

3. Importe arquivos de despejo para o Amazon RDS usando o Oracle Data Pump.

Pilha de tecnologias de destino usando o AWS DMS

- Amazon RDS for Oracle executando o Oracle Database SE2
- AWS DMS

1. Exporte dados usando o Oracle Data Pump com FLASHBACK_SCN.
2. Copie arquivos de despejo para o Amazon RDS por meio de um link de banco de dados.
3. Importe arquivos de despejo para o Amazon RDS usando o Oracle Data Pump.
4. Use captura de dados de alteração (CDC) do AWS DMS.

Ferramentas

Serviços da AWS

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS. Esse padrão usa o Amazon RDS para Oracle.
- O AWS SCT fornece uma interface de usuário baseada em projetos para avaliar automaticamente, converter e copiar o esquema do banco de dados do seu banco de dados Oracle de origem em um formato compatível com o Amazon RDS para Oracle. O AWS SCT permite que você analise as economias de custo que podem ser obtidas alterando o tipo de licença do Oracle de Enterprise para Standard Edition. A seção License Evaluation and Cloud Support do relatório AWS SCT fornece informações detalhadas sobre os atributos da Oracle em uso para que você possa tomar uma decisão informada ao migrar para o Amazon RDS para Oracle.

Outras ferramentas

- Os utilitários nativos de importação e exportação da Oracle suportam mover dados da Oracle para dentro e para fora dos bancos de dados Oracle. A Oracle oferece dois tipos de utilitários de

importação e exportação de banco de dados: Original Export and Import (para versões anteriores) e Oracle Data Pump Export and Import (disponível no Oracle Database 10g versão 1 e superiores).

- GoldenGateA Oracle oferece recursos de replicação em tempo real para que você possa sincronizar seu banco de dados de destino após um carregamento inicial. Essa opção pode ajudar a reduzir o tempo de inatividade da aplicação durante a colocação em funcionamento no ambiente de produção.

Épicos

Faça uma avaliação pré-migração

Tarefa	Descrição	Habilidades necessárias
Valide os requisitos de banco de dados para seus aplicativos.	Garanta que seus aplicativos sejam certificados para execução no Oracle Database SE2. Consulte diretamente o fornecedor do software, desenvolvedor ou documentação de inscrição.	Desenvolvedor de aplicativos, DBA, proprietário do aplicativo
Investigue o uso dos atributos de EE diretamente no banco de dados.	Para determinar o uso do atributo EE, siga um destes procedimentos: • Gere um relatório de avaliação do AWS SCT para seu banco de dados Oracle EE. O relatório informa quais recursos do seu banco de dados de EE atual devem ser removidos se você quiser alterar os tipos de licença. • Se você tiver uma conta do Oracle Support, obtenha e execute o script `options_p`	Proprietário do aplicativo, DBA, desenvolvedor do aplicativo

Tarefa	Descrição	Habilidades necessárias
	`acks_usage_statistics.sql` no documento de suporte 1317265.1 para gerar um relatório de opções e atributos que estão sendo usados em seu banco de dados Oracle. • Consulte DBA_FEATURE_USAGE_STATISTICS para exibir detalhes de todos os atributos que estão em uso.	

Tarefa	Descrição	Habilidades necessárias
Identifique o uso dos atributos de EE para atividades operacionais.	Às vezes, os administr adores de bancos de dados ou aplicativos confiam em atributos exclusivos do EE para atividades operacionais. Exemplos comuns incluem atividades de manutenção on-line (recompilação de índice, movimentação de tabelas) e uso de paralelismo feitos por trabalhos em lote. Essas dependências podem ser mitigadas modificando suas operações sempre que possível. Identifique o uso desses atributos e tome uma decisão com base no custo comparado aos benefícios. Use a tabela Comparando o Oracle Database EE e os SE2 recursos como guia para identificar os recursos que estão disponíveis no Oracle Database SE2.	Desenvolvedor de aplicativos, DBA, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Analise os padrões de workload do banco de dados EE Oracle.	O Oracle Database restringe SE2 automaticamente o uso a um máximo de 16 threads de CPU a qualquer momento. Se seu banco de dados Oracle EE estiver licenciado para usar o Oracle Diagnosti c Pack, use a ferramenta Automatic Workload Repositor y (AWR) ou as visualizações DBA_HIST_* para analisar os padrões de carga de trabalho do banco de dados e determinar se o limite máximo de 16 threads de CPU afetará negativamente os níveis de serviço quando você fizer o downgrade para. SE2 Certifique-se de que sua avaliação abranja períodos de pico de atividade, como processamento de final de dia, mês ou ano.	Proprietário do aplicativ o, DBA, desenvolvedor do aplicativo

Prepare a infraestrutura de destino na AWS

Tarefa	Descrição	Habilidades necessárias
Implante e configure a infraestrutura de rede.	Crie uma nuvem privada virtual (VPC) e sub-redes, grupos de segurança e listas de controle de acesso à rede.	Administrador da AWS, arquiteto de nuvem, administr ador de rede, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Provisione o banco de dados Amazon RDS for SE2 Oracle.	Provisione o banco de dados de destino do Amazon RDS SE2 for Oracle para atender aos requisitos de desempenho, disponibi lidade e segurança de seus aplicativos. Recomendamos a configuração do Multi-AZ para workloads de produção. No entanto, para melhorar o desempenho da migração, você pode adiar a ativação do Multi-AZ para depois da migração dos dados.	Administrador de nuvem, arquiteto de nuvem, DBA, DevOps engenheiro, administr ador da AWS
Personalize o ambiente do Amazon RDS.	Configure parâmetros e opções personalizados e ative o monitoramento adicional. Para obter mais informações, consulte Práticas recomenda das de migração para o Amazon RDS para Oracle.	Administrador da AWS, administrador de sistemas da AWS, administrador de nuvem, DBA, arquiteto de nuvem

Execute a migração, o dry run e o teste do aplicativo

Tarefa	Descrição	Habilidades necessárias
Migre os dados (dry run).	Migre dados do banco de dados Oracle EE de origem para a instância do banco de dados Amazon RDS for SE2 Oracle usando a abordagem mais adequada ao seu ambiente específic	DBA

Tarefa	Descrição	Habilidades necessárias
	o. Selecione uma estratégi a de migração com base em fatores como tamanho, complexidade e a janela de tempo de inatividade disponível. Use um ou uma combinação do seguinte: • Ferramentas nativas da Oracle, como Oracle Data Pump (recomendado), utilitários Oracle Import-Ex port e Oracle. GoldenGate • AWS DMS, usando a carga completa com replicação contínua por meio do CDC.	
Valide o banco de dados de destino.	Execute a validação pós-migração do armazenamento do banco de dados e dos objetos de código. Reveja os registros de migração e corrija os problemas identificados. Para obter mais informaçõ es, consulte o guia Migrar bancos de dados Oracle para a Nuvem AWS.	DBA

Tarefa	Descrição	Habilidades necessárias
Teste os aplicativos.	Os administradores de aplicativos e bancos de dados devem realizar testes funcionais, de desempenho e operacionais, conforme apropriado. Para obter mais informações, consulte Práticas recomendadas de migração para o Amazon RDS para Oracle. Por fim, obtenha a aprovação dos resultados dos testes das partes interessadas.	Desenvolvedor de aplicativos, proprietário do aplicativo, DBA, engenheiro de migração, líder de migração

Substituir

Tarefa	Descrição	Habilidades necessárias
Atualize os dados do Oracle Database EE.	Selecione uma abordagem de atualização de dados com base no requisito de disponibilidade do aplicativo. Para obter mais informações, consulte os métodos de migração em Estratégias para migrar bancos de dados Oracle para a AWS. Por exemplo, você pode alcançar um tempo de inatividade quase zero usando ferramentas como Oracle ou GoldenGate AWS DMS com replicação contínua. Se a	Proprietário do aplicativo, líder de substituição, DBA, engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	janela de tempo de inatividade permitir, você poderá realizar a substituição final de dados usando métodos off-line, como o Oracle Data Pump ou o Original Export-Import.	
Aponte os aplicativos para a instância de banco de dados de destino.	Atualize os parâmetros de conexão em aplicativos e outros clientes para apontar para o banco de dados Amazon RDS for SE2 Oracle.	Desenvolvedor de aplicativos, proprietário do aplicativo, engenheiro de migração, líder de migração, líder de substituição
Realize as atividades pós-migração	Execute tarefas pós-migração de dados, como habilitar o Multi-AZ, validação de dados e outras verificações.	DBA, Engenheiro de migração
Realize o monitoramento pós-substituição.	Use ferramentas como Amazon CloudWatch e Amazon RDS Performance Insights para monitorar o banco de dados Amazon RDS for SE2 Oracle.	Desenvolvedor do aplicativo, proprietário do aplicativo, administrador da AWS, DBA, engenheiro de migração

Recursos relacionados

Recomendações da AWS

- Migrar bancos de dados Oracle para a Nuvem AWS (guia)
- Avaliar o downgrade dos bancos de dados Oracle para o Standard Edition 2 na AWS (guia)
- Migrate an on-premises Oracle database to Amazon RDS para Oracle (padrão)
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump (modelo)

Publicações no blog

- Migração de bancos de dados Oracle com tempo de inatividade quase zero usando o AWS DMS
- Analisar o gerenciamento de performance no Oracle SE usando o Amazon RDS para Oracle
- Gerenciar o plano de SQL no Oracle SE com o Amazon RDS para Oracle
- Implementar o particionamento de tabelas no Oracle Standard Edition: Parte 1

Replique bancos de dados de mainframe para AWS usando o Precisely Connect

Criado por Lucio Pereira (AWS), Balaji Mohan (AWS) e Sayantan Giri (AWS)

Resumo

Esse padrão descreve as etapas para replicar dados de bancos de dados de mainframe para armazenamentos de dados da Amazon quase em tempo real usando o Precisely Connect. O padrão usa uma arquitetura baseada em eventos com o Amazon Managed Streaming for Apache Kafka (Amazon MSK) e conectores de banco de dados personalizados para melhorar a escalabilidade, a resiliência e o desempenho.

O Precisely Connect é uma ferramenta de replicação que captura dados de sistemas de mainframe legados e os integra a ambientes de nuvem. Os dados são replicados dos mainframes para a AWS por meio da captura de dados de alteração (CDC) usando fluxos de mensagens quase em tempo real com pipelines de dados heterogêneos de baixa latência e alto throughput.

Esse padrão também abrange uma estratégia de recuperação de desastres para pipelines de dados resilientes com replicação de dados em várias regiões e roteamento por failover.

Pré-requisitos e limitações

Pré-requisitos

- Um banco de dados de mainframe existente — por exemplo, IBM DB2, IBM Information Management System (IMS) ou Virtual Storage Access Method (VSAM) — que você deseja replicar para a nuvem da AWS
- Uma conta AWS ativa
- AWS Direct Connect ou AWS Virtual Private Network (AWS VPN) do seu ambiente corporativo para a AWS
- Uma nuvem privada virtual com uma sub-rede que pode ser acessada por sua plataforma legada

Arquitetura

Pilha de tecnologia de origem

Um ambiente de mainframe que inclua pelo menos um dos seguintes bancos de dados:

- Banco de dados IBM IMS
- Banco de DB2 dados IBM
- Arquivos VSAM

Pilha de tecnologias de destino

- Amazon MSK
- Amazon Elastic Kubernetes Service (Amazon EKS) e Amazon EKS Anywhere
- Docker
- Um banco de dados relacional ou NoSQL da AWS, como o seguinte:
  - Amazon DynamoDB
  - Amazon Relational Database Service (Amazon RDS) para Oracle, Amazon RDS para PostgreSQL ou Amazon Aurora
  - Amazon ElastiCache para Redis
  - Amazon Keyspaces (para Apache Cassandra)

Arquitetura de destino

Replicação de dados de mainframe para bancos de dados da AWS

O diagrama a seguir ilustra a replicação de dados de mainframe em um banco de dados da AWS, como DynamoDB, Amazon RDS, Amazon ou Amazon Keyspaces. ElastiCache A replicação ocorre quase em tempo real usando o Precisely Capture and Publisher em seu ambiente de mainframe on-premises, o Precisely Dispatcher no Amazon EKS Anywhere em seu ambiente distribuído on-premises e os conectores de banco de dados e do Precisely Apply Engine na nuvem AWS.

O diagrama mostra o seguinte fluxo de trabalho:

1. O Precisely Capture obtém dados do mainframe dos logs do CDC e mantém os dados em armazenamento temporário interno.
2. O Precisely Publisher recebe as alterações no armazenamento de dados interno e envia os registros do CDC para o Precisely Dispatcher por meio de uma conexão TCP/IP.
3. O Precision Dispatcher recebe os registros do CDC do Publisher e os envia para o Amazon MSK. O Dispatcher cria chaves Kafka com base na configuração do usuário e em várias tarefas

de trabalho para enviar dados paralelamente. O Dispatcher envia uma confirmação de volta ao Publisher quando os registros são armazenados no Amazon MSK.

4. O Amazon MSK mantém os registros do CDC no ambiente de nuvem. O tamanho da partição dos tópicos depende dos requisitos do sistema de processamento de transações (TPS) para throughput. A chave Kafka é obrigatória para futuras transformações e pedidos de transações.
5. O Precisely Apply Engine recebe os registros do CDC do Amazon MSK e transforma os dados (por exemplo, filtrando ou mapeando) com base nos requisitos do banco de dados de destino. Você pode adicionar lógica personalizada aos scripts Precisamente SQD. (SQD é a linguagem proprietária do Precisely.) O Precised Apply Engine transforma cada registro do CDC no formato Apache Avro ou JSON e o distribui para diferentes tópicos com base em seus requisitos.
6. Os tópicos de destino do Kafka mantêm registros do CDC em vários tópicos com base no banco de dados de destino, e o Kafka facilita a ordenação de transações com base na chave definida do Kafka. As chaves de partição se alinham com as partições correspondentes para suportar um processo sequencial.
7. Os conectores de banco de dados (aplicativos Java personalizados) recebem os registros CDC do Amazon MSK e os armazenam no banco de dados de destino.
8. Você pode selecionar um banco de dados de destino dependendo das suas necessidades. Esse padrão é compatível com bancos de dados relacionais e NoSQL .

Recuperação de desastres

A continuidade dos negócios é fundamental para o sucesso da organização. A nuvem AWS fornece recursos para alta disponibilidade (HA) e recuperação de desastres (DR), além de oferecer suporte aos planos de failover e fallback da sua organização. Esse padrão segue uma estratégia de DR ativa/passiva e fornece orientação de alto nível para implementar uma estratégia de DR que atenda aos seus requisitos de RTO e RPO.

O diagrama a seguir mostra o fluxo de trabalho do DR.

O diagrama mostra o seguinte:

1. Um failover semiautomático é necessário se ocorrer alguma falha na Região da AWS 1. No caso de falha na Região 1, o sistema deve iniciar as alterações de roteamento para conectar o Precisely Dispatcher à Região 2.
2. O Amazon MSK replica dados por meio de espelhamento entre regiões. Por esse motivo, durante o failover, o cluster Amazon MSK na Região 2 precisa ser promovido como líder principal.

3. O Precisely Apply Engine e os conectores de banco de dados são aplicativos sem estado que podem funcionar em qualquer região.
4. A sincronização do banco de dados depende do banco de dados de destino. Por exemplo, o DynamoDB pode usar tabelas globais ElastiCache e pode usar datastores globais.

Processamento de baixa latência e alto throughput por meio de conectores de banco de dados

Os conectores de banco de dados são componentes essenciais nesse padrão. Os conectores seguem uma abordagem baseada em receptores para coletar dados do Amazon MSK e enviar transações para o banco de dados por meio de processamento de alto throughput e baixa latência para aplicativos de missão crítica (níveis 0 e 1). O diagrama a seguir ilustra esse processo.

Esse padrão é compatível com o desenvolvimento de um aplicativo personalizado com consumo de thread único por meio de um mecanismo de processamento multithread.

1. O encadeamento principal do conector consome registros CDC do Amazon MSK e os envia ao pool de encadeamentos para processamento.
2. Os encadeamentos do pool de encadeamentos processam os registros do CDC e os enviam para o banco de dados de destino.
3. Se todos os encadeamentos estiverem ocupados, os registros do CDC serão mantidos em espera pela fila de encadeamentos.
4. O encadeamento principal espera que todos os registros sejam apagados da fila de encadeamentos e confirma os deslocamentos no Amazon MSK.
5. Os tópicos secundários lidam com falhas. Se ocorrerem falhas durante o processamento, as mensagens com falha serão enviadas para o tópico DLQ (fila de mensagens não entregues).
6. Os threads secundários iniciam atualizações condicionais (consulte Expressões de condição na documentação do DynamoDB), com base no timestamp do mainframe, para evitar duplicações ou atualizações no banco de dados. out-of-order

Para obter informações sobre como implementar um aplicativo de consumidor do Kafka com recursos de múltiplos encadeamentos, consulte a postagem do blog Consumo de mensagens com múltiplos encadeamentos com o consumidor Apache Kafka no site do Confluent.

Ferramentas

Serviços da AWS

- O Amazon Managed Streaming for Apache Kafka (Amazon MSK) é um serviço totalmente gerenciado que ajuda você a criar e executar aplicações que usam o Apache Kafka para processar dados em streaming.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem ter que instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- O Amazon EKS Anywhere ajuda você a implantar, usar e gerenciar clusters Kubernetes que são executados em seus próprios datacenters.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- ElastiCacheA Amazon ajuda você a configurar, gerenciar e escalar ambientes distribuídos de cache na memória na nuvem da AWS.
- O Amazon Keyspaces (para Apache Cassandra) é um serviço de banco de dados gerenciado que ajuda você a migrar, executar e escalar suas workloads do Cassandra na nuvem AWS.

Outras ferramentas

- O Precisely Connect integra dados de sistemas de mainframe antigos, como conjuntos de dados VSAM ou bancos de dados de mainframe IBM, às plataformas de nuvem e dados da próxima geração.

Práticas recomendadas

- Encontrar a melhor combinação de partições Kafka e conectores com múltiplos encadeamentos para equilibrar desempenho e custo ideais. Várias instâncias do Precisely Capture and Dispatcher podem aumentar o custo devido ao maior consumo de MIPS (milhões de instruções por segundo).
- Evitar adicionar lógica de manipulação e transformação de dados aos conectores do banco de dados. Para isso, use o Precisely Apply Engine, que fornece tempos de processamento em microssegundos.
- Crie chamadas periódicas de solicitação ou verificação de integridade para o banco de dados (pulsações) nos conectores do banco de dados para aquecer a conexão com frequência e reduzir a latência.

- Implemente a lógica de validação do pool de encadeamentos para entender as tarefas pendentes na fila de encadeamentos e aguarde a conclusão de todos os threads antes da próxima pesquisa do Kafka. Isso ajuda a evitar a perda de dados se um nó, contêiner ou processo falhar.
- Exponha métricas de latência por meio de endpoints de integridade para aprimorar os recursos de observabilidade por meio de painéis e mecanismos de rastreamento.

Épicos

Preparar o ambiente de origem (on-premises)

Tarefa	Descrição	Habilidades necessárias
Configurar o processo de mainframe (utilitário em lote ou on-line) para iniciar o processo CDC a partir de bancos de dados de mainframe.	1. Identificar o ambiente de mainframe. 2. Identificar os bancos de dados de mainframe que estarão envolvidos no processo do CDC. 3. No ambiente de mainframe , desenvolva um processo que inicie a ferrament a CDC para capturar alterações no banco de dados de origem. Para obter instruções, consulte a documentação do seu mainframe. 4. Documentar o processo do CDC, incluindo a configura ção. 5. Implantar o processo em ambientes de teste e produção.	Engenheiro de mainframe

Tarefa	Descrição	Habilidades necessárias
Ativar os fluxos de log do banco de dados de mainframe .	1. Configurar fluxos de log no ambiente de mainframe para capturar logs do CDC. Para obter instruções, consulte a documentação do seu mainframe. 2. Testar os fluxos de logs para garantir que eles capturem os dados necessários. 3. Implantar os fluxos de log em ambientes de teste e produção.	Especialista em banco de dados de mainframe

Tarefa	Descrição	Habilidades necessárias
Usar o componente Capturar para capturar registros do CDC.	1. Instalar e configurar o componente Precisely Capture no ambiente de mainframe. Para obter instruções, consulte a Documentação do Precisely . 2. Testar a configuração para garantir que o componente Capture funcione corretamente. 3. Configurar um processo de replicação para replicar os registros CDC capturados por meio do componente Capture. 4. Documentar a configuração do Capture para cada banco de dados de origem. 5. Desenvolver um sistema de monitoramento para garantir que o componente Capture colete os logs adequadamente ao longo do tempo. 6. Implantar a instalação e as configurações nos ambientes de teste e produção.	Engenheiro de mainframe, Precisely Connect SME

Tarefa	Descrição	Habilidades necessárias
Configurar o componente Publisher para receber o componente Capture.	1. Instalar e configurar o componente Precisely Publisher no ambiente de mainframe. Para obter instruções, consulte a Documentação do Precisely . 2. Testar a configuração para garantir que o component e Publisher funcione corretamente. 3. Configurar um processo de replicação para publicar os registros do CDC no componente Precisely Dispatcher do Publisher. 4. Documentar a configuração do Publisher. 5. Desenvolver um sistema de monitoramento para garantir que o component e Publisher funcione adequadamente ao longo do tempo. 6. Implantar a instalação e as configurações nos ambientes de teste e produção.	Engenheiro de mainframe, Precisely Connect SME

Tarefa	Descrição	Habilidades necessárias
Provisionar o Amazon EKS Anywhere no ambiente distribuído on-premises.	1. Instale o Amazon EKS Anywhere na infraestrutura on-premises e verifique se ela está configurada corretamente. Para obter instruções, consulte a documentação do Amazon EKS Anywhere. 2. Configurar um ambiente de rede seguro para o cluster Kubernetes, incluindo firewalls. 3. Implementar e testar a implantação do aplicativ o de amostra no cluster Amazon EKS Anywhere. 4. Implementar recursos de escalabilidade automática para o cluster. 5. Desenvolver e implementar procedimentos de backup e recuperação de desastres.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Implantar e configurar o componente Dispatcher no ambiente distribuído para publicar os tópicos na Nuvem AWS.	1. Configurar e colocar em contêineres o componente Precisely Dispatcher. Para obter instruções, consulte a Documentação do Precisely . 2. Implantar a imagem do Docker no ambiente on-premises do Amazon EKS Anywhere. 3. Configurar uma conexão segura entre a nuvem AWS e o Dispatcher. 4. Desenvolver um sistema de monitoramento para garantir que o component e Dispatcher funcione adequadamente ao longo do tempo. 5. Implantar a instalação e as configurações nos ambientes de teste e produção.	DevOps engenheiro, Precisely Connect SME

Preparar o ambiente de destino (AWS)

Tarefa	Descrição	Habilidades necessárias
Provisionar um cluster Amazon EKS na região da AWS designada.	1. Fazer login na sua conta AWS e configurá-la para garantir que as permissõe s necessárias estejam em	DevOps engenheiro, administr ador de rede

Tarefa	Descrição	Habilidades necessárias
	vigor para criar e gerenciar o cluster Amazon EKS. 2. Criar sua nuvem privada virtual (VPC) e sub-redes na região da AWS selecionada. Para obter instruções, consulte a Documentação do Amazon EKS. 3. Criar e configurar os grupos de segurança de rede necessários para permitir a comunicação entre o cluster do Amazon EKS e outros recursos na VPC. Para obter mais informações, consulte a documentação do Amazon EKS. 4. Criar o cluster Amazon EKS e configurá-lo com o tamanho correto do grupo de nós e os tipos de instância. 5. Validar o cluster Amazon EKS implantando um aplicativo de amostra.	

Tarefa	Descrição	Habilidades necessárias
Provisionar um cluster MSK e configurar os tópicos aplicáveis do Kafka.	1. Configurar sua conta AWS para garantir que as permissões necessárias estejam em vigor para criar e gerenciar o cluster MSK. 2. Criar e configurar os grupos de segurança de rede necessários para permitir a comunicação entre o cluster MSK e outros recursos na VPC. Para obter mais informações, consulte a documentação da Amazon VPC. 3. Criar o cluster MSK e configurá-lo para incluir os tópicos do Kafka que serão usados pelo aplicativo. Para obter mais informações, consulte a documentação do Amazon MSK.	DevOps engenheiro, administrador de rede

Tarefa	Descrição	Habilidades necessárias
Configurar o componente Apply Engine para ser receptor dos tópicos replicados do Kafka.	1. Configurar e conteinerizar o componente Precisely Apply Engine. 2. Implantar a imagem do Docker do Apply Engine no cluster Amazon EKS em sua conta AWS. 3. Configurar o Apply Engine para ouvir os tópicos do MSK. 4. Desenvolver e configurar um script SQD no Apply Engine para lidar com a filtragem e a transformação. Para obter mais informações, consulte a Documentação do Precisely. 5. Implantar o Apply Engine em ambientes de teste e produção.	Conectar PME com precisão

Tarefa	Descrição	Habilidades necessárias
Provisionar instâncias de banco de dados na nuvem AWS	1. Configurar sua conta AWS para garantir que as permissões necessári as estejam em vigor para criar e gerenciar clusters e tabelas de banco de dados. Para obter instruçõe s, consulte a documenta ção da AWS para o serviço de banco de dados da AWS que você deseja usar. (Consulte a seção Recursos para obter links). 2. Criar sua VPC e sub-redes na região da AWS selecionada. 3. Criar e configurar os grupos de segurança de rede necessários para permitir a comunicação entre as instâncias de banco de dados e outros recursos na VPC. 4. Criar os bancos de dados e configurá-los para incluir as tabelas que o aplicativo usará. 5. Projetar e validar os esquemas do banco de dados.	Engenheiro de dados, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Configurar e implantar conectores de banco de dados para receber os tópicos publicados pelo Apply Engine.	1. Criar conectores de banco de dados para conectar os tópicos do Kafka aos bancos de dados da AWS que você criou nas etapas anteriores. 2. Desenvolver os conectores com base no banco de dados de destino. 3. Configurar os conectores para receber os tópicos do Kafka publicados pelo Apply Engine. 4. Implantar os conectores no cluster Amazon EKS.	Desenvolvedor de aplicativos, arquiteto de nuvem, engenheiro de dados

Configurar a continuidade dos negócios e a recuperação de desastres

Tarefa	Descrição	Habilidades necessárias
Definir metas de recuperação de desastres para seus aplicativos de negócios.	1. Definir as metas de RPO e RTO para pipelines de CDC com base nas necessidades de seus negócios e na análise de impacto. 2. Definir os procedimentos de comunicação e notificação para garantir que todas as partes interessadas estejam cientes do plano de recuperação de desastres. 3. Determinar o orçamento e os recursos necessári	Arquiteto de nuvem, engenheiro de dados, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	os para implementar o plano de recuperação de desastres. 4. Documentar as metas de recuperação de desastres, incluindo as metas de RPO e RTO.	
Criar estratégias de recuperação de desastres com base em RTO/RPO definido.	1. Determinar as estratégias de recuperação de desastres mais apropriadas para pipelines de CDC com base em seus requisitos de criticidade e recuperação. 2. Definir a arquitetura e a topologia da recuperação de desastres. 3. Definir os procedimentos de failover e failback para pipelines do CDC para garantir que eles possam ser transferidos de forma rápida e perfeita para a região de backup. 4. Documentar as estratégias e procedimentos de recuperação de desastres e garanta que todas as partes interessadas tenham uma compreensão clara do projeto.	Arquiteto de nuvem, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
Provisionar clusters e configurações de recuperação de desastres.	1. Provisionar uma região da AWS secundária para recuperação de desastres. 2. Na região da AWS secundária, crie um ambiente idêntico à região da AWS primária. 3. Configure o Apache Kafka MirrorMaker entre as regiões primária e secundária. Para obter mais informações, consulte a documentação do Amazon MSK. 4. Configurar aplicativos em espera na região secundária. 5. Configurar replicações de banco de dados entre as regiões primária e secundária.	DevOps engenheiro, administrador de rede, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Testar o pipeline do CDC para recuperação de desastres.	1. Definir o escopo e os objetivos do teste de recuperação de desastres para o pipeline do CDC, incluindo os cenários de teste e o RTO a serem alcançados. 2. Identificar o ambiente de teste e a infraestrutura para realizar o teste de recuperação de desastres. 3. Preparar os conjuntos de dados de teste e o script para simular cenários de falha. 4. Verificar a integridade e a consistência dos dados para garantir que não haja perda de dados.	Proprietário do aplicativo, engenheiro de dados, arquiteto de nuvem

Recursos relacionados

Recursos da AWS

- Amazon DynamoDB
- Expressões condicionais com o Amazon DynamoDB
- Amazon EKS
- Amazon EKS Anywhere
- Amazon ElasticCache
- Amazon Keyspaces
- Amazon MSK
- Amazon RDS e Amazon Aurora

- Amazon VPC

Conecte recursos com precisão

- Visão geral do Precisely Connect
- Captura de dados de alteração com o Precie Connect

Recursos confluentes

- Consumo de mensagens com múltiplos encadeamentos com o Apache Kafka Consumer

Agendar trabalhos para o Amazon RDS para PostgreSQL e Aurora PostgreSQL usando o Lambda e o Secrets Manager

Criado por Yaser Raja (AWS)

Resumo

Para bancos de dados locais e bancos de dados hospedados em instâncias do Amazon Elastic Compute Cloud EC2 (Amazon), os administradores de banco de dados geralmente usam o utilitário cron para agendar trabalhos.

Por exemplo, um trabalho para extração de dados ou um trabalho para limpeza de dados pode ser facilmente agendado usando o cron. Para esses trabalhos, as credenciais do banco de dados geralmente passam por codificação rígida ou são armazenadas em um arquivo de propriedades. No entanto, ao migrar para o Amazon Relational Database Service (Amazon RDS) ou edição compatível do Amazon Aurora PostgreSQL, você perde a capacidade de fazer login na instância host para agendar tarefas cron.

Esse padrão descreve como usar AWS Lambda e programar trabalhos para AWS Secrets Manager o Amazon RDS for PostgreSQL e bancos de dados compatíveis com o Aurora PostgreSQL após a migração.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um banco de dados compatível com Amazon RDS para PostgreSQL ou Aurora compatível com PostgreSQL

Limitações

- Um trabalho deve ser concluído em 15 minutos, que é o limite do tempo limite da função do Lambda. Para outros limites, consulte a AWS Lambda documentação.
- O código do trabalho deve ser escrito em uma linguagem compatível com o Lambda.

Arquitetura

Pilha de tecnologia de origem

Essa pilha apresenta trabalhos escritos em linguagens como Bash, Python e Java. As credenciais do banco de dados são armazenadas no arquivo de propriedades e o trabalho é agendado usando o Linux cron.

Pilha de tecnologias de destino

Essa pilha tem uma função do Lambda que usa as credenciais armazenadas no Secrets Manager para se conectar ao banco de dados e realizar a atividade. A função Lambda é iniciada no intervalo programado usando o Amazon CloudWatch Events.

Arquitetura de destino

Ferramentas

- A Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. Usando regras simples que você pode configurar rapidamente, você pode combinar eventos e roteá-los para uma ou mais funções ou fluxos de destino. CloudWatch Os eventos ficam cientes das mudanças operacionais à medida que elas ocorrem. Ele responde a essas alterações operacionais e executa a ação corretiva conforme necessário, enviando mensagens para responder ao ambiente, ativando funções, fazendo alterações e capturando informações de estado. Você também pode usar CloudWatch Eventos para programar ações automatizadas que se iniciam automaticamente em determinados momentos usando expressões cron ou rate.
- O AWS Lambda é um serviço de computação que permite executar código sem o provisionamento ou gerenciamento de servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga somente pelo tempo de computação utilizado; não haverá cobrança quando seu código não estiver em execução. Com o Lambda, você pode executar código para praticamente qualquer tipo de aplicativo ou serviço de back-end sem nenhuma administração. O Lambda executa seu código em uma infraestrutura computacional de alta disponibilidade e gerencia todos os recursos computacionais, incluindo manutenção do servidor e do sistema operacional, provisionamento de capacidade e escalabilidade automática, monitoramento de código e registro. Tudo o que você precisa fazer é fornecer seu código em uma das linguagens suportadas pelo Lambda.
- AWS Secrets Managerajuda você a proteger segredos para acessar seus aplicativos, serviços e recursos de TI. Você pode alternar, gerenciar e recuperar facilmente credenciais de banco de dados, chaves de API e outros segredos durante seu ciclo de vida. Usuários e aplicativos recuperam segredos chamando o Secrets Manager APIs, o que elimina a necessidade de codificar

informações confidenciais em texto simples. O Secrets Manager oferece alternância secreta com integração embutida para o Amazon RDS, o Amazon Redshift e o Amazon DocumentDB. O serviço é extensível a outros tipos de segredos, incluindo chaves e OAuth tokens de API. O Secrets Manager permite que você controle o acesso a segredos usando permissões refinadas e audite centralmente a rotação de segredos em busca de recursos nos serviços de terceiros e no Nuvem AWS local.

Épicos

Credenciais de banco de dados no Secrets Manager

Tarefa	Descrição	Habilidades necessárias
Crie um usuário de banco de dados para a função do Lambda.	É uma boa prática usar usuários de banco de dados separados para diferentes partes do seu aplicativo. Se já existir um usuário de banco de dados separado para seus trabalhos cron, use-o. Caso contrário, crie um novo usuário de banco de dados. Para obter mais informaçõ es, consulte Gerencian do usuários e funções do PostgreSQLAWS (postagem no blog).	DBA
Armazene as credenciais de banco de dados como um segredo no Secrets Manager	Siga as instruções em Criação de um segredo de banco de dados do AWS Secrets Manager (documentação do Secrets Manager).	DBA, DevOps

Crie o código da função do Lambda.

Tarefa	Descrição	Habilidades necessárias
Escolha uma linguagem de programação compatível com o Lambda.	Para obter uma lista das linguagens compatíveis, consulte os Runtimes do Lambda (documentação do Lambda).	Desenvolvedor
Escreva a lógica para buscar as credenciais do banco de dados no Secrets Manager.	Para ver um exemplo de código, consulte Como fornecer com segurança as credenciais do banco de dados às funções do Lambda usando AWS Secrets Manager (postagem do blog).AWS	Desenvolvedor
Grave a lógica para realizar a atividade agendada do banco de dados.	Migre seu código existente para o trabalho de agendamento que você está usando no local para a função Lambda. Para obter mais informações, consulte Implantar funções do Lambda (documentação do Lambda).	Desenvolvedor

Implante o código e crie a função do Lambda.

Tarefa	Descrição	Habilidades necessárias
Crie o pacote de implantação da função do Lambda.	Esse pacote contém o código e suas dependências. Para obter mais informações, consulte Pacotes de	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	implantação (documentação do Lambda).	
Criar a função do Lambda.	No console Lambda, escolha Criar função, insira um nome de função, escolha o ambiente de tempo de execução e, em seguida, escolha Criar função.	DevOps
Faça upload do pacote de implantação.	Escolha a função do Lambda que você criou para abrir sua configuração. Você pode gravar seu código diretamente na seção de código ou fazer o upload do seu pacote de implantação. Para carregar seu pacote, acesse a seção Código do perfil, escolha o Tipo de entrada de código para carregar um arquivo .zip e selecione o pacote.	DevOps
Configure a função do Lambda de acordo com seus requisitos.	Por exemplo, você pode definir o parâmetro de Tempo limite para a duração que você espera que sua função do Lambda dure. Para obter mais informações, consulte Configurar as opções da função do Lambda (documentação do Lambda).	DevOps

Tarefa	Descrição	Habilidades necessárias
Defina permissões para o perfil da função do Lambda para acessar o Secrets Manager.	Para obter instruções, consulte Usar segredos em AWS Lambda funções (documentação do Secrets Manager).	DevOps
Testar a função do Lambda.	Inicie a função Lambda manualmente para garantir que ela funcione conforme o esperado.	DevOps

Programe a função Lambda usando Eventos CloudWatch

Tarefa	Descrição	Habilidades necessárias
Crie uma regra para executar a função do Lambda em uma programação.	Agende a função Lambda usando CloudWatch Eventos. Para obter instruções, consulte Programar funções do Lambda usando CloudWatch eventos (tutorial de CloudWatch eventos).	DevOps

Recursos relacionados

- AWS Secrets Manager
- Conceitos básicos do Lambda
- Criando uma regra de CloudWatch eventos que é acionada em um evento
- AWS Lambda Limites
- Consulte seu AWS banco de dados a partir do seu aplicativo sem servidor (postagem no blog)

Envie notificações para uma instância de banco de dados Amazon RDS para SQL Server usando um servidor SMTP on-premises e o Database Mail

Criado por Nishad Mankar (AWS)

Resumo

O Database Mail (documentação da Microsoft) envia mensagens de e-mail, como notificações ou alertas, de um banco de dados do Microsoft SQL Server usando um servidor SMTP (Simple Mail Transfer Protocol). A documentação do Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server fornece instruções para usar o Amazon Simple Email Service (Amazon SES) como servidor SMTP para o Database Mail. Para ter mais informações, consulte Usar o Database Mail no Amazon RDS para SQL Server. Como configuração alternativa, esse padrão explica como configurar o Database Mail para enviar e-mails de uma instância de banco de dados (DB) do Amazon RDS para SQL Server usando um servidor SMTP on-premises como servidor de e-mail.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância de banco de dados do Amazon RDS executando uma edição Standard ou Enterprise do SQL Server
- O endereço IP ou nome do host do servidor SMTP on-premises.
- Uma regra de grupo de segurança de entrada que permite conexões com a instância de banco de dados Amazon RDS para SQL Server a partir do endereço IP do servidor SMTP
- Uma conexão, como uma conexão do AWS Direct Connect, entre sua rede on-premises e a nuvem privada virtual (VPC) que contém a instância de banco de dados Amazon RDS

Limitações

- Não há suporte para edições Express do SQL Server.
- Para obter mais informações sobre limitações, consulte Limitações no uso do Database Mail no Amazon RDS para SQL Server na documentação do Amazon RDS.

Versões do produto

- Edições Standard e Enterprise das versões do SQL Server suportadas no RDS

Arquitetura

Pilha de tecnologias de destino

- Instância de banco de dados do Amazon RDS para SQL Server
- Regra de redirecionamento do Amazon Route 53
- Correspondência de banco de dados
- Servidor SMTP no on-premises
- Microsoft SQL Server Management Studio (SSMS)

Arquitetura de destino

A imagem a seguir mostra a arquitetura de destino para esse padrão. Quando ocorre um evento ou ação que inicia uma notificação ou alerta sobre a instância do banco de dados, o Amazon RDS para SQL Server usa o Database Mail para enviar uma notificação por e-mail. O Database Mail usa o servidor SMTP on-premises para enviar o e-mail.

Ferramentas

Serviços da AWS

- O Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server ajuda você a configurar, operar e escalar um banco de dados relacional do SQL Server na Nuvem AWS.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.

Outras ferramentas

- O Database Mail é uma ferramenta que envia mensagens de email, como notificações e alertas, do Mecanismo de Banco de Dados do SQL Server para os usuários.
- O Microsoft SQL Server Management Studio (SSMS) é uma ferramenta para gerenciar o SQL Server, incluindo acesso, configuração e administração de componentes do SQL Server. Nesse padrão, você usa o SSMS para executar os comandos SQL para configurar o Database Mail em uma instância de banco de dados Amazon RDS para SQL Server.

Épicos

Habilite a conectividade de rede com o servidor SMTP on-premises

Tarefa	Descrição	Habilidades necessárias
Remover Multi-AZ da instância de banco de dados do RDS.	Se você estiver usando uma instância de banco de dados do Multi-Zone, converta a instância Multi-AZ em uma instância Single-AZ. Ao terminar de configurar o Database Mail, você converterá a instância de banco de dados de volta para uma implantação Multi-AZ. A configuração do Database Mail funciona, então, nos nós primário e secundário. Para obter instruções, consulte Remover multi-AZ de uma instância de banco de dados do Microsoft SQL Server.	DBA
Crie uma lista de permissões para o endpoint ou endereço IP do Amazon RDS no servidor SMTP on-premises.	O servidor SMTP está fora da rede da AWS. No servidor SMTP local, crie uma lista de permissões que permita que o servidor se comunique com o endpoint de saída ou o endereço IP da instância do Amazon RDS ou da instância do Amazon Elastic Compute Cloud (Amazon EC2) hospedada no Amazon RDS. Esse procedimento varia de organização para	DBA

Tarefa	Descrição	Habilidades necessárias
	organização. Para obter mais informações sobre o endpoint da instância de banco de dados, consulte Como encontrar o endpoint da instância de banco de dados e o número da porta.	

Tarefa	Descrição	Habilidades necessárias
Remova as restrições da porta 25.	Por padrão, a AWS restringe a porta 25 nas EC2 instâncias. Para remover a restrição da porta 25, faça o seguinte: 1. Faça login com sua conta da AWS e, em seguida, abra o Formulário Solicitação para remover limitações de envio de e-mail. 2. Insira seu endereço de e-mail para que o AWS Support possa entrar em contato com você com atualizações sobre sua solicitação. 3. Forneça as informações necessárias no campo Descrição do caso de uso. 4. Selecione Enviar. **Note** • Se você tiver instâncias em mais de uma região da AWS, envie uma solicitação separada para cada região. • Pode levar até 48 horas para que sua solicitação seja processada.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Adicione uma regra do Route 53 para resolver consultas de DNS para o servidor SMTP.	Use o Route 53 para resolver consultas ao DNS entre seus recursos da AWS e o servidor SMTP on-premises. Você deve criar uma regra que encaminhe as consultas de DNS para o domínio do servidor SMTP, como `example.com` . Para obter instruções, consulte Criação de regras de encaminhamento na documentação do Route 53.	Administrador de rede

Configurar o Database Mail na instância de banco de dados do Amazon RDS para SQL Server

Tarefa	Descrição	Habilidades necessárias
Habilite o Database Mail.	Crie um grupo de parâmetros para o Database Mail, defina o parâmetro `database mail xps` como 1 e associe o grupo de parâmetros do Database Mail à instância de banco de dados RDS de destino. Para obter instruções, consulte Habilitando o Database Mail na documentação do Amazon RDS. Não vá para a seção Configurando o Database Mail nestas instruções. A configuração do servidor SMTP on-premises é diferente da do Amazon SES.	DBA

Tarefa	Descrição	Habilidades necessárias
Conecte-se à instância de banco de dados.	Em um Bastion Host, use o Microsoft SQL Server Management Studio (SSMS - Microsoft SQL Server Management Studio) para conectar-se à instância de banco de dados do Amazon RDS para SQL Server. Para obter instruções, consulte Conectar-se a uma instância de banco de dados executando o mecanismo de banco de dados Microsoft SQL Server. Se você encontrar algum erro, consulte as referências de solução de problemas de conexão na seção Recursos relacionados.	DBA

Tarefa	Descrição	Habilidades necessárias
Crie o perfil.	Em SSMS, insira a seguinte instrução SQL para criar o perfil Database Mail. Substitua os valores a seguir: • Em `profile_name` , insira um nome para o novo perfil. • Em `description` , insira uma breve descrição do novo perfil. Para obter mais informaçõ es sobre esse procedime nto armazenado e seus argumentos, consulte sysmail_add_profile_sp na documentação da Microsoft. `EXECUTE msdb.dbo. sysmail_add_profil e_sp @profile_name = 'SQL Alerts profile', @description = 'Profile used for sending outgoing notifications using OM SMTP Server.';`	DBA

Tarefa	Descrição	Habilidades necessárias
Adicione diretores ao perfil.	Insira a seguinte instrução SQL para adicionar entidades públicas ou privadas ao perfil do Database Mail. Um principal é uma entidade que pode solicitar recursos do SQL Server. Substitua os valores a seguir: • Em `profile_name` , insira o nome do perfil criado anteriormente. • Em `principal_name` , insira o nome do usuário ou do perfil do banco de dados. Esse valor deverá ser mapeado para um usuário de autenticação do SQL Server, um usuário de autenticação do Windows ou um grupo de autentica ção do Windows. Para obter mais informaçõ es sobre esse procedime nto armazenado e seus argumentos, consulte sysmail_add_principalprofil e_sp na documentação da Microsoft. `EXECUTE msdb.dbo. sysmail_add_princi palprofile_sp`	DBA

Tarefa	Descrição	Habilidades necessárias
	`@profile_name = 'SQL Alerts profile', @principal_name = 'public', @is_default = 1 ;`	

Tarefa	Descrição	Habilidades necessárias
Crie a conta.	Digite a seguinte instrução SQL para criar a conta Database Mail. Substitua os valores a seguir: • Em `account_name`, insira um nome para a nova conta. • Em `description`, insira uma breve descrição da nova conta. • Para `email_address`, insira o endereço de e-mail do qual enviar as mensagens do Database Mail. • Para `display_address`, insira um nome de exibição para usar nas mensagens enviadas para essa conta, como `SQL Server Automated Notification`. Você também pode usar o valor inserido para `email_address`. • Em `mailserver_name`, insira o nome ou endereço IP do servidor de e-mail SMTP. • Para `port`, deixe o valor em `25`. • Para `enable_ssl`, deixe o valor em `1` ou insira `0`	DBA

Tarefa	Descrição	Habilidades necessárias
	se você não quiser que o Database Mail criptografe a comunicação usando SSL. • Para `username`, insira o nome de usuário para fazer login no servidor de e-mail SMTP. Se o servidor não exigir autenticação, insira `NULL`. • Para `password`, digite a senha para fazer login no servidor de e-mail SMTP. Se o servidor não exigir autenticação, insira `NULL`. Para obter mais informaçõ es sobre esse procedime nto armazenado e seus argumentos, consulte sysmail_add_account_sp na documentação da Microsoft. `EXECUTE msdb.dbo. sysmail_add_accoun t_sp @account_name = 'SQL Alerts account', @description = 'Database Mail account for sending outgoing notifications.', @email_address = 'xyz@example.com', @display_name = 'xyz@example.com',`	

Tarefa	Descrição	Habilidades necessárias
	<pre>@mailserver_name = 'test_smtp.example.com', @port = 25, @enable_ssl = 1, @username = 'SMTP-username', @password = 'SMTP-password';</pre>	

Tarefa	Descrição	Habilidades necessárias
Adicione a conta ao perfil.	Digite a seguinte instrução SQL para adicionar a conta Database Mail ao perfil Database Mail. Substitua os valores a seguir: • Em `profile_name` , insira o nome do perfil criado anteriormente. • Em `account_name` , insira o nome da conta criada anteriormente. Para obter mais informaçõ es sobre esse procedime nto armazenado e seus argumentos, consulte sysmail_add_profileaccount_ sp na documentação da Microsoft. `EXECUTE msdb.dbo. sysmail_add_profil eaccount_sp @profile_name = 'SQL Alerts profile', @account_name = 'SQL Alerts account', @sequence_number = 1;`	DBA

Tarefa	Descrição	Habilidades necessárias
(Opcional) Adicione Multi-AZ à instância de banco de dados do RDS.	Se você quiser adicionar Multi-AZ com Espelhamento de Banco de Dados (DBM) ou Grupos de Disponibilidade Always On (AGs), consulte as instruções em Adicionar Multi-AZ a uma instância de banco de dados Microsoft SQL Server.	DBA

Recursos relacionados

- Uso do Database Mail no Amazon RDS para SQL Server (documentação do Amazon RDS)
- Trabalhando com anexos de arquivo (documentação do Amazon RDS)
- Solução de problemas de conexões com a instância de banco de dados do SQL Server (documentação do Amazon RDS)
- Não é possível conectar-se à instância de banco de dados do Amazon RDS (documentação do Amazon RDS)

Configure a recuperação de desastres para SAP no IBM Db2 na AWS

Criado por Ambarish Satarkar (AWS) e Debasis Sahoo (AWS)

Resumo

Esse padrão descreve as etapas para configurar um sistema de recuperação de desastres (DR) para workloads do SAP com o IBM Db2 como plataforma de banco de dados, executado na nuvem da Amazon Web Services (AWS). O objetivo é fornecer uma solução de baixo custo para fornecer continuidade de negócios no caso de uma interrupção.

O padrão usa a abordagem de piloto leve. Ao implementar o DR de piloto leve na AWS, você pode reduzir o tempo de inatividade e manter a continuidade dos negócios. A abordagem de piloto leve se concentra na configuração de um ambiente mínimo de DR na AWS, incluindo um sistema SAP e um banco de dados DB2 em espera, sincronizados com o ambiente de produção.

Essa solução é escalável. Você pode estendê-lo para um ambiente de recuperação de desastres em grande escala, conforme necessário.

Pré-requisitos e limitações

Pré-requisitos

- Uma instância SAP em execução em uma instância do Amazon Elastic Compute Cloud (Amazon EC2)
- Um banco de dados IBM Db2
- Um sistema operacional compatível com a Product Availability Matrix (PAM – Matriz de Disponibilidade de Produtos) da SAP
- Nomes de host de banco de dados físicos diferentes para hosts de banco de dados de produção e de espera
- Um bucket do Amazon Simple Storage Service (Amazon S3) em cada região da AWS com a replicação entre regiões (CRR) habilitada

Versões do produto

- IBM Db2 Database versão 11.5.7 ou superior

Arquitetura

Pilha de tecnologias de destino

- Amazon EC2
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (Emparelhamento de VPC)
- Amazon Route 53
- Recuperação de desastres de alta disponibilidade do IBM Db2 (HADR)

Arquitetura de destino

Essa arquitetura implementa uma solução de DR para workloads do SAP com o Db2 como plataforma de banco de dados. O banco de dados de produção é implantado na Região da AWS 1 e um banco de dados em espera é implantado em uma segunda região. O banco de dados em espera é chamado de sistema DR. O Db2 Database suporta vários bancos de dados em espera (até três). Ele usa o Db2 HADR para configurar o banco de dados de DR e automatizar o envio de registros em log entre os bancos de dados de produção e de espera.

No caso de um desastre que torne a Região 1 indisponível, o banco de dados em espera na Região DR assume a função de banco de dados de produção. Os servidores de aplicativos SAP podem ser criados com antecedência ou usando o AWS Elastic Disaster Recovery ou uma imagem de máquina da Amazon (AMI) para atender aos requisitos do objetivo de tempo de recuperação (RTO). Esse padrão usa uma AMI.

O Db2 HADR implementa uma configuração de produção em espera, na qual a produção atua como o servidor primário e todos os usuários estão conectados a ele. Todas as transações são gravadas em arquivos de log, que são transferidos para o servidor em espera usando TCP/IP. O servidor em espera atualiza seu banco de dados local transferindo os registros de log transferidos, o que ajuda a garantir que ele seja mantido em sincronia com o servidor de produção.

O emparelhamento de VPC é usado para que as instâncias na região de produção e na região de DR possam se comunicar entre si. O Amazon Route 53 encaminha os usuários finais para aplicativos da Internet.

1. Crie uma AMI do servidor de aplicativos na Região 1 e copie a AMI para a Região 2. Use a AMI para iniciar servidores na Região 2 no caso de um desastre.

2. Configure a replicação do Db2 HADR entre o banco de dados de produção (na Região 1) e o banco de dados em espera (na Região 2).
3. Altere o tipo de EC2 instância para corresponder à instância de produção no caso de um desastre.
4. Na Região 1, `LOGARCHMETH1` está definido como `db2remote: S3 path`.
5. Na Região 2, `LOGARCHMETH1` está definido como `db2remote: S3 path`.
6. A replicação entre regiões é realizada entre os buckets do S3.

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS. Esse padrão usa o emparelhamento de VPC.

Práticas recomendadas

- A rede desempenha um papel fundamental na decisão do modo de replicação do HADR. Para DR em todas as regiões da AWS, recomendamos que você use o modo Db2 HADR ASYNC ou SUPERASYNC.
- Para obter mais informações sobre os modos de replicação do Db2 HADR, consulte a documentação da IBM.
- Você pode usar o Console de Gerenciamento da AWS ou a AWS Command Line Interface (AWS CLI) para criar uma nova AMI do seu sistema SAP existente. Em seguida, você pode usar a AMI para recuperar seu sistema SAP existente ou criar um clone.
- O AWS Systems Manager Automation pode ajudar nas tarefas comuns de manutenção e implantação de EC2 instâncias e outros recursos da AWS.

- A AWS fornece vários serviços nativos para monitorar e gerenciar sua infraestrutura e aplicativos na AWS. Serviços como Amazon CloudWatch e AWS CloudTrail podem ser usados para monitorar sua infraestrutura subjacente e operações de API, respectivamente. Para obter mais detalhes, consulte SAP na AWS – IBM Db2 HADR com Pacemaker.

Épicos

Prepare o ambiente

Tarefa	Descrição	Habilidades necessárias
Verifique o sistema e os logs.	1. Confirme se o SAP de produção no sistema Db2 está configurado. 2. Confirme se o backup de registros em log está ativado e configurado para salvar os registros no bucket do S3. Isso pode ser verificado pelo parâmetro `LOGARCHMETH1` do Db2. 3. Crie uma AMI do servidor de aplicativos adicional.	Administrador da AWS, administrador do SAP Basis

Configurar os servidores e a replicação

Tarefa	Descrição	Habilidades necessárias
Crie o SAP e os servidores de banco de dados.	1. Para implantar a infraestrutura para a região de DR, use um CloudFormation script da AWS ou use uma AMI da instância de produção. Como parte da abordagem piloto, você pode usar uma	Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	EC2 instância menor na mesma família da instância de produção. Por exemplo, se seu tipo de instância de produção for `r6i.12xlarge` , você poderá usar o tipo de instância `r6i.xlarge` para a compilação de DR. No entanto, certifique-se de alocar a mesma capacidade de armazenamento na instância de DR para restaurar o backup do banco de dados de produção. 2. Crie pontos de montagem do Amazon Elastic File System (Amazon EFS) e certifique-se de que eles estejam configurados para serem replicados do sistema primário `/sapmnt/<SID>/` . 3. Faça um backup COMPLETO do banco de dados (on-line ou off-line) do sistema de produção. Você usará esse backup para criar o banco de dados de DR. 4. No sistema de DR, use o método de cópia do sistema SAP Software Provision	

Tarefa	Descrição	Habilidades necessárias
	ing Manager (SWPM) em Usando a cópia do sistema com backup/restore for HA/DR propósitos para criar o sistema SAP de DR. 5. Quando solicitado pelo SWPM, restaure o banco de dados no DR com o backup que você tirou da produção. O banco de dados de DR estará no estado pendente de rollforward. O estado pendente de rollforward é definido por padrão depois que o backup completo é restaurado. O estado pendente de rollforwa rd indica que o banco de dados está sendo restaurad o e que algumas alterações talvez precisem ser aplicadas . Para obter mais informações, consulte a documentação da IBM.	

Tarefa	Descrição	Habilidades necessárias
Verifique a configuração.	1. Para configurar o arquivamento de registros em log para o HADR, os bancos de dados de produção e de DR devem ser capazes de recuperar registros automaticamente de todos os locais de arquivamento de registros . Verifique se o parâmetro `LOGARCHMETH1` no banco de dados de DR está definido no mesmo local do banco de dados de produção. Se o mesmo local não estiver acessível devido a limitações regionais, certifique-se de que o sistema de DR possa buscar automaticamente os registros em log do sistema primário. 2. Para habilitar portas TCP/IP para habilitar a replicação de banco de dados, modifique `/etc/services` nos hosts de produção e de DR adicionando as duas entradas a seguir. No código, `<SID>` refere-se ao ID do sistema (SID) do banco de dados Db2 (por exemplo, `PR1`).	Administrador da AWS, administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	<SID>_HADR_1 55001/tcp # DB2 HADR Port1 <SID>_HADR_2 55002/tcp # DB2 HADR Port2 Confirme se as duas portas permitem tráfego de entrada e saída entre a principal e a de espera. 3. Verifique `/etc/hosts` nos hosts de produção e de DR para confirmar se os nomes dos hosts de produção e de espera estão apontando para os endereços IP corretos.	

Tarefa	Descrição	Habilidades necessárias

Configure a replicação do banco de dados de produção para o banco de dados de recuperação de desastres (usando o modo ASSÍNCRONO).	1. No banco de dados de produção, execute os comandos a seguir para atualizar os parâmetros.
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	2. No banco de dados de DR, execute os comandos a
		Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias

	seguir para atualizar os parâmetros.
	
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	
	Esses parâmetros são necessários para fornecer informações relacionadas ao HADR aos dois bancos de dados. No	

Tarefa	Descrição	Habilidades necessárias

	banco de dados Db2, o HADR é ativado com base nos valores de cada um dos parâmetros definidos anteriormente. Para obter informações adicionais sobre esses parâmetros, consulte a documentação da IBM.
	3. Inicie primeiro o HADR no banco de dados em espera recém-criado usando o comando a seguir.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as standby`
	4. Inicie o HADR no banco de dados de produção usando o comando a seguir.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as primary`
	5. Verifique se os bancos de dados DB2 de produção e espera estão sincronizados e se o envio de registros está em andamento.
	Para monitorar o status de replicação do HADR, use o comando `db2pd` a seguir.	

Tarefa	Descrição	Habilidades necessárias
	`db2pd -d <SID> -hadr` Para obter informaçõ es adicionais sobre o monitoramento do HADR, consulte a documentação da IBM.	

Teste tarefas de failover de DR

Tarefa	Descrição	Habilidades necessárias
Planeje o tempo de inatividade da empresa de produção para o teste de DR.	Certifique-se de planejar o tempo de inatividade comercial necessário no ambiente de produção para testar o cenário de failover de DR.	Administrador do SAP Basis
Crie um usuário de teste.	Crie um usuário de teste (ou qualquer alteração de teste) que possa ser validado no host de DR para confirmar a replicação do log após o failover de DR.	Administrador do SAP Basis
No console, interrompa as EC2 instâncias de produção.	O desligamento incorreto é iniciado nesta etapa para imitar um cenário de desastre.	Administrador de sistemas AWS
Amplie a EC2 instância de DR para atender aos requisitos.	No EC2 console, altere o tipo de instância na região DR. 1. Interrompa a instância : se a instância estiver	Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias

	em execução, você deve interrompê-la para poder alterar o tipo da instância. No EC2 console, selecione a instância e escolha Parar.
	2. Modifique o tipo de instância: no EC2 console, selecione a instância e escolha Ações, Configura ções da instância, Alterar tipo de instância. Selecione o tipo de instância que corresponde à instância primária e selecione Aplicar.
	3. Iniciar a instância: depois que a alteração do tipo de instância for concluída, inicie a instância no EC2 console selecionando a instância e escolhendo Iniciar.
	4. Para iniciar o banco de dados Db2, use o comando a seguir.
	`db2start`
	`db2 start HADR on db <SID> as standby`	

Tarefa	Descrição	Habilidades necessárias

Iniciar a aquisição.	No sistema de DR (`host2`), inicie o processo de aquisição e crie o banco de dados de DR como principal.
	`db2 takeover hadr on database <SID> by force`
	Opcionalmente, você pode definir os seguintes parâmetros para ajustar automaticamente a alocação de memória do banco de dados com base no tipo de instância. O valor de `INSTANCE_MEMORY` pode ser decidido com base na parte dedicada da memória a ser alocada ao banco de dados Db2.
	`db2 update db cfg for <SID> using INSTANCE_MEMORY <FIXED VALUE> IMMEDIATE;`
	`db2 get db cfg for <SID> | grep -i DATABASE_MEMORY AUTOMATIC IMMEDIATE;`
	`db2 update db cfg for <SID> using self_tuning_mem ON IMMEDIATE;`
	Verifique a alteração usando os comandos a seguir.
	`db2 get db cfg for <SID> | grep -i MEMORY`
		Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	`db2 get db cfg for <SID> | grep -i self_tuning_mem`	
Inicie o servidor de aplicativos para SAP na região DR.	Usando a AMI que você criou do sistema de produção, inicie um novo servidor de aplicativos adicional na região de DR.	Administrador do SAP Basis
Execute a validação antes de iniciar o aplicativo SAP.	1. Valide as entradas `/etc/hosts` e `/etc/fstab`. 2. Monte `/sapmnt/<SID>/` no sistema de DR. 3. Valide se o sistema de arquivos DR `/sapmnt/<SID>/` está sincronizado com o arquivo de produção `/sapmnt/<SID>/`. 4. Faça login no usuário `<sid>adm`, execute `R3trans -d` e verifique a saída no arquivo `trans.log`. O arquivo `trans.log` é gerado no mesmo local em que você executou o comando `R3trans -d`.	Administrador da AWS, administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias

Inicie o aplicativo SAP no sistema DR.	Inicie o aplicativo SAP no sistema de DR usando o usuário `<sid>adm`. Use o código a seguir, em que XX representa o número da instância do seu servidor SAP ABAP SAP Central Services (ASCS) e YY representa o número da instância do seu servidor de aplicativos SAP.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
		Administrador do SAP Basis

Execute a validação do SAP.	Isso é realizado como um teste de DR para fornecer evidências ou verificar o sucesso da replicação de dados na região de DR.	Engenheiro de testes

Execute tarefas de failback de DR

Tarefa	Descrição	Habilidades necessárias
Inicie a produção de servidores SAP e de banco de dados.	No console, inicie as EC2 instâncias que hospedam o	Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	SAP e o banco de dados no sistema de produção.	

Inicie o banco de dados de produção e configure o HADR.	Faça login no sistema de produção (`host1`) e verifique se o banco de dados está no modo de recuperação usando o comando a seguir.
	`db2start`
	`db2 start HADR on db P3V as standby`
	`db2 connect to <SID>`
	Verifique se o status do HADR é `connected` . O status da replicação deve ser `peer`.
	`db2pd -d <SID> -hadr`
	Se o banco de dados não for inconsistente e não estiver nos status `connected` e `peer`, talvez seja necessário fazer backup e restauração para sincronizar o banco de dados (de `host1`) com o banco de dados atualmente ativo (`host2` na região de DR). Nesse caso, restaure o backup do banco de dados na região de DR `host2` para o banco de dados na região de produção `host1`.
		Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias
Retorne o banco de dados para a região de produção.	Em um business-as-usual cenário normal, essa etapa é executada em um tempo de inatividade programado. Os aplicativos em execução no sistema de DR são interrompidos e o banco de dados retorna à região de produção (Região 1) para retomar as operações da região de produção. 1. Faça login no servidor de aplicativos SAP na região de DR e interrompa o aplicativo SAP. 2. Desmonte `/sapmnt/<SID>` do sistema de DR, certificando-se de que as alterações sejam replicadas de forma reversa para `/sapmnt/<SID>` do sistema de produção. 3. Faça login no servidor de banco de dados (`host1`) na região de produção e execute a aquisição. `db2 takeover hadr on database <SID>` 4. Verifique o status do HADR: `HADR_ROLE` deve ser `PRIMARY` em `host1` e `StandBy` em `host2`.	Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	`db2pd -d <SID> -hadr`	
Execute a validação antes de iniciar o aplicativo SAP.	1. Valide as entradas `/etc/hosts` e `/etc/fstab`. 2. Monte `/sapmnt/<SID>/` no sistema de produção. 3. Certifique-se de que esteja sincronizado com o sistema DR `/sapmnt/<SID>/`. 4. Faça login no usuário `<sid>adm`, execute `R3trans -d` e verifique a saída no arquivo `trans.log`. O arquivo `trans.log` é gerado no mesmo local em que você executou o comando `R3trans -d`.	Administrador da AWS, administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias

Inicie o aplicativo SAP.	1. Inicie o aplicativo SAP no sistema de produção usando o usuário `<sid>adm`. Use o código a seguir, que XX represent a o número da instância do seu servidor SAP ASCS e YY representa o número da instância do seu servidor de aplicativos SAP.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
	2. Para confirmar se os servidores de aplicativos estão disponíveis, faça login no SAP e realize verificações usando o SICK e SM51 as transações.
		Administrador do SAP Basis

Solução de problemas

Problema	Solução
Principais arquivos de log e comandos para solucionar problemas relacionados ao HADR	• `db2 get db cfg | grep -i hadr` • `db2pd -d sid -hadr`

Problema	Solução
	• `Db2diag.log` (Esse arquivo geralmente está localizado dentro do diretório `db2dump` e o caminho `db2dump` é definido pelo parâmetro `DIAGPATH`.)
Nota do SAP para solucionar problemas de HADR no Db2 UDB	Consulte a Nota SAP 1154013 - DB6: Problemas de banco de dados no ambiente HADR. (Você precisa das credenciais do portal SAP para acessar esta nota.)

Recursos relacionados

- Abordagens de recuperação de desastres para bancos de dados Db2 na publicação do (blog da AWS)
- SAP na AWS – IBM Db2 HADR com Pacemaker
- Procedimento passo a passo para configurar a replicação de HADR entre bancos de dados DB2
- Wiki do Db2 HARD

Mais informações

Usando esse padrão, você pode configurar um sistema de recuperação de desastres para um sistema SAP executado no banco de dados Db2. Em uma situação de desastre, a empresa deve poder continuar dentro dos requisitos definidos de objetivo de tempo de recuperação (RTO) e ao objetivo de ponto de recuperação (RPO):

- O RTO é o atraso máximo aceitável entre a interrupção e a restauração do serviço. Ele determina o que é considerado uma janela de tempo aceitável quando o serviço não está disponível.
- O RPO é o período máximo de tempo aceitável desde o último ponto de recuperação de dados. Isso determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

Para informações FAQs relacionadas ao HADR, consulte a nota SAP #1612105 - DB6: FAQ on Db2 High Availability Disaster Recovery (HADR). (Você precisa das credenciais do portal SAP para acessar esta nota.)

Configure um pipeline de CI/CD para migração de banco de dados usando o Terraform

Criado pelo Dr. Rahul Sharad Gaikwad (AWS), Aarti Rajput (AWS), Ashish Bhatt (AWS), Aniket Dekate (AWS), Naveen Suthar (AWS), Nadeem Rahaman (AWS), Ruchika Modi (AWS) e Tamilselvan P (AWS)

Resumo

Esse padrão consiste em estabelecer um pipeline de integração e implantação contínuas (CI/CD) para gerenciar migrações de banco de dados de maneira confiável e automatizada. Ele abrange o processo de provisionamento da infraestrutura necessária, migração de dados e personalização de alterações de esquema usando o Terraform, que é uma ferramenta de infraestrutura como código (IaC).

Especificamente, o padrão configura um pipeline de CI/CD para migrar um banco de dados local do Microsoft SQL Server para o Amazon Relational Database Service (Amazon RDS) em. AWS Você também pode usar esse padrão para migrar um banco de dados SQL Server que está em uma máquina virtual (VM) ou em outro ambiente de nuvem para o Amazon RDS.

Esse padrão aborda os seguintes desafios associados ao gerenciamento e à implantação do banco de dados:

- As implantações manuais de banco de dados são demoradas, propensas a erros e carecem de consistência em todos os ambientes.
- Coordenar o provisionamento da infraestrutura, as migrações de dados e as mudanças no esquema pode ser complexo e difícil de gerenciar.
- Garantir a integridade dos dados e minimizar o tempo de inatividade durante as atualizações do banco de dados é crucial para os sistemas de produção.

Esse padrão fornece os seguintes benefícios:

- Simplifica o processo de atualização e implantação de alterações no banco de dados implementando um pipeline de CI/CD para migrações de banco de dados. Isso reduz o risco de erros, garante a consistência em todos os ambientes e minimiza o tempo de inatividade.
- Ajuda a melhorar a confiabilidade, a eficiência e a colaboração. Permite um tempo de lançamento mais rápido no mercado e reduz o tempo de inatividade durante as atualizações do banco de dados.

- Ajuda você a adotar DevOps práticas modernas de gerenciamento de banco de dados, o que leva a uma maior agilidade, confiabilidade e eficiência em seus processos de entrega de software.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Terraform 0.12 ou posterior instalado em sua máquina local (para obter instruções, consulte a documentação do Terraform)
- Terraform AWS Provider versão 3.0.0 ou posterior de HashiCorp (consulte o GitHub repositório deste provedor)
- Política de privilégios mínimos AWS Identity and Access Management (IAM) (consulte a postagem do blog Técnicas para escrever políticas de IAM com privilégios mínimos)

Arquitetura

Esse padrão implementa a arquitetura a seguir, que fornece a infraestrutura completa para o processo de migração do banco de dados.

Nesta arquitetura:

- O banco de dados de origem é um banco de dados do SQL Server que está no local, em uma máquina virtual (VM) ou hospedado por outro provedor de nuvem. O diagrama pressupõe que o banco de dados de origem esteja em um data center local.
- O data center local e AWS estão conectados por meio de uma VPN ou AWS Direct Connect conexão. Isso fornece comunicações seguras entre o banco de dados de origem e a AWS infraestrutura.
- O banco de dados de destino é um banco de dados do Amazon RDS hospedado na nuvem privada virtual (VPC) com a ajuda de um AWS pipeline de provisionamento de banco de dados.
- AWS Database Migration Service (AWS DMS) replica seu banco de dados local para o. AWS Ele é usado para configurar a replicação do banco de dados de origem para o banco de dados de destino.

O diagrama a seguir mostra a infraestrutura configurada com diferentes níveis do processo de migração do banco de dados, que envolve provisionamento, AWS DMS configuração e validação.

Nesse processo:

- O pipeline de validação valida todas as verificações. O pipeline integrado passa para a próxima etapa quando todas as validações necessárias forem concluídas.
- O pipeline de provisionamento de banco de dados consiste em vários AWS CodeBuild estágios que executam ações do Terraform no código do Terraform fornecido para o banco de dados. Quando essas etapas são concluídas, ele implanta recursos no destino Conta da AWS.
- O AWS DMS pipeline consiste em vários CodeBuild estágios que realizam testes e, em seguida, provisionam a AWS DMS infraestrutura para realizar a migração usando o IaC.

Ferramentas

Serviços da AWS e ferramentas

- AWS CodeBuildé um serviço de integração contínua totalmente gerenciado que compila o código-fonte, executa testes e produz pacotes ready-to-deploy de software.
- AWS CodePipelineé um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional no. Nuvem AWS
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e desempenho.
- AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para Nuvem AWS ou entre combinações de configurações na nuvem e no local.

Outros serviços

- O Terraform é uma ferramenta de IaC HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Repositório de código

O código desse padrão está disponível no GitHub Database Migration DevOps Framework usando o repositório de amostras do Terraform.

Práticas recomendadas

- Implemente testes automatizados para a migração do seu banco de dados para verificar a exatidão das alterações no esquema e a integridade dos dados. Isso inclui testes de unidade, testes de integração e end-to-end testes.
- Implemente uma estratégia robusta de backup e restauração para seus bancos de dados, especialmente antes da migração. Isso garante a integridade dos dados e fornece uma opção alternativa em caso de falhas.
- Implemente uma estratégia de reversão robusta para reverter as alterações do banco de dados em caso de falhas ou problemas durante a migração. Isso pode envolver a reversão para um estado anterior do banco de dados ou a reversão de scripts de migração individuais.
- Configure mecanismos de monitoramento e registro para acompanhar o progresso e o status das migrações de banco de dados. Isso ajuda você a identificar e resolver problemas rapidamente.

Épicos

Configure sua estação de trabalho local.

Tarefa	Descrição	Habilidades necessárias
Configure e configure o Git em sua estação de trabalho local.	Instale e configure o Git em sua estação de trabalho local seguindo as instruções na documentação do Git.	DevOps engenheiro
Crie uma pasta de projeto e adicione os arquivos do GitHub repositório.	1. Abra o GitHub repositório desse padrão. 2. Escolha Código para ver as opções de clonagem e copie o URL fornecido na guia HTTPS. 3. Crie uma pasta para seu projeto na sua estação de trabalho.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	4. Abra um terminal e navegue até essa pasta.
	5. Clone o GitHub repositório:
	`git clone <github-repository-url>`
	onde `<github-repository-url>` está o URL que você copiou na etapa 2.
	6. Quando a clonagem estiver concluída, acesse o repositório clonado na pasta do seu projeto:
	`cd <folder-name>/aws-terraform-db-migration-framework-samples`
	7. Abra este projeto em um ambiente de desenvolvimento integrado (IDE) de sua escolha.	

Provisionar a arquitetura de destino

Tarefa	Descrição	Habilidades necessárias
Atualize os parâmetros necessários.	O `ssm-parameters.sh` arquivo armazena todos os AWS Systems Manager parâmetros necessários. Você pode configurar esses	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	parâmetros com os valores personalizados do seu projeto. Na `setup/db-ssm-params` pasta da sua estação de trabalho local, abra o `ssm-parameters.sh` arquivo e defina esses parâmetros antes de executar o pipeline de CI/CD.	
Inicialize a configuração do Terraform.	Na `db-cicd-integration` pasta, digite o seguinte comando para inicializar seu diretório de trabalho que contém os arquivos de configuração do Terraform: `terraform init`	DevOps engenheiro
Visualize o plano do Terraform.	Para criar um plano do Terraform, digite o seguinte comando: `terraform plan -var-file="terraform.sample"` O Terraform avalia os arquivos de configuração para determinar o estado de destino dos recursos declarados. Em seguida, ele compara o estado de destino com o estado atual e cria um plano.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Verificar o plano.	Revise o plano e confirme se ele configura a arquitetura necessária em seu destino Conta da AWS.	DevOps engenheiro
Implante a solução.	1. Insira o comando a seguir para aplicar o plano: `terraform apply -var-file="terraform.sample"` 2. Digite `yes` para confirmar. O Terraform cria, atualiza ou destrói a infraestrutura para atingir o estado de destino declarado nos arquivos de configuração. Para obter mais informações sobre a sequência, consulte a seção Arquitetura desse padrão.	DevOps engenheiro

Verificar a implantação

Tarefa	Descrição	Habilidades necessárias
Valide a implantação.	Verifique o status do `db-cicd-integration` pipeline para confirmar se a migração do banco de dados foi concluída. 1. Faça login no e AWS Management Console,	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	em seguida, abra o AWS CodePipeline console. 2. No painel de navegação, selecione Pipelines. 3. Escolha o `db-cicd-integration` pipeline. 4. Valide se a execução do pipeline foi concluída com êxito.	

Limpe a infraestrutura após o uso

Tarefa	Descrição	Habilidades necessárias
Limpe a infraestrutura.	1. Depois que seu projeto estiver concluído, limpe a infraestrutura que você criou usando o comando: `terraform destroy --var-file=terraform.sample` 2. Digite `yes` para confirmar.	DevOps engenheiro

Recursos relacionados

AWS documentação

- Começando com um produto Terraform

Documentação do Terraform

- Instalação do Terraform
- Configuração de back-end do Terraform
- Documentação do Terraform AWS Provider

Configure uma arquitetura de HA/DR para o Oracle E-Business Suite no Amazon RDS Custom com um banco de dados ativo em espera

Criado por Simon Cunningham (AWS) e Nitin Saxena

Resumo

Esse padrão descreve como você pode arquitetar sua solução Oracle E-Business no Amazon Relational Database Service (Amazon RDS) Custom para alta disponibilidade (HA) e recuperação de desastres (DR) configurando um banco de dados de réplica de leitura do Amazon RDS Custom em outra zona de disponibilidade da Amazon Web Services (AWS) e convertendo-o em um banco de dados ativo em espera. A criação da réplica de leitura do Amazon RDS Custom é totalmente automatizada por meio do Console de Gerenciamento da AWS.

Esse padrão não discute as etapas para adicionar camadas adicionais de aplicativos e sistemas de arquivos compartilhados, que também podem fazer parte de uma arquitetura de HA/DR. Para obter mais informações sobre esses tópicos, consulte as seguintes notas de suporte da Oracle: 1375769.1, 1375670.1 e 1383621.1 (seção 5, Opções avançadas de clonagem). (O acesso requer uma conta do Oracle Support.)

Para migrar o sistema E-Business Suite para uma arquitetura Single-AZ de camada única na Amazon Web Services (AWS), consulte o padrão Migrar o Oracle E-Business Suite para o Amazon RDS Custom.

O Oracle E-Business Suite é uma solução de Planejamento de recursos empresariais (ERP - Enterprise Resource Planning) para automatizar processos em toda a empresa, como finanças, recursos humanos, cadeias de suprimentos e manufatura. Ele tem uma arquitetura de três camadas: cliente, aplicação e banco de dados. Anteriormente, você precisava executar seu banco de dados do E-Business Suite em uma instância autogerenciada do Amazon Elastic Compute Cloud (Amazon EC2), mas agora você pode se beneficiar do Amazon RDS Custom.

Pré-requisitos e limitações

Pré-requisitos

- Uma instalação existente do E-Business Suite no Amazon RDS Custom; veja o padrão Migrar o Oracle E-Business Suite para o Amazon RDS Custom

- Se você quiser alterar a réplica de leitura para somente leitura e usá-la para transferir os relatórios para o modo de espera, uma licença de banco de dados Oracle Active Data Guard (consulte a Lista de preços comerciais de tecnologia da Oracle)

Limitações

- Limitações e configurações não suportadas para bancos de dados Oracle no Amazon RDS Custom
- Limitações associadas às réplicas de leitura do Amazon RDS Custom for Oracle

Versões do produto

Para versões do banco de dados Oracle e classes de instância suportadas pelo Amazon RDS Custom, consulte Requisitos e limitações do Amazon RDS Custom for Oracle.

Arquitetura

O diagrama a seguir ilustra uma arquitetura representativa do E-Business Suite na AWS que inclui várias zonas de disponibilidade e níveis de aplicativos em uma configuração ativa/passiva. O banco de dados usa uma instância de banco de dados do Amazon RDS Custom e uma réplica de leitura do Amazon RDS Custom. A réplica de leitura usa o Active Data Guard para replicar em outra zona de disponibilidade. Você também pode usar a réplica de leitura para descarregar o tráfego de leitura no banco de dados principal e para fins de geração de relatórios.

Para obter mais informações, consulte Trabalhar com réplicas de leitura do Amazon RDS Custom para Oracle na documentação do Amazon RDS.

A réplica de leitura do Amazon RDS Custom é criada por padrão como montada. No entanto, se você quiser transferir algumas de suas cargas de trabalho somente para leitura no banco de dados em espera para reduzir a carga no banco de dados principal, você pode alterar manualmente o modo das réplicas montadas para somente leitura seguindo as etapas na seção Épicos. Um caso de uso típico para isso seria executar seus relatórios a partir do banco de dados em espera. Mudar para somente leitura requer uma licença ativa de banco de dados em espera.

Quando você cria uma réplica de leitura na AWS, o sistema usa o agente Oracle Data Guard nos bastidores. Essa configuração é gerada e configurada automaticamente no modo Desempenho Máximo da seguinte forma:

```
DGMGRL> show configuration
Configuration - rds_dg
  Protection Mode: MaxPerformance
  Members:
  vis_a - Primary database
    vis_b - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS   (status updated 58 seconds ago)
```

Ferramentas

Serviços da AWS

- O Amazon RDS Custom para Oracle é um serviço de banco de dados gerenciado para aplicações herdadas, personalizadas e em pacote que exigem acesso ao sistema operacional subjacente e ao ambiente de banco de dados. Ele automatiza tarefas e operações de administração de banco de dados e permite que você, como administrador de banco de dados, acesse e personalize seu ambiente de banco de dados e sistema operacional.

Outras ferramentas

- O Oracle Data Guard é uma ferramenta que ajuda você a criar e gerenciar bancos de dados Oracle standby. Esse padrão usa o Oracle Data Guard para configurar um banco de dados em espera ativo no Amazon RDS Custom.

Épicos

Criar uma réplica de leitura

Tarefa	Descrição	Habilidades necessárias
Crie uma réplica de leitura da instância de banco de dados do Amazon RDS Custom.	Para criar uma réplica de leitura, siga as instruções na documentação do Amazon RDS e use a instância de banco de dados do Amazon RDS Custom que você criou	DBA

Tarefa	Descrição	Habilidades necessárias
	(consulte a seção Pré-requisitos) como banco de dados de origem. Por padrão, a réplica de leitura do Amazon RDS Custom é criada como uma espera física e está no estado montado. Isso é intencional para garantir a conformidade com a licença do Oracle Active Data Guard. Siga as próximas etapas para converter a réplica de leitura no modo somente leitura.	

Altere a réplica de leitura para um modo de espera ativo somente para leitura

Tarefa	Descrição	Habilidades necessárias
Conecte-se à réplica de leitura do Amazon RDS Custom.	Use os comandos a seguir para converter seu banco de dados stand-by físico em um banco de dados stand-by ativo. ⚠ Important Esses comandos exigem uma licença de espera ativa da Oracle. Para obter uma licença, entre em contato com seu	DBA

Tarefa	Descrição	Habilidades necessárias
	representante da Oracle.	

	`$ sudo su - rdsdb`
	`-bash-4.2$ sql`
	`SQL> select process,s`
	`tatus,sequence# from v`
	`$managed_standby;`
	
	`PROCESS STATUS`
	`SEQUENCE#`
	`--------- ------------`
	`----------`
	`ARCH CLOSING`
	`3956`
	`ARCH CONNECTED`
	`0`
	`ARCH CLOSING`
	`3955`
	`ARCH CLOSING`
	`3957`
	`RFS IDLE`
	`0`
	`RFS IDLE`
	`3958`
	`MRP0 APPLYING_LOG`
	`3958`
	`SQL> select name,`
	`database_role,`
	`open_mode from v`
	`$database;`
	
	`NAME DATABASE_`
	`ROLE OPEN_MODE`
	`--------- ---------`
	`------- ---------`
	`----------`
	`VIS PHYSICAL`
	`STANDBY MOUNTED`	

Tarefa	Descrição	Habilidades necessárias

	SQL> alter database
	  recover managed standby
	  database cancel;
	Database altered.
	Open the standby
	  database
	SQL> alter database
	  open;
	Database altered.
	SQL> select name,
	  database_role,
	  open_mode from v
	$database;
	
	NAME DATABASE_
	ROLE OPEN_MODE
	--------- ---------
	------- ---------
	----------- 	
	VIS PHYSICAL
	  STANDBY READ ONLY	

Tarefa	Descrição	Habilidades necessárias

Inicie a recuperação de mídia com a aplicação de registros em tempo real.	Para ativar o atributo de aplicação de log em tempo real, use os comandos a seguir. Eles convertem e validam o standby (réplica de leitura) como um banco de dados em espera ativo, para que você possa se conectar e executar consultas somente para leitura.
	`SQL>  alter database recover managed standby database using current logfile disconnect from session;`
	`Database altered`
		DBA

Verifique o status do banco de dados.	Para verificar o status do banco de dados, use o comando a seguir.
	`SQL> select name, database_role, open_mode from v$database;`
	`NAME  DATABASE_ROLE  OPEN_MODE`
	`--------- ---------- ----------`
	`VIS  PHYSICAL STANDBY  READ ONLY WITH APPLY`
		DBA

Tarefa	Descrição	Habilidades necessárias

Marque o modo de refazer aplicação.	Para verificar o modo de aplicação de refazer, use o seguinte comando.
	
	`SQL> select process,s tatus,sequence# from v $managed_standby;`
	`PROCESS STATUS SEQUENCE#`
	`--------- ------------ ----------`
	`ARCH CLOSING 3956`
	`ARCH CONNECTED 0`
	`ARCH CLOSING 3955`
	`ARCH CLOSING 3957`
	`RFS IDLE 0`
	`RFS IDLE 3958`
	`MRP0 APPLYING_LOG 3958`
	
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`--------------------`
	`READ ONLY WITH APPLY`
		DBA

Recursos relacionados

- Migre o Oracle E-Business Suite para o Amazon RDS Custom (Recomendações da AWS)
- Trabalhando com o Amazon RDS Custom (documentação do Amazon RDS)
- Trabalhar com réplicas de leitura do Amazon RDS Custom for Oracle (documentação do Amazon RDS)

- Amazon RDS Custom para Oracle – Novos recursos de controle no ambiente de banco de dados (blog de notícias da AWS)
- Migração do Oracle E-Business Suite na AWS (whitepaper da AWS)
- Arquitetura do Oracle E-Business Suite na AWS (whitepaper da AWS)

Configure a replicação de dados entre o Amazon RDS for MySQL e o MySQL na Amazon usando o GTID EC2

Criado por Rajesh Madiwale (AWS)

Resumo

Esse padrão descreve como configurar a replicação de dados na nuvem da Amazon Web Services (AWS) entre uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS) para MySQL e um banco de dados MySQL em uma instância do Amazon Elastic Compute Cloud (Amazon) usando a replicação do identificador de transação global nativo (GTID) do MySQL. EC2

Com GTIDs, as transações são identificadas e rastreadas quando são confirmadas no servidor de origem e aplicadas por réplicas. Você não precisa consultar os arquivos de log ao iniciar uma nova réplica durante o failover.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância do Amazon Linux implantada

Restrições

- Essa configuração precisa que uma equipe interna execute as consultas somente para leitura.
- As versões de origem e de destino do MySQL devem ser as mesmas.
- A replicação é configurada na mesma região da AWS e nuvem privada virtual (VPC).

Versões do produto

- Versões do Amazon RDS 5.7.23 e mais recentes, que são as compatíveis com o GTID

Arquitetura

Pilha de tecnologia de origem

- Amazon RDS para MySQL

Pilha de tecnologias de destino

- MySQL na Amazon EC2

Arquitetura de destino

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.

Outros serviços

- Os identificadores globais de transação (GTIDs) são identificadores exclusivos gerados para transações confirmadas do MySQL.
- O mysqldump é um utilitário cliente para realizar backups lógicos produzindo instruções SQL que podem ser executadas para reproduzir as definições do objeto do banco de dados de origem e os dados da tabela.
- O mysql é o cliente de linha de comando para o MySQL.

Épicos

Crie e prepare a instância de banco de dados do Amazon RDS para MySQL

Tarefa	Descrição	Habilidades necessárias
Crie a instância do RDS para MySQL.	Para criar a instância do RDS para MySQL, siga as etapas na documentação do Amazon	DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
	RDS, usando os valores dos parâmetros abordados na próxima tarefa.	
Ative as configurações relacionadas ao GTID no grupo de parâmetros do banco de dados.	Ative os parâmetros a seguir no grupo de parâmetros do banco de dados do Amazon RDS para MySQL. Defina `enforce_gtid_consistency` para on e defina `gtid-mode` para on.	DBA
Reinicie a instância do Amazon RDS para MySQL.	É necessária uma reinicialização para que as alterações virem efetivas.	DBA

Crie um usuário e conceda a ele permissões de replicação.	Para instalar o MySQL, use os comandos a seguir.
	
	`CREATE USER 'repl'@'%' IDENTIFIED BY 'xxxx';`
	`GRANT REPLICATION SLAVE ON *.* TO 'repl'@'%' ;`
	`FLUSH PRIVILEGES;`
		DBA

Instale e prepare o MySQL na instância da Amazon EC2

Tarefa	Descrição	Habilidades necessárias

Instale o MySQL no Amazon Linux	Para instalar o MySQL, use os comandos a seguir.
	`sudo yum update`
	`sudo wget https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm`
	`sudo yum localinstall mysql57-community-release-el7-11.noarch.rpm`
	`sudo yum install mysql-community-server`
	`sudo systemctl start mysqld`
		DBA

Faça login no MySQL na EC2 instância e crie o banco de dados.	O nome do banco de dados deve ser igual ao nome do banco de dados no Amazon RDS para MySQL. No exemplo a seguir, o nome do banco de dados é `replication` . `create database replication;`	DBA
Edite o arquivo de configuração do MySQL e reinicie o banco de dados.	Edite o arquivo `my.conf` localizado em `/etc/` adicionando os seguintes parâmetros. `server-id=3`	DBA

Tarefa	Descrição	Habilidades necessárias

	`gtid_mode=ON enforce_gtid_consistency=ON replicate-ignore-db=mysql binlog-format=ROW log_bin=mysql-bin`
	
	Depois reinicie o serviço `mysqld`.
	
	`systemctl mysqld restart`	

Replicação da configuração

Tarefa	Descrição	Habilidades necessárias
Exporte o dump de dados do banco de dados Amazon RDS para MySQL.	Para exportar o dump do Amazon RDS para o Amazon RDS para MySQL, use o comando a seguir. `mysqldump --single-transaction -h mydb.xxxxxxx.amazonaws.com -uadmin -p --databases replication > replication-db.sql`	DBA
Restaure o arquivo de despejo .sql no banco de dados MySQL na Amazon. EC2	Para importar o dump para o banco de dados MySQL na EC2 Amazon, use o comando a seguir.	DBA

Tarefa	Descrição	Habilidades necessárias
	`mysql -D replication -uroot -p < replication-db.sql`	

Configure o banco de dados MySQL na Amazon EC2 como uma réplica.	Para iniciar a replicação e verificar o status da replicação, faça login no banco de dados MySQL na Amazon EC2 e use o comando a seguir.
	`CHANGE MASTER TO MASTER_HOST="mydb.xxxxxxx.amazonaws.com", MASTER_USER="repl", MASTER_PASSWORD="rep123", MASTER_PORT=3306, MASTER_AUTO_POSITION = 1;`
	`START SLAVE;`
	`SHOW SLAVE STATUS\G`
		DBA

Recursos relacionados

- Guia EC2 do usuário da Amazon para instâncias Linux
- Instalar o MySQL no Linux usando o repositório MySQL Yum
- Replicação com identificadores globais de transações
- Uso da replicação baseada em GTID para o Amazon RDS para MySQL

Funções de transição para um PeopleSoft aplicativo Oracle no Amazon RDS Custom for Oracle

Criado por sampath kathirvel (AWS)

Resumo

Para executar a solução Oracle PeopleSoft Enterprise Resource Planning (ERP) na Amazon Web Services (AWS), você pode usar o Amazon Relational Database Service (Amazon RDS) ou o Amazon RDS Custom for Oracle, que oferece suporte a aplicativos legados, personalizados e empacotados que exigem acesso ao sistema operacional (SO) e ao ambiente de banco de dados subjacentes. Para ver os principais fatores a serem considerados ao planejar uma migração, consulte as estratégias de migração do banco de dados Oracle nas Recomendações da AWS.

Esse padrão se concentra nas etapas para realizar uma transição de função, ou transição de função, do Oracle Data Guard para um banco de dados de PeopleSoft aplicativos executado no Amazon RDS Custom como o banco de dados principal com um banco de dados de réplica de leitura. O padrão inclui etapas para configurar o failover de início rápido (FSFO). Durante esse processo, os bancos de dados na configuração do Oracle Data Guard continuam funcionando em suas novas funções. Os casos de uso típicos da transição do Oracle Data Guard são exercícios de recuperação de desastres (DR), atividades de manutenção programada em bancos de dados e patches contínuos em espera-First Patch Apply. Para obter mais informações, consulte a postagem de blog Reduza o tempo de inatividade de patch de banco de dados no Amazon RDS Custom.

Pré-requisitos e limitações

Pré-requisitos

- Conclusão do Add HA to Oracle PeopleSoft on Amazon RDS Custom usando um padrão de réplica de leitura.

Limitações

- Limitações gerais e configurações incompatíveis para o RDS Personalizado para Oracle
- Limitações associadas às réplicas de leitura do Amazon RDS Custom para Oracle

Versões do produto

- Para versões do Oracle Database suportadas pelo Amazon RDS Custom, consulte RDS Custom for Oracle
- Para classes de instância de banco de dados do Oracle Database suportadas pelo Amazon RDS Custom, consulte Suporte a classes de instância de banco de dados do RDS Custom for Oracle.

Arquitetura

Pilha de tecnologia

- Amazon RDS Custom para Oracle

Arquitetura de destino

O diagrama a seguir mostra uma instância de banco de dados do Amazon RDS Custom e uma réplica de leitura personalizada do Amazon RDS Custom. O Oracle Data Guard fornece transição de funções durante o failover para DR.

Para uma arquitetura representativa usando o Oracle PeopleSoft na AWS, consulte Configurar uma PeopleSoft arquitetura altamente disponível na AWS.

Ferramentas

Serviços da AWS

- O Amazon RDS Custom para Oracle é um serviço de banco de dados gerenciado para aplicativos legados, personalizados e em pacote que exigem acesso ao sistema operacional subjacente e ao ambiente de banco de dados.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente. Nesse padrão, você recupera as senhas de usuário do banco de dados do Secrets Manager for `RDS_DATAGUARD` com o nome secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Outros serviços

- O Oracle Data Guard ajuda você a criar, manter, gerenciar e monitorar bancos de dados em espera. Esse padrão usa o Oracle Data Guard Maximum Performance para funções de transição (transição do Oracle Data Guard).

Práticas recomendadas

Para sua implantação de produção, recomendamos iniciar a instância observadora em uma terceira zona de disponibilidade, separada dos nós primário e de réplica de leitura.

Épicos

Iniciar a transição de funções

Tarefa	Descrição	Habilidades necessárias
Pausar a automação do banco de dados tanto para o primário quanto para a réplica.	Embora o framework de automação personalizada do RDS não interfira no processo de transição de funções, é uma boa prática pausar a automação durante a transição do Oracle Data Guard. Para pausar e retomar a Automação personalizada do banco de dados RDS, siga as instruções em Pausar e retomar a automação personalizada do RDS.	Administrador de nuvem, DBA
Verificar o status do Oracle Data Guard.	Para verificar o status do Oracle Data Guard, faça login no banco de dados primário. Esse padrão inclui código para usar um banco de dados de contêiner multilocação (CDB) ou uma instância não CDB.	DBA

Tarefa	Descrição	Habilidades necessárias

	Não CDB
	
	`-bash-4.2$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_A`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Mon Nov 28 20:55:50 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for information.`
	`Password:`
	`Connected to "ORCL_A"`
	`Connected as SYSDG.`
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 59 seconds ago)`
	`DGMGRL>`
	
	CDB	

Tarefa	Descrição	Habilidades necessárias

	CDB-bash-4.2$ dgmgrl
	 C##RDS_DATAGUARD@R
	DS_CUSTOM_RDSCDB_A
	DGMGRL for Linux:
	 Release 19.0.0.0.0 -
	 Production on Wed Jan
	 18 06:13:07 2023
	Version 19.16.0.0.0
	Copyright (c) 1982,
	 2019, Oracle and/or
	 its affiliates. All
	 rights reserved.
	Welcome to DGMGRL, type
	 "help" for informati
	on.
	Password:
	Connected to "RDSCDB_A
	"
	Connected as SYSDG.
	DGMGRL> show configura
	tion
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	    rdscdb_b - Physical
	 standby database
	Fast-Start Failover:
	 Disabled
	Configuration Status:
	SUCCESS (status
	 updated 52 seconds ago)
	DGMGRL>	

Tarefa	Descrição	Habilidades necessárias
Verifique a função da instância.	Abra o Console de Gerenciamento da AWS e navegue para o console do Amazon RDS. Na seção Replicação do banco de dados, na guia Conectividade e segurança, verifique a função da instância primária e da réplica. A função primária deve corresponder ao banco de dados primário do Oracle Data Guard, e a função de réplica deve corresponder ao banco de dados físico em espera do Oracle Data Guard.	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias

Executar a transição.	Para realizar a transição, conecte-se a DGMGRL a partir do nó primário.
	
	Não CDB
	
	`DGMGRL> switchover to orcl_d;`
	`Performing switchover NOW, please wait...`
	`Operation requires a connection to database "orcl_d"`
	`Connecting ...`
	`Connected to "ORCL_D"`
	`Connected as SYSDG.`
	`New primary database "orcl_d" is opening...`
	`Operation requires start up of instance "ORCL" on database "orcl_a"`
	`Starting instance "ORCL"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "ORCL_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "ORCL_A"`
	`Switchover succeeded, new primary is "orcl_d"`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> switchover to rdscdb_b`
		DBA

Tarefa	Descrição	Habilidades necessárias

	`Performing switchover NOW, please wait...`
	`New primary database "rdscdb_b" is opening...`
	`Operation requires start up of instance "RDSCDB" on database "rdscdb_a"`
	`Starting instance "RDSCDB"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "RDSCDB_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "RDSCDB_A"`
	`Switchover succeeded, new primary is "rdscdb_b"`	

Tarefa	Descrição	Habilidades necessárias

Verificar a conexão do Oracle Data Guard.	Após a transição, verifique a conexão do Oracle Data Guard do nó primário com `DGMGRL`.
	
	Não CDB
	
	`DGMGRL> show configura tion;`
	`Configuration - rds_dg`
	`Protection Mode:`
	` MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	` database`
	`orcl_a - Physical`
	` standby database`
	`Fast-Start Failover:`
	` Disabled`
	`Configuration Status:`
	`SUCCESS (status updated`
	` 60 seconds ago)`
	`DGMGRL>`
	
	`DGMGRL> show configura tion lag;`
	`Configuration - rds_dg`
	`Protection Mode:`
	` MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	` database`
	`orcl_a - Physical`
	` standby database`
	`Transport Lag: 0`
	` seconds (computed 0`
	` seconds ago)`
	`Apply Lag: 0 seconds`
	` (computed 0 seconds`
	` ago)`
		DBA

Tarefa	Descrição	Habilidades necessárias
	Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 44 seconds ago) DGMGRL>	

	CDB
	
	DGMGRL> show configura
	tion
	DGMGRL> show configura
	tion
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_b - Primary
	 database
	  rdscdb_a - Physical
	 standby database
	Fast-Start Failover:
	 Disabled
	Configuration Status:
	SUCCESS (status
	 updated 52 seconds ago)
	DGMGRL>
	
	DGMGRL> show configura
	tion lag
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_b - Primary
	 database
	  rdscdb_a - Physical
	 standby database
	  Transport
	 Lag: 0 seconds	

Tarefa	Descrição	Habilidades necessárias
	(computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 53 seconds ago) DGMGRL>	
Verificar a função da instância no console do Amazon RDS.	Depois de mudar a função, o console do Amazon RDS mostra as novas funções na seção Replicação, na guia Conectividade e segurança, em Bancos de dados. Pode levar alguns minutos para que o Estado da Replicação seja atualizado de vazio para Replicando.	DBA

Configurar FSFO

Tarefa	Descrição	Habilidades necessárias
Redefinir a transição.	Definir a transição de volta para o nó primário.	DBA
Instalar e iniciar o observador.	Um processo observador é um componente cliente DGMGRL, normalmente executado em uma máquina diferente dos bancos de	DBA

Tarefa	Descrição	Habilidades necessárias
	dados primário e em espera. A instalação do ORACLE HOME para o observador pode ser uma instalação do Oracle Client Administrator, ou você pode instalar o Oracle Database Enterprise Edition ou o Personal Edition. Para obter mais informações sobre a instalação do observador para sua versão do banco de dados, consulte Instalar e iniciar o observador. Para configurar a alta disponibilidade do processo do observador, faça uma das seguintes opções: • Ative a recuperação automática de EC2 instâncias para a EC2 instância que executa seu observador. Você precisa automatizar o processo de startup do observador como parte do startup do sistema operacional. • Implante um observador na EC2 instância e configure um grupo do Amazon EC2 Auto Scaling com tamanho um (1). Em caso de falha na EC2 instância, o grupo de escalabilidade automática	

Tarefa	Descrição	Habilidades necessárias
	ativa automaticamente outra EC2 instância. Para o Oracle 12c liberação 2 e posterior, você pode implantar até três observadores. Um observador é o observador primário e os demais são observadores de backup. Quando o observador primário falha, um dos observadores de backup assume a função primária.	

Tarefa	Descrição	Habilidades necessárias

Conectar ao DGMGRL a partir do host observador.	O host observador é configurado com `tnsnames.ora` entradas para conectividade de banco de dados primário e em espera. Você pode ativar o FSFO com o modo de proteção de desempenho máximo, desde que a perda de dados esteja dentro da FastStartFailoverLagLimitconfiguração (valor em segundos). No entanto, você deve usar o modo de proteção de disponibilidade máxima para trabalhar para obter zero perda de dados (RPO = 0).
	
	Não CDB
	
	`DGMGRL> show configuration;`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 58 seconds ago)`
	`DGMGRL> show configuration lag`
	`Configuration - rds_dg`
		DBA

Tarefa	Descrição	Habilidades necessárias
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - Physical standby database Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 5 seconds ago) DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_A DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 18 06:55:09 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_A" Connected as SYSDG.	

Tarefa	Descrição	Habilidades necessárias

	DGMGRL> show configura
	tion
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	  rdscdb_b - Physical
	 standby database
	Fast-Start Failover:
	 Disabled
	Configuration Status:
	SUCCESS (status
	 updated 18 seconds ago)
	DGMGRL>	

Tarefa	Descrição	Habilidades necessárias

Modificar o banco de dados em espera para ser o destino do failover.	Conectar do nó primário ou do nó observador a um banco de dados em espera. (Embora sua configuração possa ter vários bancos de dados em espera, você precisa se conectar a somente um no momento.)
	
	Não CDB
	
	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='orcl_d';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database orcl_d set property FastStartFailoverTarget='orcl_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database orcl_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_d'`
	`DGMGRL> show database orcl_d FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_a'`
	`DGMGRL>`
	
	CDB
		DBA

Tarefa	Descrição	Habilidades necessárias

	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='rdscdb_b';`
	`Object "orcl_a" was not found`
	`DGMGRL> edit database rdscdb_a set property FastStartFailoverTarget='rdscdb_b';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database rdscdb_b set property FastStartFailoverTarget='rdscdb_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database rdscdb_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'rdscdb_b'`
	`DGMGRL> show database rdscdb_b FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'rdscdb_a'`
	`DGMGRL>`	

Tarefa	Descrição	Habilidades necessárias

Configure FastStartFailoverThreshold para a conexão com o DGMGRL.	O valor padrão é 30 segundos no Oracle 19c e o valor mínimo é 6 segundos. Um valor menor pode reduzir potencialmente o objetivo de tempo de recuperação (RTO) durante o failover. Um valor maior ajuda a reduzir a chance de erros transitórios de failover desnecessários no banco de dados primário.
	
	O framework de automação RDS Custom for Oracle monitora a integridade do banco de dados e executa ações corretivas a cada poucos segundos. Portanto, recomendamos FastStartFailoverThreshold definir um valor maior que 10 segundos. O exemplo a seguir configura o valor limite em 35 segundos.
	
	Não CBD ou CDB
	
	`DGMGRL> edit configuration set property FastStartFailoverThreshold=35;`
	`Property "faststartfailoverthreshold" updated`
	`DGMGRL> show configuration FastStartFailoverThreshold;`
		DBA

Tarefa	Descrição	Habilidades necessárias
	`FastStartFailover Threshold = '35' DGMGRL>`	

Tarefa	Descrição	Habilidades necessárias

Habilitar o FSFO conectando-se ao DGMGRL a partir do nó primário ou observador.	Se o banco de dados não tiver o Flashback Database habilitado, a mensagem de aviso `ORA-16827` será exibida. O banco de dados de flashback opcional ajuda a restabelecer automatic amente os bancos de dados primários com falha em um ponto no tempo antes do failover, se a propriedade de FastStartFailoverAutoReinstateconfiguração estiver definida como TRUE (que é o padrão).
	
	Não CDB
	
	`DGMGRL> enable fast_start failover;`
	`Warning: ORA-16827: Flashback Database is disabled`
	`Enabled in Zero Data Loss Mode.`
	`DGMGRL>`
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`Warning: ORA-16819: fast-start failover observer not started`
		DBA

Tarefa	Descrição	Habilidades necessárias

	orcl_d - (*) Physical
	 standby database
	Warning: ORA-16819:
	 fast-start failover
	 observer not started
	Fast-Start Failover:
	 Enabled in Zero Data
	 Loss Mode
	Configuration Status:
	WARNING (status updated
	 29 seconds ago)
	DGMGRL>
	
	CDB
	
	DGMGRL> enable fast_star
	t failover;
	Warning: ORA-16827:
	 Flashback Database is
	 disabled
	Enabled in Zero Data
	 Loss Mode.
	DGMGRL> show configura
	tion;
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	  Warning: ORA-16819
	: fast-start failover
	 observer not started
	  rdscdb_b - (*)
	 Physical standby
	 database
	Fast-Start Failover:
	 Enabled in Zero Data
	 Loss Mode
	Configuration Status:	

Tarefa	Descrição	Habilidades necessárias
	`WARNING (status updated 11 seconds ago)` `DGMGRL>`	

Tarefa	Descrição	Habilidades necessárias

Iniciar o observador para monitoramento do FSFO e verifique o status.	Você pode iniciar o observador antes ou depois de habilitar o FSFO. Se o FSFO já estiver habilitado, o observador imediatamente começará a monitorar o status e as conexões com os bancos de dados em espera primários e de destino. Se o FSFO não estiver habilitado, o observador não iniciará o monitoramento até que o FSFO seja habilitado.
	
	Quando você inicia o observador, a configuração primária do banco de dados será exibida sem nenhuma mensagem de erro, conforme evidenciado pelo comando anterior `show configuration` .
	
	Não CDB
	
	`DGMGRL> start observer;`
	`[W000 2022-12-01T06:16:51.271+00:00] FSFO target standby is orcl_d`
	`Observer 'ip-10-0-1-89' started`
	`[W000 2022-12-01T06:16:51.352+00:00] Observer trace level is set to USER`
		DBA

Tarefa	Descrição	Habilidades necessárias
	DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 56 seconds ago) DGMGRL> DGMGRL> show observer Configuration - rds_dg Primary: orcl_a Active Target: orcl_d Observer "ip-10-0- 1-89" - Master Host Name: ip-10-0-1 -89 Last Ping to Primary: 1 second ago Last Ping to Target: 1 second ago DGMGRL> CDB DGMGRL> start observer; Succeeded in opening the observer file "/home/oracle/fsfo _ip-10-0-1-56.dat". [W000 2023-01-1 8T07:31:32.589+00:00]	

Tarefa	Descrição	Habilidades necessárias
	FSFO target standby is rdscdb_b Observer 'ip-10-0-1-56' started The observer log file is '/home/oracle/observer_ip-10-0-1-56.log'. DGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 12 seconds ago) DGMGRL> DGMGRL> show observer; Configuration - rds_dg Primary: rdscdb_a Active Target: rdscdb_b Observer "ip-10-0-1-56" - Master Host Name: ip-10-0-1-56 Last Ping to Primary: 1 second ago Last Ping to Target: 2 seconds ago	

Tarefa	Descrição	Habilidades necessárias
	DGMGRL>	

Tarefa	Descrição	Habilidades necessárias
Verifique o failover.	Nesse cenário, um teste de failover pode ser realizado interrompendo manualmente a EC2 instância primária. Antes de interromper a EC2 instância, use o `tail` comando para monitorar o arquivo de log do observador com base na sua configuração. Use `DGMGRL` para iniciar sessão no banco de dados `orcl_d` em espera com o usuário `RDS_DATAGUARD` e verificar o status do Oracle Data Guard. Deve ser mostrado que `orcl_d` é o novo banco de dados primário. **Note** Nesse cenário de teste de failover, `orcl_d` está o banco de dados não CDB. Antes do failover, o banco de dados de flashback foi habilitado em `orcl_a`. Depois que o antigo banco de dados primário retorna on-line e inicia no estado `MOUNT`, o observador o restabelece em um novo banco de	DBA

Tarefa	Descrição	Habilidades necessárias
	dados em espera. O banco de dados restabelecido atua como o destino do FSFO para o novo banco de dados primário. Você pode verificar os detalhes nos logs do observador. `DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: orcl_d - Primary database Warning: ORA-16824 : multiple warnings, including fast-star t failover-related warnings, detected for the database orcl_a - (*) Physical standby database (disabled) ORA-16661: the standby database needs to be reinstated Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: WARNING (status updated 25 seconds ago) DGMGRL>`  A seguir, alguns exemplos de saída no `observer.log` .	

Tarefa	Descrição	Habilidades necessárias

	`$ tail -f /tmp/obse rver.log`
	`Unable to connect to database using rds_custom_orcl_a`
	`[W000 2023-01-1 8T07:50:32.589+00:00] Primary database cannot be reached.`
	`[W000 2023-01-1 8T07:50:32.589+00:00] Fast-Start Failover threshold has expired.`
	`[W000 2023-01-1 8T07:50:32.590+00:00] Try to connect to the standby.`
	`[W000 2023-01-1 8T07:50:32.590+00: 00] Making a last connection attempt to primary database before proceeding with Fast-Start Failover.`
	`[W000 2023-01-1 8T07:50:32.591+00:00] Check if the standby is ready for failover.`
	`[S002 2023-01-1 8T07:50:32.591+00:00] Fast-Start Failover started...`
	`2023-01-18T07:50 :32.591+00:00`
	`Initiating Fast-Star t Failover to database "orcl_d"...`
	`[S002 2023-01-1 8T07:50:32.592+00:00] Initiating Fast-start Failover.`	

Tarefa	Descrição	Habilidades necessárias
	Performing failover NOW, please wait... Failover succeeded, new primary is "orcl_d" 2023-01-18T07:55:32.101+00:00 [S002 2023-01-18T07:55:32.591+00:00] Fast-Start Failover finished... [W000 2023-01-18T07:55:32.591+00:00] Failover succeeded. Restart pinging. [W000 2023-01-18T07:55:32.603+00:00] Primary database has changed to orcl_d. [W000 2023-01-18T07:55:33.618+00:00] Try to connect to the primary. [W000 2023-01-18T07:55:33.622+00:00] Try to connect to the primary rds_custom_orcl_d. [W000 2023-01-18T07:55:33.634+00:00] The standby orcl_a needs to be reinstated [W000 2023-01-18T07:55:33.654+00:00] Try to connect to the new standby orcl_a. [W000 2023-01-18T07:55:33.654+00:00] Connection to the primary restored! [W000 2023-01-18T07:55:35.654+00:00] Disconnecting	

Tarefa	Descrição	Habilidades necessárias

	`from database rds_custom_orcl_d.`
	`[W000 2023-01-18T07:55:57.701+00:00] Try to connect to the new standby orcl_a.`
	`ORA-12170: TNS:Connect timeout occurred`	

Configurar a conectividade entre o aplicativo Oracle Peoplesoft e o banco de dados

Tarefa	Descrição	Habilidades necessárias
Criar e iniciar o serviço no banco de dados primário.	Você pode evitar alterações na configuração de aplicativo durante uma transição de função usando uma entrada TNS que contém os endpoints do banco de dados primário e em espera na configuração. Você pode definir dois serviços de banco de dados baseados em funções para dar suporte a workloads de leitura/gravação e somente leitura. No exemplo a seguir, `orcl_rw` é o serviço de leitura/gravação que está ativo no banco de dados primário. `orcl_ro` é o serviço somente leitura e está ativo no banco de dados em espera que foi aberto no modo somente leitura.	DBA

Tarefa	Descrição	Habilidades necessárias
	SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ---------- ORCL READ WRITE SQL> exec dbms_serv ice.create_service ('orcl_rw','orcl_r w'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.create_service ('orcl_ro','orcl_r o'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.start_service('orcl_rw'); PL/SQL procedure successfully completed . SQL>	

Tarefa	Descrição	Habilidades necessárias
Iniciar o serviço no banco de dados em espera.	Para iniciar o serviço no banco de dados em espera somente leitura, use o código a seguir. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- ORCL READ ONLY WITH APPLY SQL> exec dbms_serv ice.start_service( 'orcl_ro'); PL/SQL procedure successfully completed . SQL>`	DBA

Tarefa	Descrição	Habilidades necessárias
Automatizar a inicialização do serviço quando o banco de dados primário for reiniciado.	Para iniciar automaticamente o serviço no banco de dados primário quando ele for reiniciado, use o código a seguir. `SQL> CREATE OR REPLACE TRIGGER TrgDgServices after startup on database DECLARE db_role VARCHAR(30); db_open_mode VARCHAR(30); BEGIN SELECT DATABASE_ROLE, OPEN_MODE INTO db_role, db_open_mode FROM V$DATABASE; IF db_role = 'PRIMARY' THEN DBMS_SERV 2 ICE.START_SERVICE('orcl_rw'); END IF; IF db_role = 'PHYSICAL STANDBY' AND db_open_mode LIKE 'READ ONLY%' THEN DBMS_SERVICE.START_SERVICE('orcl_ro'); END IF; END; / Trigger created. SQL>`	DBA

Tarefa	Descrição	Habilidades necessárias
Configurar uma conexão entre os bancos de dados de leitura/gravação e somente leitura.	Você pode usar o seguinte exemplo de configuração de aplicativo para a conexão de leitura/gravação e somente leitura a seguir. `ORCL_RW = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com) (PORT=1521))) (CONNECT_DATA=(SERVICE_NAME = orcl_rw))) ORCL_RO = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2`	DBA

Tarefa	Descrição	Habilidades necessárias
	.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread .******.us-west-2. rds.amazonaws.com) (PORT=1521))) (CONNECT_DATA=(SERVIC E_NAME = orcl_ro)))	

Recursos relacionados

- Habilitar a alta disponibilidade com o Data Guard no Amazon RDS Custom para Oracle (Guia técnico da AWS)
- Configurando o Amazon RDS como um PeopleSoft banco de dados Oracle (whitepaper da AWS)
- Guia do Oracle Data Guard Broker (documentação de referência da Oracle)
- Conceitos e administração do Data Guard (documentação de referência da Oracle)
- Requisitos específicos de configuração de FAN e FCF do Oracle Data Guard (documentação de referência da Oracle)

Descarregue dados de um cluster do Amazon Redshift entre contas para o Amazon S3

Criado por Andrew Kamel (AWS)

Resumo

Ao testar aplicativos, é útil ter dados de produção em seu ambiente de teste. O uso de dados de produção pode fornecer uma avaliação mais precisa do aplicativo que você está desenvolvendo.

Esse padrão extrai dados de um cluster do Amazon Redshift em um ambiente de produção para um bucket do Amazon Simple Storage Service (Amazon S3) em um ambiente de desenvolvimento no Amazon Web Services ().AWS

O padrão percorre a configuração das contas DEV e PROD, incluindo o seguinte:

- Recursos necessários
- AWS Identity and Access Management Funções (IAM)
- Ajustes de rede em sub-redes, grupos de segurança e na nuvem privada virtual (VPC) para dar suporte à conexão do Amazon Redshift
- Um exemplo de AWS Lambda função com um tempo de execução em Python para testar a arquitetura

Para conceder acesso ao cluster do Amazon Redshift, o padrão é usado AWS Secrets Manager para armazenar as credenciais relevantes. O benefício é ter todas as informações necessárias para se conectar diretamente ao cluster do Amazon Redshift sem precisar saber onde o cluster do Amazon Redshift reside. Além disso, você pode monitorar o uso do segredo.

O segredo salvo no Secrets Manager inclui o host, o nome do banco de dados, a porta e as credenciais relevantes do cluster Amazon Redshift.

Para obter informações sobre considerações de segurança ao usar esse padrão, consulte a seção Melhores práticas.

Pré-requisitos e limitações

Pré-requisitos

- Um cluster do Amazon Redshift em execução na conta PROD
- Um bucket S3 criado na conta DEV
- Emparelhamento de VPC entre as contas DEV e PROD, com tabelas de rotas ajustadas adequadamente
- Nomes de host DNS e resolução de DNS habilitados para ambos emparelhados VPCs

Limitações

- Dependendo da quantidade de dados que você deseja consultar, a função Lambda pode atingir o tempo limite.

  Se sua execução demorar mais do que o tempo limite máximo do Lambda (15 minutos), use uma abordagem assíncrona para seu código Lambda. O exemplo de código desse padrão usa a biblioteca psycopg2 para Python, que atualmente não oferece suporte ao processamento assíncrono.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra a arquitetura de destino, com contas DEV e PROD.

O diagrama mostra o seguinte fluxo de trabalho:

1. A função Lambda na conta DEV assume a função do IAM necessária para acessar as credenciais do Amazon Redshift no Secrets Manager na conta PROD.

   Em seguida, a função Lambda recupera o segredo do cluster Amazon Redshift.
2. A função Lambda na conta DEV usa as informações para se conectar ao cluster Amazon Redshift na conta PROD por meio do peering. VPCs

   Em seguida, a função Lambda envia um comando de descarregamento para consultar o cluster do Amazon Redshift na conta PROD.
3. O cluster Amazon Redshift na conta PROD assume a função relevante do IAM para acessar o bucket do S3 na conta DEV.

O cluster Amazon Redshift descarrega os dados consultados no bucket do S3 na conta DEV.

Consultando dados do Amazon Redshift

O diagrama a seguir mostra as funções que são usadas para recuperar as credenciais do Amazon Redshift e conectar-se ao cluster do Amazon Redshift. O fluxo de trabalho é iniciado pela função Lambda.

O diagrama mostra o seguinte fluxo de trabalho:

1. O `CrossAccount-SM-Read-Role` na conta DEV pressupõe o `SM-Read-Role` na conta PROD.
2. A `SM-Read-Role` função usa a política anexada para recuperar o segredo do Secrets Manager.
3. As credenciais são usadas para acessar o cluster do Amazon Redshift.

Carregando dados para o Amazon S3

O diagrama a seguir mostra o processo de leitura e gravação entre contas para extrair dados e enviá-los para o Amazon S3. O fluxo de trabalho é iniciado pela função Lambda. O padrão encadeia as funções do IAM no Amazon Redshift. O comando unload que vem do cluster do Amazon Redshift assume `CrossAccount-S3-Write-Role` o e, em seguida, assume o. `S3-Write-Role` Esse encadeamento de funções dá ao Amazon Redshift acesso ao Amazon S3.

O fluxo de trabalho inclui as seguintes etapas:

1. O `CrossAccount-SM-Read-Role` na conta DEV pressupõe o `SM-Read-Role` na conta PROD.
2. Ele `SM-Read-Role` recupera as credenciais do Amazon Redshift do Secrets Manager.
3. A função Lambda se conecta ao cluster Amazon Redshift e envia uma consulta.
4. O cluster do Amazon Redshift pressupõe o. `CrossAccount-S3-Write-Role`
5. Isso `CrossAccount-S3-Write-Role` pressupõe que `S3-Write-Role` na conta DEV.
6. Os resultados da consulta são descarregados no bucket do S3 na conta DEV.

Ferramentas

Serviços da AWS

- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Redshift é um serviço de data warehouse em escala de petabytes gerenciado na Nuvem AWS.
- O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Repositório de código

O código desse padrão está disponível no repositório GitHub unload-redshift-to-s3-python.

Práticas recomendadas

Isenção de responsabilidade de segurança

Antes de implementar essa solução, considere as seguintes recomendações de segurança importantes:

- Lembre-se de que conectar as contas de desenvolvimento e produção pode aumentar o escopo e reduzir a postura geral de segurança. Recomendamos implantar essa solução apenas temporariamente, extraindo a parte necessária dos dados e destruindo imediatamente os recursos implantados. Para destruir os recursos, você deve excluir a função Lambda, remover todas as funções e políticas do IAM criadas para essa solução e revogar qualquer acesso à rede concedido entre as contas.
- Consulte suas equipes de segurança e conformidade antes de copiar quaisquer dados dos ambientes de produção para os de desenvolvimento. Informações de identificação pessoal (PII), informações de saúde protegidas (PHI) e outros dados confidenciais ou regulamentados geralmente não devem ser copiados dessa maneira. Copie somente informações não confidenciais disponíveis publicamente (por exemplo, dados de estoque público do front-end de uma loja). Considere tokenizar ou anonimizar dados, ou gerar dados de teste sintéticos, em vez

de usar dados de produção sempre que possível. Um dos princípios de AWS segurança é manter as pessoas afastadas dos dados. Em outras palavras, os desenvolvedores não devem realizar operações na conta de produção.

- Restrinja o acesso à função Lambda na conta de desenvolvimento porque ela pode ler dados do cluster Amazon Redshift no ambiente de produção.
- Para evitar a interrupção do ambiente de produção, implemente as seguintes recomendações:
  - Use uma conta de desenvolvimento separada e dedicada para atividades de teste e desenvolvimento.
  - Implemente controles rígidos de acesso à rede e limite o tráfego entre contas somente ao necessário.
  - Monitore e audite o acesso ao ambiente de produção e às fontes de dados.
  - Implemente controles de acesso com privilégios mínimos para todos os recursos e serviços envolvidos.
  - Revise e alterne regularmente as credenciais, como AWS Secrets Manager segredos e chaves de acesso à função do IAM.
- Consulte a documentação de segurança a seguir para os serviços usados neste artigo:
  - AWS Lambda segurança
  - Segurança do Amazon Redshift
  - Segurança do Amazon S3
  - AWS Secrets Manager segurança
  - Práticas recomendadas de segurança do IAM

A segurança é a principal prioridade ao acessar dados e recursos de produção. Sempre siga as melhores práticas, implemente controles de acesso com privilégios mínimos e revise e atualize regularmente suas medidas de segurança.

Épicos

Consulte dados do Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Crie um segredo para o cluster Amazon Redshift.	Para criar o segredo para o cluster do Amazon Redshift, faça o seguinte: 1. Na conta PROD, faça login no e abra o AWS Management Console console do Secrets Manager em https://console.aws.amazon.com/secretsmanager/. 2. Escolha Armazenar um novo segredo. 3. Selecione Credenciais para o armazém de dados do Amazon Redshift. 4. Em Nome de usuário e Senha, insira valores para sua instância e confirme ou escolha um valor para a chave de criptografia. 5. Escolha o armazém de dados do Amazon Redshift que seu segredo acessará. 6. Digite `Redshift-Creds-Secret` o nome secreto. 7. Conclua as etapas restantes da criação com as opções padrão e escolha Armazenar.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	8. Visualize seu segredo e anote o valor do ARN secreto que foi gerado para identificar o segredo.	

Tarefa	Descrição	Habilidades necessárias
Crie uma função para acessar o Secrets Manager.	Para criar a função, faça o seguinte: 1. Na conta PROD, abra o console do IAM em https://console.aws.amazon.com/iam/. 2. Selecione Políticas. 3. Selecione Criar política. 4. Escolha a guia JSON e, em seguida, insira uma política do IAM, como a seguinte: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "secretsmanager:GetResourcePolicy", "secretsmanager:GetSecretValue", "secretsmanager:DescribeSecret", "secretsmanager:ListSecretVersionIds" ], "Resource": [`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre>"<Redshift-Creds-Secret-ARN>"
	            ]
	        },
	        {
	            "Effect": "Allow",
	            "Action": "secretsmanager:ListSecrets",
	            "Resource": "*"
	        }
	    ]
	}</pre>
	`Redshift-Creds-Secret-ARN` Substitua pelo Amazon Resource Name (ARN) do segredo do Secrets Manager que contém as informações e as credenciais do cluster Amazon Redshift.	

Carregar dados no Amazon S3

Tarefa	Descrição	Habilidades necessárias
Crie uma função para acessar o bucket do S3.	Para criar a função para acessar o bucket do S3, faça o seguinte: 1. Na conta DEV, abra o console do IAM. 2. Selecione Políticas.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	3. Selecione Criar política. 4. Escolha a guia JSON e, em seguida, insira uma política do IAM, como a seguinte: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "kmsstmt", "Effect": "Allow", "Action": [ "kms:Decrypt", "kms:Encrypt", "kms:GenerateDataKey" ], "Resource": [ "<kms-key-arn>" ] }, { "Sid": "s3stmt", "Effect": "Allow", "Action": [ "s3:PutObject", "s3:Get*", "s3:List*" ], "Resource": [`	

Tarefa	Descrição	Habilidades necessárias

	<pre>"arn:aws:
	s3:::mybucket",
	"arn:aws:
	s3:::mybucket/*"
	]
	}
	]
	}</pre>
	`mybucket`Substitua pelo nome do bucket do S3 que você deseja acessar. Além disso, se o bucket do S3 estiver criptografado, `kms-key-arn` substitua-o pelo ARN da chave AWS KMS() usada para criptografar AWS Key Management Service o bucket do S3. Caso contrário, você não precisará da AWS KMS seção na política.
	5. Escolha Revisar política, insira `S3-Write-Policy` como nome da política e escolha Criar política.
	6. No painel de navegação, selecione Perfis.
	7. Escolha Criar Perfil.
	8. Para a função de entidade confiável, escolha Política de confiança personalizada.
	9. Escolha Avançar: Permissões e, em seguida,	

Tarefa	Descrição	Habilidades necessárias
	selecione a política S3-Write-Policy que você criou. 10. Insira `S3-Write-Role` como nome da função e, em seguida, escolha Criar função.	

Tarefa	Descrição	Habilidades necessárias
Crie a função do Amazon Redshift.	Para criar a função do Amazon Redshift, faça o seguinte: 1. Na conta PROD, abra o console do IAM. 2. Selecione Políticas. 3. Selecione Criar política. 4. Escolha a guia JSON e, em seguida, insira uma política do IAM, como a seguinte: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "CrossAccountPolicy", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "S3-Write-Role-ARN" } ] }` `S3-Write-Role-ARN`Substitua pelo ARN da conta `S3-Write-Role` DEV. 5. Escolha Revisar política, insira `S3-Write-Role-`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`Assume-Policy` como nome da política e escolha Criar política. 6. No painel de navegação, escolha Perfis e Criar perfil. 7. Escolha o serviço da AWS como seu tipo de entidade confiável e, em seguida, escolha Redshift, Redshift - Personalizável. 8. Escolha Avançar: Permissões e, em seguida, selecione a política S3-Write-Role-Assume-Policy que você criou. 9. Insira `CrossAccount-S3-Write-Role` como nome da função e, em seguida, escolha Criar função. 10 Associe a função do IAM ao seu cluster do Amazon Redshift.	

Implantar a função do Lambda

Tarefa	Descrição	Habilidades necessárias
Implante a função do Lambda.	Para implantar uma função Lambda na VPC emparelhada, faça o seguinte:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	1. Abra o console Lambda em. https://console.aws.amazon.com/lambda/ 2. Selecione Funções. 3. Escolha a opção Criar função. 4. Em Basic information (Informações básicas), para Function name (Nome da função), insira um nome para a função. 5. Em Runtime, escolha Python 3.8. 6. Expanda Alterar função de execução padrão e faça o seguinte: a. Escolha Usar um perfil existente. b. Em Função existente, selecione a função Lambda CrossAccount-RM-Read-Role que você criou anteriormente. 7. Expanda Configurações avançadas e faça o seguinte: a. Marque a caixa de seleção Ativar VPC. b. Para VPC, selecione a VPC emparelhada na conta DEV. c. Em Sub-redes, selecione a sub-rede privada.	

Tarefa	Descrição	Habilidades necessárias
	d. Em Security groups (Grupos de segurança), selecione o grupo de segurança padrão. 8. Escolha a opção Criar função. 9. Adicione a biblioteca psycopg2 como uma camada à função Lambda. **Note** Você pode usar uma camada já implantada do repositório psycopg2-lambda-layer. Certifique-se de usar o URL com base no seu tempo de execução Região da AWS e no Python.	

Teste a arquitetura

Tarefa	Descrição	Habilidades necessárias

Importe os recursos necessários.	Para importar os recursos necessários, execute os seguintes comandos:
	`import ast`
	`import boto3`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	`import psycopg2`
	`import base64`
	`from botocore.`
	`exceptions import`
	` ClientError`	

Tarefa	Descrição	Habilidades necessárias

Execute a função de manipulador do Lambda.	A função Lambda usa AWS Security Token Service (AWS STS) para acesso entre contas e gerenciamento temporário de credenciais. A função usa a operação AssumeRole da API para assumir temporariamente as permissões da função `sm_read_role` do IAM.
	
	Para executar a função Lambda, use o código de exemplo a seguir:
	
	`def lambda_handler(eve nt, context):`
	`  sts_client = boto3.client('sts')`
	
	`  # Secrets Manager Configurations`
	`  secret_name = "redshift_creds"`
	`  sm_region = "eu-west-1"`
	`  sm_read_role = "arn:aws:iam::PROD _ACCOUNT_NUMBER:role/ SM-Read-Role"`
	
	`  # S3 Bucket Configurations`
	`  s3_bucket_path = "s3://mybucket/"`
	`  s3_bucket_region = "eu-west-1"`
	`  s3_write_role = "arn:aws:iam::DEV_`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	ACCOUNT_NUMBER:role/S3-Write-Role"
	
	# Redshift Configurations
	sql_query = "select * from category"
	redshift_db = "dev"
	redshift_s3_write_role = "arn:aws:iam::PROD_ACCOUNT_NUMBER:role/CrossAccount-S3-Write-Role"
	
	chained_s3_write_role = "%s,%s" % (redshift_s3_write_role, s3_write_role)
	
	assumed_role_object = sts_client.assume_role(
	RoleArn=sm_read_role,
	RoleSessionName="CrossAccountRoleAssumption",
	ExternalId="YOUR_EXTERNAL_ID",
	)
	credentials = assumed_role_object['Credentials']
	
	secret_dict = ast.literal_eval(get_secret(credentials, secret_name, sm_region))
	execute_query(secret_dict, sql_query, s3_bucket_path,	

Tarefa	Descrição	Habilidades necessárias

	chained_s3_write_role, s3_bucket_region, redshift_db)
	
	    return {
	        'statusCode': 200
	    }	

Tarefa	Descrição	Habilidades necessárias

Descubra o segredo.	Para obter o segredo do Amazon Redshift, use o seguinte código de exemplo:
	
	`def get_secret(credentials, secret_name, sm_region):`
	`  # Create a Secrets Manager client`
	`  session = boto3.session.Session()`
	`  sm_client = session.client(`
	`  service_name='secretsmanager',`
	`  aws_access_key_id=credentials['AccessKeyId'],`
	`  aws_secret_access_key=credentials['SecretAccessKey'],`
	`  aws_session_token=credentials['SessionToken'],`
	`  region_name=sm_region`
	`  )`
	
	`  try:`
	`  get_secret_value_response = sm_client.get_secret_value(`
	`  SecretId=secret_name`
	`  )`
	`  except ClientError as e:`
	`  print(e)`
	`  raise e`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	<pre> else:
	        if 'SecretSt
	ring' in get_secre
	t_value_response:
	            return
	 get_secret_value_r
	esponse['SecretStr
	ing']
	        else:
	            return
	 base64.b64decode(g
	et_secret_value_re
	sponse['SecretBina
	ry'])</pre>	

Tarefa	Descrição	Habilidades necessárias

Execute o comando de descarga.	Para descarregar os dados no bucket do S3, use o código de exemplo a seguir.
	
	`def execute_query(secret_dict, sql_query, s3_bucket_path, chained_s3_write_role, s3_bucket_region, redshift_db):`
	`  conn_string = "dbname='%s' port='%s' user='%s' password='%s' host='%s'" \`
	`  % (redshift_db,`
	`  secret_dict["port"],`
	`  secret_dict["username"],`
	`  secret_dict["password"],`
	`  secret_dict["host"])`
	`  con = psycopg2.connect(conn_string)`
	`  unload_command = "UNLOAD ('{}') TO '{}' IAM_ROLE '{}' DELIMITER '|' REGION '{}';" \`
	`  .format(sql_query,`
	`  s3_bucket_path + str(datetime.datetime.now()) + ".csv",`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	<pre>chained_s3_write_role,
	
	s3_bucket_region)
	
	# Opening a cursor and run query
	cur = con.cursor()
	cur.execute(unload_command)
	
	print(cur.fetchone())
	cur.close()
	con.close()</pre>	

Limpeza

Tarefa	Descrição	Habilidades necessárias
Exclua a função do Lambda.	Para evitar custos não planejados, remova os recursos e a conexão entre as contas DEV e PROD. Para remover a função Lambda, faça o seguinte: 1. Abra o AWS Lambda console em https://console.aws.amazon.com/lambda/. 2. Localize e selecione a função Lambda que você criou.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	3. Escolha Ações e, em seguida, escolha Excluir. 4. Confirme a exclusão.	

Tarefa	Descrição	Habilidades necessárias
Remova as funções e políticas do IAM.	Remova as funções e políticas do IAM das contas DEV e PROD. Na conta DEV, faça o seguinte: 1. Abra o console do IAM. 2. Exclua as seguintes funções: • `S3-Write-Role` • `CrossAccount-RM-Read-Role` (Função Lambda) 3. Exclua as políticas associadas: • `S3-Write-Policy` • A CrossAccount política para assumir funções na conta PROD Na conta PROD, faça o seguinte: 1. Abra o console do IAM. 2. Exclua as seguintes funções: • `SM-Read-Role` • `CrossAccount-S3-Write-Role` 3. Exclua as políticas associadas:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• A CrossAccount política para acessar o Secrets Manager • `S3-Write-Role-Assume-Policy`	
Exclua o segredo no Secrets Manager.	Para excluir o segredo, faça o seguinte: 1. Na conta PROD, abra o console do Secrets Manager. 2. Localize e selecione o segredo chamado`Redshift-Creds-Secret` . 3. Escolha Actions (Ações) e selecione Delete secret (Excluir segredo). 4. Confirme a exclusão.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Remova as regras de emparelhamento de VPC e de grupos de segurança.	Para remover as regras de emparelhamento de VPC e de grupos de segurança, faça o seguinte: 1. Na conta PROD, abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/. 2. Navegue até Grupos de segurança. 3. Encontre o grupo de segurança usado pelo cluster do Amazon Redshift. 4. Edite as regras de entrada e remova a regra que permite conexões da Lambda VPC da conta DEV. 5. Navegue até Conexões de emparelhamento de VPC e exclua a conexão de emparelhamento.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Remova os dados do bucket do S3.	Para remover os dados do Amazon S3, faça o seguinte: 1. Na conta DEV, abra o console do Amazon S3 em. https://console.aws.amazon.com/s3/ 2. Localize o bucket que você usou para armazenamento de dados. 3. Exclua os objetos dentro do bucket ou exclua o bucket inteiro se não for mais necessário.	DevOps engenheiro
Limpe AWS KMS as chaves.	Se você criou alguma AWS KMS chave personalizada para criptografia, faça o seguinte: 1. Abra o AWS KMS console em https://console.aws.amazon.com/kms/. 2. Localize todas as chaves criadas para esse padrão. 3. Agende a exclusão das chaves. (Há um período de espera obrigatório para a exclusão da chave).	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Revise e exclua CloudWatch os registros da Amazon.	Para excluir os CloudWatch registros, faça o seguinte: 1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/. 2. Verifique se há grupos de log criados pela sua função Lambda ou pelo cluster do Amazon Redshift. 3. Exclua esses grupos de registros se eles não forem mais necessários.	DevOps engenheiro

Recursos relacionados

- CloudWatch Documentação da Amazon
- Documentação do IAM
- Documentação do Lambda
- Documentação do Amazon Redshift
- Documentação do Amazon S3
- AWS Secrets Manager documentação
- AWS princípios de segurança

Mais informações

Depois de descarregar os dados do Amazon Redshift para o Amazon S3, você pode analisá-los usando o Amazon Athena.

O Amazon Athena é um serviço de consulta de big data que é benéfico quando você precisa acessar grandes volumes de dados. Você pode usar o Athena sem precisar provisionar servidores ou bancos de dados. O Athena oferece suporte a consultas complexas e você pode executá-lo em objetos diferentes.

Como acontece com a maioria Serviços da AWS, o principal benefício de usar o Athena é que ele oferece grande flexibilidade na forma como você executa consultas sem a complexidade adicional. Ao usar o Athena, você pode consultar diferentes tipos de dados, como CSV e JSON, no Amazon S3 sem alterar o tipo de dados. Você pode consultar dados de várias fontes, inclusive externas AWS. O Athena reduz a complexidade porque você não precisa gerenciar servidores. O Athena lê dados diretamente do Amazon S3 sem carregar ou alterar os dados antes de você executar a consulta.

Padrões de migração de base de dados por workload

Tópicos

- IBM
- Microsoft
- N/D
- Código aberto
- Oracle
- SAP

IBM

- Migre um banco de dados Db2 da Amazon para o EC2 Aurora MySQL compatível usando o AWS DMS
- Migre o Db2 for LUW para a Amazon EC2 usando o envio de registros para reduzir o tempo de interrupção
- Migre o Db2 for LUW para a Amazon EC2 com recuperação de desastres de alta disponibilidade
- Migre do IBM Db2 na Amazon para o EC2 Aurora compatível com PostgreSQL usando o AWS DMS e o AWS SCT
- Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2
- Transmita dados do IBM Db2, SAP, Sybase e outros bancos de dados para o MongoDB Atlas em AWS

Microsoft

- Acelere a descoberta e a migração de cargas de trabalho da Microsoft para a AWS
- Acesse tabelas locais do Microsoft SQL Server a partir do Microsoft SQL Server na Amazon EC2 usando servidores vinculados
- Avaliar o desempenho das consultas para migrar bancos de dados do SQL Server para o MongoDB Atlas na AWS
- Automatize tarefas de banco de dados na edição SQL Server Express em execução na Amazon EC2 usando AWS Lambda um Agendador de Tarefas
- Altere os aplicativos Python e Perl para oferecer suporte à migração do banco de dados do Microsoft SQL Server para o Amazon Aurora Edição Compatível com PostgreSQL
- Configurar o roteamento somente leitura em um grupo de disponibilidade Always On (Sempre ativo) no SQL Server na AWS
- Crie CloudFormation modelos da AWS para tarefas do AWS DMS usando Microsoft Excel e Python
- Implante instâncias de cluster de failover do SQL Server na Amazon EC2 e na Amazon FSx usando o Terraform
- Exportar um banco de dados do Microsoft SQL Server para o Amazon S3 usando o AWS DMS
- Exporter tabelas do Amazon RDS para SQL Server para um bucket do S3 usando o AWS DMS
- Implemente SHA1 o hashing para dados de PII ao migrar do SQL Server para o PostgreSQL
- Ingira e migre instâncias EC2 do Windows para uma conta do AWS Managed Services
- Migrar uma fila de mensagens do Microsoft Azure Service Bus para o Amazon SQS
- Migre um banco de dados Microsoft SQL Server da Amazon EC2 para o Amazon DocumentDB usando o AWS DMS
- Migre um banco de dados Microsoft SQL Server para o Aurora MySQL usando o AWS DMS e o AWS SCT
- Migre uma aplicação .NET do Microsoft Azure App Service para o AWS Elastic Beanstalk
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando servidores vinculados

- Saiba como migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando backup e restauração nativos.
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift utilizando o AWS DMS
- Migre um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift usando agentes de extração de dados da AWS SCT
- Migre um banco de dados local do Microsoft SQL Server para o Microsoft SQL Server na Amazon executando Linux EC2
- Migre dados do Microsoft Azure Blob para o Amazon S3 usando o Rclone
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2 usando o Application Migration Service
- Migre um banco de dados relacional para o MongoDB Atlas em AWS
- Migre o SQL Server para a AWS usando grupos de disponibilidade distribuídos
- Migrar certificados SSL do Windows para um Application Load Balancer usando o ACM
- Redefinir a hospedagem de workloads on-premises na Nuvem AWS: lista de verificação de migração
- Resolva erros de conexão após migrar o Microsoft SQL Server para a Nuvem AWS
- Envie notificações para uma instância de banco de dados Amazon RDS para SQL Server usando um servidor SMTP on-premises e o Database Mail
- Configure um pipeline de CI/CD para migração de banco de dados usando o Terraform
- Configure a infraestrutura Multi-AZ para um SQL Server Always On FCI usando a Amazon FSx

N/D

- Crie um processo de aprovação para solicitações de firewall durante uma migração de rehospedagem para AWS
- Criptografe uma instância de banco de dados Amazon RDS para PostgreSQL existente
- Estime os custos de armazenamento de uma tabela do Amazon DynamoDB
- Implemente a recuperação de desastres entre regiões com o AWS DMS e o Amazon Aurora

Código aberto

- Gere automaticamente um modelo PyNamoDB e funções CRUD para o Amazon DynamoDB usando um aplicativo Python
- Conecte-se usando um túnel SSH no pgAdmin
- Crie usuários e funções do aplicativo no Aurora compatível com PostgreSQL
- Habilite conexões criptografadas para instâncias de banco de dados PostgreSQL no Amazon RDS
- Migre o Amazon RDS for Oracle para o Amazon AWS SCT RDS for PostgreSQL com e usando e AWS DMSAWS CLIAWS CloudFormation
- Migre um banco de dados MariaDB on-premises para o Amazon RDS para MariaDB usando ferramentas nativas
- Migre um banco de dados MySQL local para a Amazon EC2
- Migrar um banco de dados MySQL on-premises para o Amazon RDS para MySQL
- Migrar um banco de dados MySQL on-premises para o Aurora MySQL
- Migrar um banco de dados PostgreSQL on-premises para o Aurora PostgreSQL
- Migrar um banco de dados do Couchbase Server para a Amazon EC2
- Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2 com o Auto Scaling
- Migre do Oracle 8i ou 9i para o Amazon RDS for Oracle usando o AWS DMS SharePlex
- Migre da Oracle GlassFish para o AWS Elastic Beanstalk
- Migre do PostgreSQL na Amazon para o EC2 Amazon RDS for PostgreSQL usando pglogical
- Migre o ML Crie, treine e implante cargas de trabalho para a Amazon SageMaker usando as ferramentas do desenvolvedor da AWS
- Migrar aplicações Java on-premises para a AWS usando o App2Container da AWS
- Migre bancos de dados MySQL locais para o Aurora MySQL usando XtraBackup Percona, Amazon EFS e Amazon S3
- Migre tabelas externas da Oracle para a compatibilidade com o Amazon Aurora PostgreSQL
- Migre funções e procedimentos do Oracle que tenham mais de 100 argumentos para o PostgreSQL
- Migre cargas de trabalho do Redis para o Redis Enterprise Cloud na AWS
- Monitore o Amazon Aurora em busca de instâncias sem criptografia

- Reinicie o AWS Replication Agent automaticamente sem desativá-lo SELinux após a reinicialização de um servidor de origem RHEL
- Agendar trabalhos para o Amazon RDS para PostgreSQL e Aurora PostgreSQL usando o Lambda e o Secrets Manager
- Configure a replicação de dados entre o Amazon RDS for MySQL e o MySQL na Amazon usando o GTID EC2
- Transporte bancos de dados PostgreSQL entre duas instâncias de banco de dados Amazon RDS usando pg_transport
- Descarregue dados de um cluster do Amazon Redshift entre contas para o Amazon S3

Oracle

- Adicione HA ao Oracle PeopleSoft no Amazon RDS Custom usando uma réplica de leitura
- Converta consultas JSON Oracle em SQL do banco de dados PostgreSQL
- Converter VARCHAR2 (1) tipo de dados para Oracle para tipo de dados booleano para Amazon Aurora PostgreSQL
- Emule o Oracle DR usando um banco de dados global Aurora compatível com PostgreSQL
- Emule workloads do Oracle RAC usando endpoints personalizados no Aurora PostgreSQL
- Estime o tamanho do mecanismo Amazon RDS para um banco de dados Oracle usando relatórios AWR
- Manipule blocos anônimos em instruções de SQL dinâmico no Aurora PostgreSQL
- Lide com funções sobrecarregadas do Oracle no Aurora compatível com PostgreSQL
- Migre incrementalmente do Amazon RDS para Oracle para o Amazon RDS para PostgreSQL usando o Oracle SQL Developer e o AWS SCT
- Faça o upload de arquivos BLOB em TEXT usando a codificação de arquivos no Aurora PostgreSQL-Compatible
- Migre instâncias do banco de dados Amazon RDS para Oracle para outras contas que usam AMS
- Migre o Amazon RDS para Oracle para o Amazon RDS para PostgreSQL no modo SSL usando o AWS DMS
- Migre um banco de dados Amazon RDS for Oracle para Conta da AWS outro Região da AWS e AWS DMS use-o para replicação contínua
- Migrar uma instância do banco de dados Amazon RDS para Oracle para outra VPC
- Migre um banco de dados Oracle local para a Amazon EC2 usando o Oracle Data Pump
- Migre um banco de dados Oracle local para o Amazon OpenSearch Service usando o Logstash
- Migre um banco de dados Oracle on-premises para o Amazon RDS para MySQL, usando o AWS DMS e o AWS SCT.
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump Import direto em um link de banco de dados
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para PostgreSQL usando um Oracle bystander e o AWS DMS

- Migre um banco de dados Oracle local para o Oracle na Amazon EC2
- Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for MariaDB usando o AWS DMS e o AWS SCT
- Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for Oracle usando o AWS DMS
- Migrar um banco de dados Oracle para o Amazon DynamoDB usando AWS DMS
- Migre um banco de dados Oracle para o Amazon RDS for Oracle usando adaptadores de arquivo simples GoldenGate Oracle
- Migre um banco de dados Oracle para o Amazon Redshift usando o AWS DMS e o AWS SCT
- Migrar um banco de dados Oracle para o Aurora PostgreSQL usando AWS DMS e AWS SCT
- Migre um banco de dados Oracle JD Edwards EnterpriseOne para a AWS usando o Oracle Data Pump e o AWS DMS
- Migre uma tabela particionada do Oracle para o PostgreSQL usando o AWS DMS
- Migre um PeopleSoft banco de dados Oracle para a AWS usando o AWS DMS
- Migrar dados de um banco de dados Oracle on-premises para o Aurora PostgreSQL
- Migre do Amazon RDS para Oracle para o Amazon RDS para MySQL
- Migre do Oracle 8i ou 9i para o Amazon RDS para PostgreSQL usando visões materializadas e o AWS DMS
- Migre do Oracle 8i ou 9i para o Amazon RDS for PostgreSQL usando o AWS DMS SharePlex
- Migre do banco de dados Oracle para o Amazon RDS for PostgreSQL usando o Oracle GoldenGate
- Migre do Oracle na Amazon EC2 para o Amazon RDS for MySQL usando o AWS DMS e o AWS SCT
- Migrar do Oracle para o Amazon DocumentDB usando o AWS DMS
- Migre do Oracle WebLogic para o Apache Tomcat (TomEE) no Amazon ECS
- Migre índices baseados em funções do Oracle para o PostgreSQL
- Migre aplicativos legados do Oracle Pro*C para o ECPG
- Migrar valores do Oracle CLOB para linhas individuais no PostgreSQL na AWS
- Migre códigos de erro do banco de dados Oracle para um banco de dados compatível com Amazon Aurora PostgreSQL
- Migre o Oracle E-Business Suite para o Amazon RDS Custom
- Migre funções nativas do Oracle para o PostgreSQL usando extensões

- Migrar variáveis de ligação Oracle OUT para um banco de dados PostgreSQL
- Migre o Oracle PeopleSoft para o Amazon RDS Custom
- Migre a funcionalidade Oracle ROWID para o PostgreSQL na AWS
- Migrar os pacotes de pragma Oracle SERIALLY_REUSABLE para o PostgreSQL
- Migre colunas geradas virtualmente do Oracle para o PostgreSQL
- Monitore GoldenGate os logs do Oracle usando a Amazon CloudWatch
- Redefinir a plataforma do Oracle Database Enterprise Edition para o Standard Edition 2 no Amazon RDS para Oracle
- Configure uma arquitetura de HA/DR para o Oracle E-Business Suite no Amazon RDS Custom com um banco de dados ativo em espera
- Configure a funcionalidade Oracle UTL_FILE no Aurora compatível com PostgreSQL
- Funções de transição para um PeopleSoft aplicativo Oracle no Amazon RDS Custom for Oracle
- Valide objetos de banco de dados após migrar do Oracle para o Amazon Aurora PostgreSQL

SAP

- Faça backup automático dos bancos de dados SAP HANA usando o Systems Manager e EventBridge
- Migre um banco de dados SAP ASE local para a Amazon EC2
- Migre do SAP ASE para o Amazon RDS para SQL Server usando o AWS DMS
- Migre o SAP ASE na Amazon EC2 para o Amazon Aurora compatível com PostgreSQL usando o AWS SCT e o AWS DMS
- Migre o SAP HANA para a AWS usando o SAP HSR com o mesmo nome de host
- Reduza o tempo de substituição homogêneo da migração do SAP usando o Application Migration Service
- Configure a recuperação de desastres para SAP no IBM Db2 na AWS

Mais padrões

- Acesse um banco de dados Amazon Neptune a partir de um contêiner Amazon EKS
- Acesse, consulte e una tabelas do Amazon DynamoDB usando o Athena
- Dados agregados no Amazon DynamoDB para previsão de ML no Athena
- Permitir que EC2 as instâncias gravem acesso aos buckets do S3 nas contas do AMS
- Analise e visualize dados JSON aninhados com o Amazon Athena e o Amazon QuickSight
- Autentique o Microsoft SQL Server na Amazon EC2 usando o AWS Directory Service
- Automatize backups para instâncias de banco de dados do Amazon RDS para PostgreSQL usando o AWS Batch
- Arquivar automaticamente itens no Amazon S3 usando o DynamoDB TTL
- Corrija automaticamente instâncias e clusters de banco de dados Amazon RDS não criptografados
- Pare e inicie automaticamente uma instância de banco de dados Amazon RDS usando o Windows AWS Systems Manager de manutenção
- Crie uma arquitetura pouco acoplada com microsserviços usando DevOps práticas e o AWS Cloud9
- Crie programas COBOL Db2 usando e AWS Mainframe ModernizationAWS CodeBuild
- Crie uma malha de dados corporativa com a Amazon DataZone, AWS CDK, e AWS CloudFormation
- Altere os aplicativos Python e Perl para oferecer suporte à migração do banco de dados do Microsoft SQL Server para o Amazon Aurora Edição Compatível com PostgreSQL
- Converta e descompacte dados EBCDIC em ASCII na AWS usando Python
- Converta o atributo temporal Teradata NORMALIZE em Amazon Redshift SQL
- Converter o atributo Teradata RESET WHEN para Amazon Redshift SQL
- Converter VARCHAR2 (1) tipo de dados para Oracle para tipo de dados booleano para Amazon Aurora PostgreSQL
- Crie usuários e funções do aplicativo no Aurora compatível com PostgreSQL
- Crie CloudFormation modelos da AWS para tarefas do AWS DMS usando Microsoft Excel e Python
- Entregue registros do DynamoDB para o Amazon S3 usando o Kinesis Data Streams e o Firehose com AWS CDK

- Implemente um cluster Cassandra na Amazon EC2 com estática privada IPs para evitar o reequilíbrio
- Desenvolva assistentes avançados baseados em bate-papo com IA generativa usando RAG e prompting ReAct
- Emule o Oracle DR usando um banco de dados global Aurora compatível com PostgreSQL
- Suporte para criptografia de dados transparente no Amazon RDS para SQL Server
- Exportar um banco de dados do Microsoft SQL Server para o Amazon S3 usando o AWS DMS
- Implemente SHA1 o hashing para dados de PII ao migrar do SQL Server para o PostgreSQL
- Migre incrementalmente do Amazon RDS para Oracle para o Amazon RDS para PostgreSQL usando o Oracle SQL Developer e o AWS SCT
- Faça o upload de arquivos BLOB em TEXT usando a codificação de arquivos no Aurora PostgreSQL-Compatible
- Gerenciar credenciais usando o AWS Secrets Manager
- Migre um banco de dados Db2 da Amazon para o EC2 Aurora MySQL compatível usando o AWS DMS
- Migre um banco de dados Microsoft SQL Server da Amazon EC2 para o Amazon DocumentDB usando o AWS DMS
- Migre um banco de dados Microsoft SQL Server para o Aurora MySQL usando o AWS DMS e o AWS SCT
- Migre um ambiente MongoDB auto-hospedado para o MongoDB Atlas em AWS
- Migre um banco de dados Teradata para o Amazon Redshift usando agentes de extração de dados do AWS SCT
- Migre o Amazon RDS para Oracle para o Amazon RDS para PostgreSQL no modo SSL usando o AWS DMS
- Migre o Amazon RDS for Oracle para o Amazon AWS SCT RDS for PostgreSQL com e usando e AWS DMSAWS CLIAWS CloudFormation
- Migrar uma instância do banco de dados Amazon RDS para outra VPC ou outra conta
- Migre um banco de dados Amazon RDS for Oracle para Conta da AWS outro Região da AWS e AWS DMS use-o para replicação contínua
- Migrar uma instância do banco de dados Amazon RDS para Oracle para outra VPC
- Migre um cluster do Amazon Redshift para uma região da AWS na China

- Migre um banco de dados MariaDB on-premises para o Amazon RDS para MariaDB usando ferramentas nativas
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando servidores vinculados
- Saiba como migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando backup e restauração nativos.
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift utilizando o AWS DMS
- Migre um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift usando agentes de extração de dados da AWS SCT
- Migre um banco de dados local do Microsoft SQL Server para o Microsoft SQL Server na Amazon executando Linux EC2
- Migre um banco de dados MySQL local para a Amazon EC2
- Migrar um banco de dados MySQL on-premises para o Amazon RDS para MySQL
- Migrar um banco de dados MySQL on-premises para o Aurora MySQL
- Migre um banco de dados Oracle local para a Amazon EC2 usando o Oracle Data Pump
- Migre um banco de dados Oracle local para o Amazon OpenSearch Service usando o Logstash
- Migre um banco de dados Oracle on-premises para o Amazon RDS para MySQL, usando o AWS DMS e o AWS SCT.
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump Import direto em um link de banco de dados
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para PostgreSQL usando um Oracle bystander e o AWS DMS
- Migre um banco de dados Oracle local para o Oracle na Amazon EC2
- Migrar um banco de dados PostgreSQL on-premises para o Aurora PostgreSQL
- Migre um banco de dados SAP ASE local para a Amazon EC2

- Migre um banco de dados ThoughtSpot Falcon local para o Amazon Redshift
- Migre um banco de dados Vertica on-premises para o Amazon Redshift usando agentes de extração de dados do AWS SCT
- Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for MariaDB usando o AWS DMS e o AWS SCT
- Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for Oracle usando o AWS DMS
- Migrar um banco de dados Oracle para o Amazon DynamoDB usando AWS DMS
- Migre um banco de dados Oracle para o Amazon RDS for Oracle usando adaptadores de arquivo simples GoldenGate Oracle
- Migre um banco de dados Oracle para o Amazon Redshift usando o AWS DMS e o AWS SCT
- Migrar um banco de dados Oracle para o Aurora PostgreSQL usando AWS DMS e AWS SCT
- Migre um banco de dados Oracle JD Edwards EnterpriseOne para a AWS usando o Oracle Data Pump e o AWS DMS
- Migre uma tabela particionada do Oracle para o PostgreSQL usando o AWS DMS
- Migre um PeopleSoft banco de dados Oracle para a AWS usando o AWS DMS
- Migrar um banco de dados do Couchbase Server para a Amazon EC2
- Migrar dados de um banco de dados Oracle on-premises para o Aurora PostgreSQL
- Migre dados para o Nuvem AWS usando o Starburst
- Migre o Db2 for LUW para a Amazon EC2 usando o envio de registros para reduzir o tempo de interrupção
- Migre o Db2 for LUW para a Amazon EC2 com recuperação de desastres de alta disponibilidade
- Migre do Amazon RDS para Oracle para o Amazon RDS para MySQL
- Migre do Couchbase Server para o Couchbase Capella na AWS
- Migre do IBM Db2 na Amazon para o EC2 Aurora compatível com PostgreSQL usando o AWS DMS e o AWS SCT
- Migre do Oracle 8i ou 9i para o Amazon RDS para PostgreSQL usando visões materializadas e o AWS DMS
- Migre do Oracle 8i ou 9i para o Amazon RDS for PostgreSQL usando o AWS DMS SharePlex
- Migre do banco de dados Oracle para o Amazon RDS for PostgreSQL usando o Oracle GoldenGate

- Migre do Oracle na Amazon EC2 para o Amazon RDS for MySQL usando o AWS DMS e o AWS SCT
- Migrar do Oracle para o Amazon DocumentDB usando o AWS DMS
- Migre do PostgreSQL na Amazon para o EC2 Amazon RDS for PostgreSQL usando pglogical
- Migre do SAP ASE para o Amazon RDS para SQL Server usando o AWS DMS
- Migre índices baseados em funções do Oracle para o PostgreSQL
- Migre aplicativos legados do Oracle Pro*C para o ECPG
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2 usando o Application Migration Service
- Migre workloads on-premises da Cloudera para a Cloudera Data Platform na AWS
- Migre bancos de dados MySQL locais para o Aurora MySQL usando XtraBackup Percona, Amazon EFS e Amazon S3
- Migrar o Oracle Business Intelligence 12c para a Nuvem AWS a partir de servidores on-premises
- Migrar valores do Oracle CLOB para linhas individuais no PostgreSQL na AWS
- Migre códigos de erro do banco de dados Oracle para um banco de dados compatível com Amazon Aurora PostgreSQL
- Migre o Oracle E-Business Suite para o Amazon RDS Custom
- Migre tabelas externas da Oracle para a compatibilidade com o Amazon Aurora PostgreSQL
- Migre funções nativas do Oracle para o PostgreSQL usando extensões
- Migre o Oracle PeopleSoft para o Amazon RDS Custom
- Migre a funcionalidade Oracle ROWID para o PostgreSQL na AWS
- Migrar os pacotes de pragma Oracle SERIALLY_REUSABLE para o PostgreSQL
- Migre cargas de trabalho do Redis para o Redis Enterprise Cloud na AWS
- Migre um banco de dados relacional para o MongoDB Atlas em AWS
- Migre o SAP ASE na Amazon EC2 para o Amazon Aurora compatível com PostgreSQL usando o AWS SCT e o AWS DMS
- Migre colunas geradas virtualmente do Oracle para o PostgreSQL
- Configure um espaço de dados mínimo viável para compartilhar dados entre organizações
- Monitore ElastiCache clusters da Amazon para criptografia em repouso
- Monitore ElastiCache clusters para grupos de segurança
- Consulte tabelas do Amazon DynamoDB com SQL usando o Amazon Athena

- Reduza o tempo de substituição homogêneo da migração do SAP usando o Application Migration Service
- Alternar as credenciais do banco de dados sem reiniciar os contêineres
- Executar workloads orientadas por mensagens em grande escala usando o AWS Fargate
- Proteja e simplifique o acesso de usuários em um banco de dados de federação Db2 na AWS usando contextos confiáveis
- Configure uma PeopleSoft arquitetura altamente disponível na AWS
- Configure a funcionalidade Oracle UTL_FILE no Aurora compatível com PostgreSQL
- Transmita dados do IBM Db2, SAP, Sybase e outros bancos de dados para o MongoDB Atlas em AWS
- Simplifique as implantações do PostgreSQL no Amazon EKS usando o PGO
- Transferir dados do Db2 z/OS em grande escala para o Amazon S3 em arquivos CSV
- Transporte bancos de dados PostgreSQL entre duas instâncias de banco de dados Amazon RDS usando pg_transport
- Valide objetos de banco de dados após migrar do Oracle para o Amazon Aurora PostgreSQL
- Verificar se os novos clusters do Amazon Redshift são executados em uma VPC

Armazenamento e backup

Tópicos

- Permitir que EC2 as instâncias gravem acesso aos buckets do S3 nas contas do AMS
- Automatize a ingestão do fluxo de dados em um banco de dados Snowflake usando o Snowflake Snowpipe, o Amazon S3, o Amazon SNS e o Amazon Data Firehose
- Criptografe automaticamente volumes novos e existentes do Amazon EBS
- Faça backup dos servidores Sun SPARC no emulador Stromasys Charon-SSP na nuvem AWS
- Faça backup e arquive dados no Amazon S3 com o Veeam Backup & Replication
- Configurar a Veritas NetBackup para VMware nuvem na AWS
- Copiar dados de um bucket do S3 para outra conta e região usando a AWS CLI
- Copie dados de um bucket do S3 para outra conta e região usando o S3 Batch Replication
- Migre dados de um ambiente Hadoop local para o Amazon S3 usando com a AWS para o Amazon S3 DistCp PrivateLink
- Mais padrões

Permitir que EC2 as instâncias gravem acesso aos buckets do S3 nas contas do AMS

Criado por Mansi Suratwala (AWS)

Resumo

AWS Managed Services (AMS) ajuda você a operar sua AWS infraestrutura com mais eficiência e segurança. As contas do AMS têm proteções de segurança para a administração padronizada de seus recursos. AWS Uma barreira é que os perfis de instância padrão do Amazon Elastic Compute Cloud (Amazon EC2) não permitem acesso de gravação aos buckets do Amazon Simple Storage Service (Amazon S3). No entanto, sua organização pode ter vários buckets do S3 e exigir mais controle sobre o acesso por EC2 instâncias. Por exemplo, talvez você queira armazenar backups de banco de dados de EC2 instâncias em um bucket do S3.

Esse padrão explica como usar requests for change (RFCs) para permitir que suas EC2 instâncias gravem acesso aos buckets do S3 na sua conta do AMS. Uma RFC é uma solicitação criada por você ou pelo AMS para fazer uma alteração em seu ambiente gerenciado e que inclui uma ID do tipo de alteração (CT) para uma operação específica.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta do AMS Advanced. Para obter mais informações sobre isso, consulte os planos de operações do AMS na documentação do AMS.
- Acesso à `customer-mc-user-role` função AWS Identity and Access Management (IAM) a ser enviada RFCs.
- AWS Command Line Interface (AWS CLI), instalado e configurado com as EC2 instâncias em sua conta do AMS.
- Uma compreensão de como criar e enviar RFCs no AMS. Para obter mais informações sobre isso, consulte Quais são os tipos de alteração do AMS? na documentação do AMS.
- Uma compreensão dos tipos de mudança manual e automatizada (CTs). Para obter mais informações sobre isso, consulte Automatizado e manual CTs na documentação do AMS.

Arquitetura

Pilha de tecnologia

- AMS
- AWS CLI
- Amazon EC2
- Amazon S3
- IAM

Ferramentas

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Managed Services (AMS) ajuda você a operar sua infraestrutura da AWS com mais eficiência e segurança.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.

Épicos

Criar um bucket do S3 com um RFC

Tarefa	Descrição	Habilidades necessárias
Crie um bucket S3 usando um RFC automatizado.	1. Faça login na sua conta AMS, escolha a página Escolher tipo de alteração , escolha e RFCs, em seguida, escolha Criar RFC. 2. Envie o RFC automatizado Create S3 Bucket.	Administrador de sistemas da AWS, desenvolvedor da AWS

Tarefa	Descrição	Habilidades necessárias
	Note Certifique-se de registrar o nome do bucket do S3.	

Crie um perfil de instância do IAM e associe-o às EC2 instâncias

Tarefa	Descrição	Habilidades necessárias
Envie um RFC manual para criar um perfil do IAM .	Quando uma conta do AMS é integrada, um perfil de instância do IAM padrão chamado `customer-mc-ec2-instance-profile` é criado e associado a cada EC2 instância na sua conta do AMS. No entanto, o perfil da instância não tem permissões de gravação em seus buckets do S3. Para adicionar as permissões de gravação, envie a RFC do manual Create IAM Resource para criar uma função do IAM que tenha as três políticas a seguir: `customer_ec2_instance_ customer_deny_policy` , e. `customer_ec2_s3_integration_policy`	Administrador de sistemas da AWS, desenvolvedor da AWS

Tarefa	Descrição	Habilidades necessárias
	Important As `customer_deny_policy` políticas `customer_ec2_instance_` e já existem na sua conta do AMS. No entanto, você precisa criar `customer_ec2_s3_integration_policy` usando o seguinte exemplo de política:	

```
{
  "Version": "2012-10-17",
   "Statement": [
    {
      "Sid": "",
       "Effect": "Allow",
       "Principal": {
         "Service": "ec2.amazonaws.com"
      },
       "Action": "sts:AssumeRole"
    }
  ]
}

Role Permissions:
{
```

Tarefa	Descrição	Habilidades necessárias
	"Version": "2012-10-17", "Statement": [{ "Action": ["s3:ListBucket", "s3:GetBucketLocation"], "Resource": "arn:aws:s3:::", "Effect": "Allow" }, { "Action": ["s3:GetObject", "s3:PutObject", "s3:ListMultipartUploadParts", "s3:AbortMultipartUpload"], "Resource": "arn:aws:s3:::/*", "Effect": "Allow" }] }	

Tarefa	Descrição	Habilidades necessárias
Envie um RFC para substituir o perfil de instância do IAM.	Envie um RFC manual para associar as EC2 instâncias de destino ao novo perfil de instância do IAM.	Administrador de sistemas da AWS, desenvolvedor da AWS
Testar uma operação de cópia no bucket do S3.	Teste uma operação de cópia no bucket do S3 executando o seguinte comando no AWS CLI: `aws s3 cp test.txt s3://<S3 bucket>/test2.txt`	Administrador de sistemas da AWS, desenvolvedor da AWS

Recursos relacionados

- Crie um perfil de instância do IAM para suas EC2 instâncias da Amazon
- Criação de um bucket do S3 (usando o console do Amazon S3 AWS SDKs, ou) AWS CLI

Automatize a ingestão do fluxo de dados em um banco de dados Snowflake usando o Snowflake Snowpipe, o Amazon S3, o Amazon SNS e o Amazon Data Firehose

Criado por Bikash Chandra Rout (AWS)

Resumo

Esse padrão descreve como você pode usar serviços na nuvem Amazon Web Services (AWS) para processar um fluxo contínuo de dados e carregá-lo em um banco de dados Snowflake. O padrão usa o Amazon Data Firehose para entregar os dados ao Amazon Simple Storage Service (Amazon S3), ao Amazon Simple Notification Service (Amazon SNS) para enviar notificações quando novos dados são recebidos e ao Snowflake Snowpipe para carregar os dados em um banco de dados do Snowflake.

Seguindo esse padrão, você pode ter dados gerados continuamente para análise em segundos, evitar vários `COPY` comandos manuais e ter suporte total para dados semiestruturados em carga.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Uma fonte de dados que envia dados continuamente para um stream de entrega do Firehose.
- Um bucket S3 existente que está recebendo os dados do stream de entrega do Firehose.
- Uma conta ativa do Snowflake.

Limitações

- O Snowflake Snowpipe não se conecta diretamente ao Firehose.

Arquitetura

Pilha de tecnologia

- Amazon Data Firehose

- Amazon SNS
- Amazon S3
- Snowflake
- Banco de dados do Snowflake

Ferramentas

- O Amazon Data Firehose é um serviço totalmente gerenciado para fornecer dados de streaming em tempo real para destinos como Amazon S3, Amazon Redshift, OpenSearch Amazon Service, Splunk e qualquer endpoint HTTP personalizado ou endpoints HTTP de propriedade de provedores de serviços terceirizados compatíveis.
- O Amazon Simple Storage Service (Amazon S3) é um armazenamento para a Internet.
- O Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que coordena e gerencia a entrega ou o envio de mensagens a endpoints ou clientes inscritos.
- Snowflake — O Snowflake é um data warehouse analítico fornecido como (SaaS). Software-as-a-Service
- Snowflake Snowpipe: o Snowpipe carrega dados dos arquivos assim que eles estão disponíveis em um estágio do Snowflake.

Épicos

Configurar um Snowflake Snowpipe

Tarefa	Descrição	Habilidades necessárias
Crie um arquivo CSV no Snowflake.	Faça login no Snowflake e execute o `CREATE FILE FORMAT` comando para criar um arquivo CSV com um delimitador de campo especificado. Para obter mais informações sobre esse e outros comandos do Snowflake, consulte a seção Informações adicionais.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Crie um estágio externo do Snowflake.	Execute o `CREATE STAGE` comando para criar um estágio externo do Snowflake que faça referência ao arquivo CSV que você criou anteriormente. Importante: você precisará da URL do bucket do S3, da sua chave de AWS acesso e da sua chave de acesso AWS secreta. Execute o `SHOW STAGES` comando para verificar se o estágio do Snowflake foi criado.	Desenvolvedor
Crie a tabela de destino do Snowflake.	Execute o `CREATE TABLE` comando para criar a tabela Snowflake.	Desenvolvedor
Crie um pipe.	Execute o `CREATE PIPE` comando; certifique-se de que `auto_ingest=true` esteja no comando. Execute o `SHOW PIPES` comando para verificar se o canal foi criado. Copie e salve o valor `notification_channel` da coluna. Esse valor será usado para configurar notificações de eventos do Amazon S3.	Desenvolvedor

Configurar o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Crie uma política de ciclo de vida de 30 dias para o bucket do S3.	Faça login no AWS Management Console e abra o console do Amazon S3. Escolha o bucket do S3 que contém os dados do Firehose. Em seguida, escolha a guia Gerenciamento no bucket do S3 e escolha Adicionar regra de ciclo de vida. Insira um nome para sua regra na caixa de diálogo Regra de ciclo de vida e configure uma regra de ciclo de vida de 30 dias para seu bucket. Para obter ajuda com esse e outros artigos, consulte a seção Recursos relacionados.	Administrador do sistema, desenvolvedor
Crie uma política do IAM para o bucket do S3.	Abra o console AWS Identity and Access Management (IAM) e escolha Políticas. Escolha Criar política e escolha a guia JSON. Copie e cole a política da seção Informações adicionais no campo JSON. Essa política `PutObject` concederá `DeleteObject` permissões, bem como `GetObject` `ListBucket` permissões e permissões. `GetObject` `Version` Escolha Revisar política, insira um nome	Administrador do sistema, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	de política e escolha Criar política.	
Atribua a política a um perfil do IAM.	Abra o console do IAM, escolha Roles e, em seguida, escolha Create role. Escolha Outra conta da AWS como entidade confiável. Insira sua Conta da AWS ID e escolha Exigir ID externa. Insira um ID de espaço reservado que você alterará posteriormente. Escolha Avançar e atribua a política do IAM que você criou anteriormente. Então, crie o perfil do IAM.	Administrador do sistema, desenvolvedor
Copie o nome do recurso da Amazon (ARN) do perfil do IAM.	Abra o console do IAM e escolha Roles. Escolha a função do IAM que você criou anteriormente e, em seguida, copie e armazene o ARN da função.	Administrador do sistema, desenvolvedor

Configurar uma integração de armazenamento no Snowflake

Tarefa	Descrição	Habilidades necessárias
Crie uma integração de armazenamento no Snowflake .	Faça login no Snowflake e execute o `CREATE STORAGE INTEGRATION` comando. Isso modificará o relaciona mento confiável, concederá acesso ao Snowflake e	Administrador do sistema, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	fornecerá a ID externa do seu estágio do Snowflake.	
Recupere o perfil do IAM da conta do Snowflake.	Execute o `DESC INTEGRATION` comando para recuperar o ARN da função do IAM. **Important** `<integration_name>` é o nome da integração de armazenamento do Snowflake que você criou anteriormente.	Administrador do sistema, desenvolvedor
Registre os valores de duas colunas.	Copie e salve os valores das `storage_aws_external_id` colunas `storage_aws_iam_user_arn` e.	Administrador do sistema, desenvolvedor

Permita que o Snowflake Snowpipe acesse o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Modifique a política de perfil do IAM.	Abra o console do IAM e selecione Funções. Escolha a função do IAM que você criou anteriormente e escolha a guia Relações de confiança. Selecione Edit trust relationship (Editar relação de confiança). `snowflake_external_id` Substitua	Administrador do sistema, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	pelo `storage_aws_external_id` valor que você copiou anteriormente. `snowflake_user_arn` Substitua pelo `storage_aws_iam_user_arn` valor que você copiou anteriormente. Em seguida, escolha Atualizar política de confiança.	

Ative e configure as notificações do SNS para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Ative as notificações de eventos para o bucket do S3.	Abra o console do Amazon S3 e selecione seu bucket. Escolha Propriedades e, em Configurações avançadas , escolha Eventos. Escolha Adicionar notificação e insira um nome para esse evento. Se você não inserir um nome, um Identificador Exclusivo Globalmente (GUID) será usado.	Administrador do sistema, desenvolvedor
Configurar notificações do Amazon SNS para o bucket do S3.	Em Eventos, escolha ObjectCreate (Tudo) e, em seguida, escolha SQS Queue na lista suspensa Enviar para. Na lista SNS, escolha Adicionar ARN da fila SQS e cole `notification_channel` o valor que você copiou	Administrador do sistema, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	anteriormente. Em seguida, escolha Salvar.	
Assinar a fila do Snowflake SQS; para um tópico do SNS.	Assinar a fila do Snowflake SQS; para um tópico do SNS que você criou. Para obter ajuda com essa etapa, consulte a seção Recursos relacionados.	Administrador do sistema, desenvolvedor

Verifique a integração do estágio do Snowflake

Tarefa	Descrição	Habilidades necessárias
Verifique e teste o Snowpipe.	Faça login no Snowflake e abra o estágio do Snowflake . Coloque os arquivos em seu bucket do S3 e verifique se a tabela do Snowflake os carrega. O Amazon S3 enviará notificações do SNS para o Snowpipe quando novos objetos aparecerem no bucket do S3.	Administrador do sistema, desenvolvedor

Recursos relacionados

- Gerenciando seu ciclo de vida de armazenamento
- Assinar a fila do Snowflake SQS; para um tópico do Amazon SNS

Mais informações

Criar um formato de arquivo:

```
CREATE FILE FORMAT <name>
TYPE = 'CSV'
FIELD_DELIMITER = '|'
SKIP_HEADER = 1;
```

Criar um estágio externo:

```
externalStageParams (for Amazon S3) ::=
  URL = 's3://[//]'

  [ { STORAGE_INTEGRATION =  } | { CREDENTIALS = ( {  { AWS_KEY_ID = `` AWS_SECRET_KEY
 = `` [ AWS_TOKEN = `` ] } | AWS_ROLE = ``  } ) ) }` ]
  [ ENCRYPTION = ( [ TYPE = 'AWS_CSE' ] [ MASTER_KEY = '' ] |
                   [ TYPE = 'AWS_SSE_S3' ] |
                   [ TYPE = 'AWS_SSE_KMS' [ KMS_KEY_ID = '' ] |
                   [ TYPE = NONE ] )
```

Criar uma tabela:

```
CREATE [ OR REPLACE ] [ { [ LOCAL | GLOBAL ] TEMP[ORARY] | VOLATILE } | TRANSIENT ]
 TABLE [ IF NOT EXISTS ]
  <table_name>
    ( <col_name> <col_type> [ { DEFAULT <expr>
                                | { AUTOINCREMENT | IDENTITY } [ ( <start_num> ,
 <step_num> ) | START <num> INCREMENT <num> ] } ]
                                 /* AUTOINCREMENT / IDENTITY supported only for numeric
 data types (NUMBER, INT, etc.) */
                             [ inlineConstraint ]
      [ , <col_name> <col_type> ... ]
      [ , outoflineConstraint ]
      [ , ... ] )
  [ CLUSTER BY ( <expr> [ , <expr> , ... ] ) ]
  [ STAGE_FILE_FORMAT = ( { FORMAT_NAME = '<file_format_name>'
                           | TYPE = { CSV | JSON | AVRO | ORC | PARQUET | XML }
 [ formatTypeOptions ] } ) ]
  [ STAGE_COPY_OPTIONS = ( copyOptions ) ]
  [ DATA_RETENTION_TIME_IN_DAYS = <num> ]
  [ COPY GRANTS ]
  [ COMMENT = '<string_literal>' ]
```

Exibir etapas:

```
SHOW STAGES;
```

Criar um pipe:

```
CREATE [ OR REPLACE ] PIPE [ IF NOT EXISTS ]
  [ AUTO_INGEST = [ TRUE | FALSE ] ]
  [ AWS_SNS_TOPIC =  ]
  [ INTEGRATION = '' ]
  [ COMMENT = '' ]
  AS
```

Exibir pipes:

```
SHOW PIPES [ LIKE '<pattern>' ]
           [ IN { ACCOUNT | [ DATABASE ] <db_name> | [ SCHEMA ] <schema_name> } ]
```

Criar uma integração de armazenamento:

```
CREATE STORAGE INTEGRATION <integration_name>
  TYPE = EXTERNAL_STAGE
  STORAGE_PROVIDER = S3
  ENABLED = TRUE
  STORAGE_AWS_ROLE_ARN = '<iam_role>'
  STORAGE_ALLOWED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/')
  [ STORAGE_BLOCKED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/') ]
```

Exemplo:

```
create storage integration s3_int
  type = external_stage
  storage_provider = s3
  enabled = true
  storage_aws_role_arn = 'arn:aws:iam::001234567890:role/myrole'
  storage_allowed_locations = ('s3://amzn-s3-demo-bucket1/mypath1/', 's3://amzn-s3-
demo-bucket2/mypath2/')
  storage_blocked_locations = ('s3://amzn-s3-demo-bucket1/mypath1/sensitivedata/',
 's3://amzn-s3-demo-bucket2/mypath2/sensitivedata/');
```

Para obter mais informações sobre essa etapa, consulte Configuração de uma integração de armazenamento do Snowflake para acessar o Amazon S3 na documentação do Snowflake.

Descreva uma integração:

```
DESC INTEGRATION <integration_name>;
```

Política de bucket do S3:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetObjectVersion",
              "s3:DeleteObject",
              "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::",
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "/*"
                    ]
                }
            }
        }
    ]
}
```

Criptografe automaticamente volumes novos e existentes do Amazon EBS

Criado por Tony DeMarco (AWS) e Josh Joy (AWS)

Resumo

A criptografia de volumes do Amazon Elastic Block Store (Amazon EBS) é importante para a estratégia de proteção de dados de uma organização. É uma etapa importante no estabelecimento de um ambiente bem arquitetado. Embora não haja uma maneira direta de criptografar um volume ou um snapshot não criptografado existente, é possível criptografá-los criando um volume ou um snapshot. Para obter mais informações, consulte Criptografar recursos do EBS na documentação da Amazon EC2 . Esse padrão fornece controles preventivos e de detecção para criptografar seus volumes do EBS, tanto novos quanto existentes. Nesse padrão, você define as configurações da conta, cria processos automatizados de remediação e implementa controles de acesso.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS)
- AWS Command Line Interface (AWS CLI) instalado e configurado em macOS, Linux ou Windows
- jq, instalado e configurado em macOS, Linux ou Windows
- As permissões do AWS Identity and Access Management (IAM) são provisionadas para ter acesso de leitura e gravação à AWS, CloudFormation Amazon Elastic Compute Cloud (Amazon EC2), AWS Systems Manager, AWS Config e AWS Key Management Service (AWS KMS)
- O AWS Organizations está configurado com todos os atributos habilitados, um requisito para políticas de controle de serviços
- O AWS Config está habilitado nas contas de destino

Limitações

- Não deve haver regras do AWS Config denominadas encrypted-volumes em sua conta de destino da AWS. Essa solução implanta uma regra com esse nome. Regras preexistentes com esse nome podem causar falhas na implantação e resultar em cobranças desnecessárias relacionadas ao processamento da mesma regra mais de uma vez.
- Essa solução criptografa todos os volumes do EBS com a mesma chave do AWS KMS.

- Se você habilitar a criptografia de volumes do EBS para a conta, essa configuração será específica da região. Se você habilitá-lo para uma região da AWS, não poderá desabilitá-lo para volumes ou snapshots individuais nessa região. Para obter mais informações, consulte Criptografia por padrão na EC2 documentação da Amazon.
- Ao corrigir volumes do EBS existentes e não criptografados, certifique-se de que a EC2 instância não esteja em uso. Essa automação desativa a instância para separar o volume não criptografado e anexar o volume criptografado. Um tempo de inatividade ocorre enquanto a remediação está em andamento. Se essa for uma parte essencial da infraestrutura da sua organização, certifique-se de que as configurações manuais ou automáticas de alta disponibilidade estejam em vigor para não afetar a disponibilidade de nenhum aplicativo em execução na instância. Recomendamos que você corrija os recursos essenciais somente durante as janelas de manutenção padrão.

Arquitetura

Fluxo de trabalho de automação

1. O AWS Config detecta um volume não criptografado do EBS.
2. Um administrador usa o AWS Config para enviar um comando de remediação ao Systems Manager.
3. A automação do Systems Manager cria um snapshot (instantâneo) do volume EBS não criptografado.
4. A automação do Systems Manager usa o AWS KMS para criar uma cópia criptografada do snapshot.
5. A automação do Systems Manager faz o seguinte:
   a. Interrompe a EC2 instância afetada se ela estiver em execução
   b. Anexa a nova cópia criptografada do volume à instância EC2
   c. Retorna a EC2 instância ao seu estado original

Ferramentas

Serviços da AWS

- AWS CLI — A AWS Command Line Interface (AWS CLI) fornece acesso direto às interfaces públicas de programação de aplicativos (APIs) dos serviços da AWS. Você pode explorar os

recursos de um serviço com a AWS CLI e desenvolver scripts de shell para gerenciar seus recursos. Além dos comandos equivalentes à API de baixo nível, vários serviços da AWS fornecem personalizações para a AWS CLI. As personalizações podem incluir comandos de nível mais elevado que simplificam o uso de um serviço com uma API complexa.

- AWS CloudFormation — CloudFormation A AWS é um serviço que ajuda você a modelar e configurar seus recursos da AWS. Você cria um modelo que descreve todos os recursos da AWS que você deseja (como EC2 instâncias da Amazon) e CloudFormation provisiona e configura esses recursos para você.
- AWS Config: o AWS Config oferece uma exibição detalhada da configuração dos recursos da AWS em sua conta da AWS. Isso inclui como os recursos estão relacionados um com o outro e como eles foram configurados no passado, de modo que você possa ver como os relacionamentos e as configurações foram alterados ao longo do tempo.
- Amazon EC2 — O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço web que fornece capacidade de computação redimensionável que você usa para criar e hospedar seus sistemas de software.
- AWS KMS: o AWS Key Management Service (AWS KMS) é um serviço de criptografia e gerenciamento de chave com escalabilidade para a nuvem. As chaves e funcionalidades do AWS KMS são usadas por outros serviços da AWS e você pode usá-las para proteger dados em seu ambiente da AWS.
- AWS Organizations: o AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS Systems Manager Automation — A automação do Systems Manager simplifica tarefas comuns de manutenção e implantação para EC2 instâncias da Amazon e outros recursos da AWS.

Outros serviços

- jq: o jq é um processador JSON de linha de comando leve e flexível. Você usa essa ferramenta para extrair informações importantes da saída da AWS CLI.

Código

- O código desse padrão está disponível no repositório de chaves GitHub KMS do cliente para corrigir automaticamente volumes do EBS não criptografados.

Épicos

Automatize a remediação de volumes não criptografados

Tarefa	Descrição	Habilidades necessárias
Baixe scripts e CloudFormation modelos.	Baixe o script de shell, o arquivo JSON e os CloudFormation modelos do repositório de chaves KMS do cliente para corrigir GitHub automaticamente volumes do EBS não criptografados.	Administrador AWS, Geral AWS
Identifique o administrador da chave do AWS KMS.	1. Faça login no Console de Gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/. 2. Identifique um usuário ou um perfil para ser o administrador da chave do AWS KMS. Se um novo usuário ou perfil precisar ser criado para essa finalidade, crie-o agora. Para obter mais informações, consulte Identidades do IAM na documentação do IAM. Essa automação cria uma nova chave do AWS KMS. 3. Uma vez identificado, copie o nome do recurso da Amazon (ARN) do usuário ou do perfil. Para obter mais informações, consulte	Administrador AWS, Geral AWS

Tarefa	Descrição	Habilidades necessárias
	IAM ARNs na documentação do IAM. Você usa esse ARN na próxima etapa.	
Implante o modelo Stack1 CloudFormation .	1. Abra o CloudFormation console da AWS em https://console.aws.amazon.com/cloudformation/. 2. Em CloudFormation, implante o `Stack1.yaml` modelo. Observe os seguintes detalhes de implantação: • Dê à pilha um nome claro e descritivo. Anote o nome da pilha, porque você precisará desse valor na próxima etapa. • Cole o ARN do administrador da chave no único campo de parâmetro no Stack1. Esse usuário ou perfil se torna o administrador da chave do AWS KMS criada pela pilha. Para obter mais informações sobre a implantação de um CloudFormation modelo, consulte Como trabalhar com CloudFormation modelos da AWS na CloudFormation documentação.	Administrador AWS, Geral AWS

Tarefa	Descrição	Habilidades necessárias
Implante o modelo Stack2 CloudFormation .	Em CloudFormation, implante o `Stack2.yaml` modelo. Observe os seguintes detalhes de implantação: • Dê à pilha um nome claro e descritivo. • No único parâmetro do Stack2, insira o nome da pilha que você criou na etapa anterior. Isso permite que o Stack2 faça referênci a ao novo perfil e chave do AWS KMS implantados pela pilha na etapa anterior.	Administrador AWS, Geral AWS
Crie um volume não criptogra fado para testes.	Crie uma EC2 instância com um volume EBS não criptogra fado. Para obter instruçõe s, consulte Criar um volume do Amazon EBS na EC2 documentação da Amazon. O tipo de instância não importa e o acesso à instância não é necessário. Você pode criar uma instância t2.micro para permanecer no nível gratuito e não precisa criar um par de chaves.	Administrador AWS, Geral AWS

Tarefa	Descrição	Habilidades necessárias
Teste a regra do AWS Config.	1. Abra o console do AWS Config em. https://console.aws.amazon.com/config/ Na página Regras, selecione a regra encrypted-volumes (volumes criptografados). 2. Confirme se sua nova instância de teste não criptografada aparece na lista de recursos não compatíveis. Se o volume não aparecer imediatamente, aguarde mais alguns minutos e atualize os resultados. A regra do AWS Config detecta as alterações nos recursos logo após a criação da instância e do volume. 3. Selecione o recurso e, em seguida, selecione Remediar. Você pode visualizar o progresso e o status da remediação no Systems Manager da seguinte forma: 1. Abra o console do AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.	Administrador AWS, Geral AWS

Tarefa	Descrição	Habilidades necessárias
	2. No painel de navegação à esquerda, escolha Automation. 3. Selecione o link ID de execução para ver as etapas e o status.	
Configure contas adicionais ou regiões da AWS.	Conforme necessário para seu caso de uso, repita esse épico para qualquer conta adicional ou região da AWS.	Administrador AWS, Geral AWS

Habilite a criptografia em nível de conta dos volumes do EBS

Tarefa	Descrição	Habilidades necessárias
Execute o script de habilitação.	1. Em um shell bash, use o comando `cd` para navegar até o repositório clonado. 2. Insira o comando a seguir para executar o script `enable-ebs-encryption-for-account .` `./Bash/enable-ebs-encryption-for-account.sh`	Administrador AWS, Geral AWS, bash
Confirme se as configurações estão atualizadas.	1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.	Administrador AWS, Geral AWS

Tarefa	Descrição	Habilidades necessárias
	2. No lado direito da tela, em Configurações, escolha Proteção e segurança de dados. 3. Na seção Criptografia do EBS, confirme se a opção Sempre criptografar novos volumes do EBS está ativada e se a chave de criptografia padrão está definida como o ARN que você especificou anteriormente. **Note** Se a configuração Sempre criptografar novos volumes do EBS estiver desativada ou a chave ainda estiver definida alias/aws/ebs, confirme se você está conectado à mesma conta e região da AWS em que executou o script de shell e verifique se há mensagens de erro no shell.	

Tarefa	Descrição	Habilidades necessárias
Configure contas adicionais ou regiões da AWS.	Conforme necessário para seu caso de uso, repita esse épico para qualquer conta adicional ou região da AWS.	Administrador AWS, Geral AWS

Evite a criação de instâncias não criptografadas

Tarefa	Descrição	Habilidades necessárias
Crie uma política de controle de serviço.	1. Abra o console do AWS Organizations em https://console.aws.amazon.com/organizations/v2/. 2. Crie uma nova política de controle de serviço. Para obter mais informações, consulte Criar uma política de controle de serviço na documentação do AWS Organizations. 3. Adicione o conteúdo de `DenyUnencryptedEC2.json` à política e salve-o. Você baixou esse arquivo JSON do GitHub repositório no primeiro épico. 4. Anexe essa política à raiz da organização ou a qualquer unidade organizacional necessária (OUs). Para obter mais informações, consulte Anexar e desanexar políticas de	Administrador AWS, Geral AWS

Tarefa	Descrição	Habilidades necessárias
	controle de serviço na documentação do AWS Organizations.	

Recursos relacionados

Documentação do serviço AWS

- CLI da AWS
- AWS Config
- AWS CloudFormation
- Amazon EC2
- AWS KMS
- AWS Organizations
- AWS Systems Manager Automation

Outros recursos

- manual do jq (site jq)
- download jq () GitHub

Faça backup dos servidores Sun SPARC no emulador Stromasys Charon-SSP na nuvem AWS

Criado por Kevin Yung (AWS), Luis Ramos (Stromasys) e Rohit Darji (AWS)

Resumo

Esse padrão fornece quatro opções para fazer backup de seus servidores SPARC da Sun Microsystems após a migração de um ambiente on-premises para a nuvem da Amazon Web Services (AWS). Essas opções de backup ajudam você a implementar um plano de backup que atenda ao objetivo de ponto de recuperação (RPO) e ao objetivo de tempo de recuperação (RTO) de sua organização, use abordagens automatizadas e reduza seus custos operacionais gerais. O padrão fornece uma visão geral das quatro opções de backup e das etapas para implementá-las.

Se você usa um servidor Sun SPARC hospedado como convidado em um emulador Stromasys Charon-SSP, você pode usar uma das três opções de backup a seguir:

- Opção de backup 1: fita virtual Stromasys : use o atributo de fita virtual Charon-SSP para configurar uma instalação de backup no servidor Sun SPARC e arquivar seus arquivos de backup no Amazon Simple Storage Service (Amazon S3) e no Amazon Simple Storage Service Glacier usando o AWS Systems Manager Automation.
- Opção de backup 2: instantâneo do Stromasys – Use o atributo de snapshot Charon-SSP para configurar um recurso de backup para os servidores convidados Sun SPARC no Charon-SSP.
- Opção de backup 3: Snapshot de volume do Amazon Elastic Block Store (Amazon EBS) — Se você hospedar o emulador Charon-SSP no Amazon Elastic Compute Cloud (Amazon EC2), você pode usar um snapshot de volume do Amazon EBS para criar backups para um sistema de arquivos Sun SPARC.

Se você usa um servidor Sun SPARC hospedado como convidado no hardware e o Charon-SSP na EC2 Amazon, você pode usar a seguinte opção de backup:

- Opção de backup 4: biblioteca de fitas virtuais (VTL) do AWS Storage Gateway : use um aplicativo de backup com um gateway de fita VTL do Storage Gateway para fazer backup dos servidores Sun SPARC.

Se você usa um servidor Sun SPARC hospedado como uma zona de marca em um servidor Sun SPARC, você pode usar as opções de backup 1, 2 e 4.

A Stromasys fornece software e serviços para emular sistemas críticos SPARC, Alpha, VAX e PA-RISC antigos. Para obter mais informações sobre a migração para a Nuvem AWS usando a emulação do Stromasys, consulte Rehosting SPARC, Alpha ou outros sistemas legados na AWS com o Stromasys no blog da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Servidores Sun SPARC existentes.
- Licenças existentes para Charon-SSP. As licenças para Charon-SSP estão disponíveis no AWS Marketplace e as licenças para o Stromasys Virtual Environment (VE) estão disponíveis na Stromasys. Para obter mais informações, entre em contato com o departamento de vendas da Stromasys.
- Familiaridade com servidores Sun SPARC e backups Linux.
- Familiaridade com a tecnologia de emulação Charon-SSP. Para obter mais informações sobre isso, consulte Emulação de servidor legado do Stromasys na documentação do Stromasys.
- Se você quiser usar o recurso de fita virtual ou os aplicativos de backup para os sistemas de arquivos dos servidores Sun SPARC, deverá criar e configurar os recursos de backup para o sistema de arquivos do servidor Sun SPARC.
- Uma compreensão do RPO e do RTO. Para obter mais informações sobre isso, consulte Objetivos de recuperação de desastres do whitepaper Reliability Pillar na documentação do AWS Well-Architected Framework.
- Para usar a opção de Backup 4, você deve ter o seguinte:
  - Um aplicativo de backup baseado em software que suporta um Gateway de Fitas Storage Gateway VTL. Para obter mais informações sobre isso, consulte Trabalho com dispositivos VTL na documentação do AWS Storage Gateway.
  - Bacula Director ou um aplicativo de backup similar, instalado e configurado. Para obter mais informações sobre isso, consulte a documentação do Bacula Director.

A tabela a seguir fornece informações sobre as quatro opções de backup nesse padrão.

Opções de backup	Alcança a consistência de falhas?	Alcança a consistência do aplicativo?	Solução de dispositivo de backup virtual?	Caso de uso típico
Opção 1 – fita virtual Stromasys	Sim Você pode automatizar os instantâneos do sistema de arquivos Sun SPARC para fazer backup dos dados em uma fita virtual. Por exemplo, é possível usar instantâneos do UFS ou do ZFS.	Sim Essa opção de backup requer um script automatizado para liberar transações em andamento , configurar um modo off-line temporári o ou somente leitura durante a captura instantân ea do sistema de arquivos ou fazer um despejo de dados do aplicativo. Você também pode precisar de tempo de inatividade do aplicativo ou do modo somente leitura.	Sim	Backup de sistemas de arquivos do servidor Sun SPARC com arquivos .tar ou .zip Backup de dados de aplicativos
Opção 2 – Stromasys snapshot	Sim Você deve configurar o Charon-SSP	Sim Essa opção de backup cria um instantân	Não	Instantâneo do servidor Sun SPARC

Manager ou usar um argumento de inicialização da linha de comando para habilitar esse atributo. Você também deve executar um comando Linux para solicitar ao emulador Charon-SSP que salve o estado do servidor convidado Sun SPARC em um arquivo de instantâneo. **Important** Você deve desligar o servidor convidado Sun SPARC.	eo do servidor convidado emulado, incluindo seus discos virtuais e despejo de memória. **Important** Você deve desligar o servidor convidado Sun SPARC durante o snapshot.	Backup de dados de aplicativos

Opção 3 – Amazon EBS volume	Sim Você pode usar o AWS Backup para automatizar o snapshot do Amazon EBS.	Sim Essa opção de backup requer um script automatizado para liberar as transações em andamento e configurar uma parada temporária ou somente para leitura da instância EC2 durante o snapshot do volume do Amazon EBS. ⚠ Important Essa opção de backup pode exigir tempo de inatividade do aplicativo ou modo somente leitura para obter a consistência do	Não	Instantâneo dos sistemas de arquivos do servidor Sun SPARC Backup de dados de aplicativos

aplicativ
o.

Opção 4 – AWS Storage Gateway VTL	Sim Você pode fazer backup automático dos dados de backup do sistema de arquivos Sun SPARC na VTL usando um agente de backup.	Sim Essa opção de backup requer um script automatizado para liberar as transações em andamento e configurar um modo off-line temporário ou somente leitura durante o instantâneo do sistema de arquivos ou o despejo de dados do aplicativo. **Important** Essa opção de backup pode exigir tempo de inatividade do aplicativo ou modo somente leitura.	Sim	Uma grande frota de backups do sistema de arquivos do servidor Sun SPARC Backup de dados de aplicativos

Limitações

- Você pode usar as abordagens desse padrão para fazer backup de servidores Sun SPARC individuais, mas também pode usar essas opções de backup para dados compartilhados se tiver aplicativos executados em um cluster.

Ferramentas

Opção de backup 1: fita virtual Stromasys

- Emulador Stromasys Charon-SSP: o emulador Charon-SSP cria a réplica virtual do hardware SPARC original dentro de um sistema de computador padrão compatível com x86 de 64 bits. Ele executa o código binário SPARC original, incluindo sistemas operacionais (OSs) como SunOS ou Solaris, seus produtos em camadas e aplicativos.
- Amazon EC2 — O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço web que fornece capacidade de computação redimensionável que você usa para criar e hospedar seus sistemas de software.
- Amazon EFS — O Amazon Elastic File System (Amazon EFS) fornece um sistema de arquivos simples, sem servidor e set-and-forget elástico para uso com serviços de nuvem e recursos locais da AWS.
- Amazon S3 : o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet.
- Amazon S3 Glacier: o Amazon Simple Storage Service Glacier é uma classe de armazenamento Amazon S3 segura, durável e de custo extremamente baixo para arquivamento de dados e backup de longo prazo.
- Automação do AWS Systems Manager — A automação, um recurso do AWS Systems Manager, simplifica as tarefas comuns de manutenção e implantação de EC2 instâncias e outros recursos da AWS.

Opção de backup 2: snapshot do Stromasys

- Emulador Stromasys Charon-SSP: o emulador Charon-SSP cria a réplica virtual do hardware SPARC original dentro de um sistema de computador padrão compatível com x86 de 64 bits. Ele executa o código binário SPARC original OSs , incluindo SunOS ou Solaris, seus produtos em camadas e aplicativos.

- Amazon EC2 — O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço web que fornece capacidade de computação redimensionável que você usa para criar e hospedar seus sistemas de software.
- Amazon EFS — O Amazon Elastic File System (Amazon EFS) fornece um sistema de arquivos simples, sem servidor e set-and-forget elástico para uso com serviços de nuvem e recursos locais da AWS.
- Amazon S3 : o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet.
- Amazon S3 Glacier: o Amazon Simple Storage Service Glacier é uma classe de armazenamento Amazon S3 segura, durável e de custo extremamente baixo para arquivamento de dados e backup de longo prazo.
- Automação do AWS Systems Manager — A automação, um recurso do AWS Systems Manager, simplifica as tarefas comuns de manutenção e implantação de EC2 instâncias e outros recursos da AWS.

Opção de backup 3: snapshot de volume do Amazon EBS

- Emulador Stromasys Charon-SSP: o emulador Charon-SSP cria a réplica virtual do hardware SPARC original dentro de um sistema de computador padrão compatível com x86 de 64 bits. Ele executa o código binário SPARC original OSs , incluindo SunOS ou Solaris, seus produtos em camadas e aplicativos.
- AWS Backup: o AWS Backup é um serviço de backup totalmente gerenciado que facilita a centralização e a automação do backup de dados entre todos os serviços da AWS na nuvem e on-premises.
- Amazon EBS — O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias. EC2
- Amazon EC2 — O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço web que fornece capacidade de computação redimensionável que você usa para criar e hospedar seus sistemas de software.

Opção de backup 4: AWS Storage Gateway VTL

- Emulador Stromasys Charon-SSP: o emulador Charon-SSP cria a réplica virtual do hardware SPARC original dentro de um sistema de computador padrão compatível com x86 de 64 bits. Ele executa o código binário SPARC original OSs , incluindo SunOS ou Solaris, seus produtos em camadas e aplicativos.
- Bacula: o Bacula é um sistema de backup de computador de código aberto e de nível corporativo. Para obter mais informações sobre se seu aplicativo de backup existente é compatível com o Gateway de Fitas, consulte Aplicativos de backup de terceiros compatíveis para um Tape Gateway na documentação do AWS Storage Gateway.
- Amazon EC2 — O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço web que fornece capacidade de computação redimensionável que você usa para criar e hospedar seus sistemas de software.
- Amazon RDS para MySQL: o Amazon Relational Database Service (Amazon RDS) suporta instâncias de banco de dados executando várias versões do MySQL.
- Amazon S3 : o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet.
- Amazon S3 Glacier: o Amazon Simple Storage Service Glacier é uma classe de armazenamento Amazon S3 segura, durável e de custo extremamente baixo para arquivamento de dados e backup de longo prazo.
- AWS Storage Gateway: o Storage Gateway conecta um dispositivo de software on-premises a um armazenamento em nuvem para oferecer uma integração perfeita e segura entre um ambiente de TI on-premises e a infraestrutura de armazenamento da AWS.

Épicos

Opção de backup 1 – Criar um backup em fita virtual da Stromasys

Tarefa	Descrição	Habilidades necessárias
Crie um sistema de arquivos compartilhado Amazon EFS para armazenamento virtual de arquivos em fita.	Faça login no Console de Gerenciamento da AWS ou use a CLI da AWS para criar um sistema de arquivos do Amazon EFS. Para obter mais informaçõ es sobre isso, consulte Criar	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	um sistema de arquivos do Amazon EFS na documentação do Amazon EFS.	
Configure o host Linux para montar o sistema de arquivos compartilhado.	Instale o driver do Amazon EFS na instância do Amazon EC2 Linux e configure o sistema operacional Linux para montar o sistema de arquivos compartilhados do Amazon EFS durante a inicialização. Para obter mais informações sobre isso, consulte Montagem de sistemas de arquivos usando o auxiliar de montagem do EFS na documentação do Amazon EFS.	DevOps engenheiro
Instale o emulador Charon-SSP.	Instale o emulador Charon-SSP na instância Amazon Linux. EC2 Para obter mais informações sobre isso, consulte Configurar uma instância de Nuvem AWS para Charon-SSP na documentação da Stromasys.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Crie um contêiner de arquivo de fita virtual no sistema de arquivos compartilhado para cada servidor convidado Sun SPARC.	Execute o comando `touch <vtape-container-name>` para criar um contêiner de arquivo de fita virtual no sistema de arquivos compartilhado para cada servidor convidado Sun SPARC implantado no emulador Charon-SSP.	DevOps engenheiro
Configure o Charon-SSP Manager para criar dispositivos de fita virtual para os servidores convidados Sun SPARC.	Faça login no Charon-SSP Manager, crie dispositivos de fita virtual e configure-os para usar os arquivos de contêiner de fita virtual para cada servidor convidado Sun SPARC. Para obter mais informações sobre isso, consulte o guia do usuário do Charon-SSP 5.2 para Linux na documentação do Stromasys.	DevOps engenheiro
Valide se o dispositivo de fita virtual está disponível nos servidores convidados Sun SPARC.	Faça login em cada servidor convidado Sun SPARC e execute o comando `mt -f /dev/rmt/1` para validar se o dispositivo de fita virtual está configurado no sistema operacional.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Desenvolva o runbook e a automação do Systems Manager Automation.	Desenvolva o runbook do Systems Manager Automation e configure janelas de manutenção e associações no Systems Manager para agendar o processo de backup. Para obter mais informações sobre isso, consulte as instruções de automação e a configuração de janelas de manutenção na documentação do AWS Systems Manager.	Arquiteto de nuvem
Configure o Systems Manager Automation para arquivar arquivos rotativos de contêiner de fita virtual.	Use o exemplo de código da opção Voltar 1 na seção Informações adicionais para desenvolver um runbook do Systems Manager Automation para arquivar arquivos rotativos de contêineres de fitas virtuais no Amazon S3 e no Amazon S3 Glacier.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Implante o runbook do Systems Manager Automation para arquivamento e agendamento.	Implante o runbook do Systems Manager Automation e agende-o para execução automática no Systems Manager. Para obter mais informações sobre isso, consulte as orientações de automação na documentação do Systems Manager.	Arquiteto de nuvem

Opção de backup 2 – Criar um instantâneo do Stromasys

Tarefa	Descrição	Habilidades necessárias
Crie um sistema de arquivos compartilhado Amazon EFS para armazenamento virtual de arquivos em fita.	Faça login no Console de Gerenciamento da AWS ou use a CLI da AWS para criar um sistema de arquivos do Amazon EFS. Para obter mais informações sobre isso, consulte Criar seu sistema de arquivos do Amazon EFS na documentação do Amazon EFS.	Arquiteto de nuvem
Configure o host Linux para montar o sistema de arquivos compartilhado.	Instale o driver do Amazon EFS na instância do Amazon EC2 Linux e configure o sistema operacional Linux para montar o sistema de arquivos compartilhados	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	do Amazon EFS durante a inicialização. Para obter mais informaçõ es sobre isso, consulte Montagem de sistemas de arquivos usando o auxiliar de montagem do EFS na documentação do Amazon EFS.	
Instale o emulador Charon-SS P.	Instale o emulador Charon-SS P na instância Amazon Linux. EC2 Para obter mais informações sobre isso, consulte Configura r uma instância de Nuvem AWS para Charon-SSP na documentação da Stromasys.	DevOps engenheiro
Configure os servidores convidados Sun SPARC para inicializar com a opção de snapshot.	Use o Charon-SSP Manager para configurar a opção de snapshot para cada servidor convidado Sun SPARC. Para obter mais informações sobre isso, consulte o guia do usuário do Charon-SSP 5.2 para Linux na documentação do Stromasys.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Desenvolva o runbook do Systems Manager Automation.	Use o exemplo de código da opção Backup 2 na seção Informações adicionais para desenvolver um runbook do Systems Manager Automation para executar remotamente o comando de snapshot em um servidor convidado Sun SPARC durante uma janela de manutenção.	Arquiteto de nuvem
Implante o runbook do Systems Manager Automation e configure a associação com os hosts EC2 Linux da Amazon.	Implante o runbook do Systems Manager Automation e configure janelas de manutenção e associações no Systems Manager para agendar o processo de backup. Para obter mais informações sobre isso, consulte as instruções de automação e a configuração de janelas de manutenção na documentação do AWS Systems Manager.	Arquiteto de nuvem
Arquive instantâneos em armazenamento de longo prazo.	Use o código de amostra do runbook da seção Informações adicionais para desenvolver um runbook do Systems Manager Automation para arquivar arquivos de snapshot no Amazon S3 e no Amazon S3 Glacier.	Arquiteto de nuvem

Opção de backup 3 – Criar um snapshot do volume do Amazon EBS

Tarefa	Descrição	Habilidades necessárias
Instale o emulador Charon-SSP.	Instale o emulador Charon-SSP na instância Amazon Linux. EC2 Para obter mais informações sobre isso, consulte Configurar uma instância de Nuvem AWS para Charon-SSP na documentação da Stromasys.	DevOps engenheiro
Crie volumes do EBS para os servidores convidados Sun SPRAC.	Faça login no Console de Gerenciamento da AWS, abra o console do Amazon EBS e crie volumes do EBS para os servidores convidados do Sun SPRAC. Para obter mais informações sobre isso, consulte Configurar uma instância de Nuvem AWS para Charon-SSP na documentação da Stromasys.	Arquiteto de nuvem
Anexe os volumes do EBS à instância Amazon EC2 Linux.	No EC2 console da Amazon, conecte os volumes do EBS à instância Amazon EC2 Linux. Para obter mais informações sobre isso, consulte Anexar um volume do Amazon EBS a uma instância na EC2 documentação da Amazon.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Mapeie volumes do EBS como unidades SCSI no emulador Charon-SSP.	Configure o Charon-SSP Manager para mapear os volumes do EBS como unidades SCSI nos servidores convidados Sun SPARC. Para obter mais informaçõ es sobre isso, consulte a seção de configuração de armazenamento SCSI do guia Charon-SSP V5.2 para Linux na documentação do Stromasys.	AWS DevOps
Configure o cronograma do AWS Backup para criar snapshots dos volumes do EBS.	Configure a política e os cronogramas do AWS Backup para capturar instantâneos dos volumes do EBS. Para obter mais informações sobre isso, consulte o tutorial de backup e restauração do Amazon EBS usando o AWS Backup na documentação do AWS Developer Center.	AWS DevOps

Opção de backup 4 – Criar uma VTL do AWS Storage Gateway

Tarefa	Descrição	Habilidades necessárias
Crie um dispositivo Gateway de Fitas.	Faça login no Console de Gerenciamento da AWS, abra o console do AWS Storage Gateway e crie um dispositi	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	vo Gateway de Fitas em uma VPC. Para obter mais informaçõ es sobre isso, consulte Criação de um gateway na documentação do AWS Storage Gateway.	
Crie uma instância de banco de dados do Amazon RDS para o Bacula Catalog.	Abra o console do Amazon RDS e crie uma instância de banco de dados do Amazon RDS para MySQL. Para obter mais informaçõ es sobre isso, consulte Criar uma instância de banco de dados MySQL e conectar-se a um banco de dados em uma instância de banco de dados MySQL na documentação do Amazon RDS.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Implante o controlador do aplicativo de backup na VPC.	Instale o Bacula na EC2 instância, implante o controlador do aplicativo de backup e configure o armazenamento de backup para se conectar ao dispositivo Tape Gateway. Você pode usar o exemplo de configuração do daemon de armazenamento do Bacula Director no arquivo `Bacula-storage-daemon-config.txt` (anexado). Para obter mais informações sobre isso, consulte a documentação do Bacula Director.	AWS DevOps
Configure o aplicativo de backup nos servidores convidados Sun SPARC.	Configure um segundo cliente para instalar e configurar o aplicativo de backup nos servidores convidados Sun SPARC usando o exemplo de configuração do Bacula no arquivo `SUN-SPARC-Guest-Bacula-Config.txt` (anexado).	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Defina a configuração e o agendamento do backup.	Configure a configuração e os agendamentos de backup no controlador do aplicativo de backup usando o exemplo de configuração do Bacula Director no arquivo `Bacula-Directory-Config.txt` (anexado). Para obter mais informaçõ es sobre isso, consulte a documentação do Bacula Director.	DevOps engenheiro
Valide se a configuração e os agendamentos de backup estão corretos.	Siga as instruções da documentação do Bacula para realizar os testes de validação e backup para sua configura ção nos servidores convidado s Sun SPARC. Por exemplo, você pode usar os seguintes comandos para validar os arquivos de configuração: • `bacula-dir -t -c bacula-dir.conf` • `bacula-fd -t -c bacula-fd.conf` • `bacula-sd -t -c bacula-sd.conf`	DevOps engenheiro

Recursos relacionados

- Charon virtual SPARC com licenciamento VE
- Charon virtual SPARC
- Usando serviços em nuvem e armazenamento de objetos com o Bacula Enterprise Edition
- Objetivos de recuperação de desastres (DR - Disaster recovery)
- Soluções de emulação de sistema herdado Charon

Mais informações

Opção de backup 1 – Criar uma fita virtual Stromasys

Você pode usar o seguinte exemplo de código de runbook do Systems Manager Automation para iniciar automaticamente o backup e depois trocar as fitas:

```
...
# example backup script saved in SUN SPARC Server
 #!/usr/bin/bash
 mt -f  rewind
 tar -cvf
 mt -f  offline
...
         mainSteps:
         - action: aws:runShellScript
           name:
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # Validate tape backup container file exists
               if [ ! -f {{TapeBackupContainerFile}} ]; then
                 logger -s -p local3.warning "Tape backup container file is not exists
 - {{TapeBackupContainerFile}}, create a new one"
                 touch {{TapeBackupContainerFile}}
               fi
         - action: aws:runShellScript
           name: startBackup
           inputs:
             onFailure: Abort
```

```
            timeoutSeconds: "1200"
            runCommand:
            - |
              user={{BACKUP_USER}}
              keypair={{KEYPAIR_PATH}}
              server={{SUN_SPARC_IP}}
              backup_script={{BACKUP_SCRIPT}}
              ssh -i $keypair $user@$server -c "/usr/bin/bash $backup_script"
        - action: aws:runShellScript
          name: swapVirtualDiskContainer
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              mv {{TapeBackupContainerFile}} {{TapeBackupContainerFile}}.$(date +%s)
              touch {{TapeBackupContainerFile}}
        - action: aws:runShellScript
          name: uploadBackupArchiveToS3
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              aws s3 cp {{TapeBackupContainerFile}} s3://{{BACKUP_BUCKET}}/
{{SUN_SPARC_IP}}/$(date '+%Y-%m-%d')/
 ...
```

Opção de backup 2 – Stromasys snapshot

Você pode usar o seguinte exemplo de código de runbook do Systems Manager Automation para automatizar o processo de backup:

```
      ...

         mainSteps:
         - action: aws:runShellScript
           name: startSnapshot
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
```

```
              # You may consider some graceful stop of the application before taking a
 snapshot
              # Query SSP PID by configuration file
              # Example: ps ax | grep ssp-4 | grep Solaris10.cfg | awk '{print $1"
 "$5}' | grep ssp4 | cut -f1 -d" "
              pid=`ps ax | grep ssp-4 | grep {{SSP_GUEST_CONFIG_FILE}} | awk '{print
 $1" "$5}' | grep ssp4 | cut -f1 -d" "`
              if [ -n "${pid}" ]; then
                kill -SIGTSTP ${pid}
              else
                echo "No PID found for SPARC guest with config
 {{SSP_GUEST_CONFIG_FILE}}"
                exit 1
              fi
        - action: aws:runShellScript
          name: startBackup
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              # upload snapshot and virtual disk files into S3
              aws s3 sync {{SNAPSHOT_FOLDER}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
              aws s3 cp {{VIRTUAL_DISK_FILE}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
        - action: aws:runShellScript
          name: restratSPARCGuest
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              /opt/charon-ssp/ssp-4u/ssp4u -f {{SSP_GUEST_CONFIG_FILE}} -d -a
 {{SPARC_GUEST_NAME}} --snapshot {{SNAPSHOT_FOLDER}}
 ...
```

Opção de backup 4 – AWS Storage Gateway VTL

Se você usa regiões não globais do Solaris para executar servidores Sun SPARC legados virtualizados, a abordagem do aplicativo de backup pode ser aplicada a regiões não globais executadas nos servidores Sun SPARC (por exemplo, o cliente de backup pode ser executado

dentro das regiões não globais). No entanto, o cliente de backup também pode ser executado no host Solaris e tirar instantâneos das regiões não globais. Os snapshots podem então ser copiados em uma fita.

O exemplo de configuração a seguir adiciona o sistema de arquivos que hospeda as regiões não globais do Solaris à configuração de backup do host Solaris:

```
FileSet {
   Name = "Branded Zones"
   Include {
     Options {
       signature = MD5
     }
     File = /zones
   }
 }
```

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Faça backup e arquive dados no Amazon S3 com o Veeam Backup & Replication

Criado por Jeanna James (AWS), Anthony Fiore (AWS) (AWS) e William Quigley (AWS)

Resumo

Esse padrão detalha o processo de envio de backups criados pelo Veeam Backup & Replication para classes de armazenamento de objetos compatíveis do Amazon Simple Storage Service (Amazon S3) usando o recurso de repositório de backup escalável da Veeam.

A Veeam suporta várias classes de armazenamento Amazon S3 para melhor atender às suas necessidades específicas. Você pode escolher o tipo de armazenamento com base nos requisitos de acesso aos dados, resiliência e custo de seus dados de backup ou arquivamento. Por exemplo, você pode armazenar dados que não planeja usar por 30 dias ou mais no acesso infrequente (IA) do Amazon S3 por um custo menor. Se você planeja arquivar dados por 90 dias ou mais, você pode usar o Amazon Simple Storage Service Glacier (Amazon S3 Glacier) Flexible Retrieval ou o S3 Glacier Deep Archive com o nível de arquivamento da Veeam. Você também pode usar o S3 Object Lock para fazer backups imutáveis no Amazon S3.

Esse padrão não abrange como configurar o Veeam Backup & Replication com um gateway de fita instalado. AWS Storage Gateway Para obter informações sobre esse tópico, consulte Veeam Backup & Replication usando o AWS VTL Gateway – Guia de implantação no site da Veeam.

> **Warning**
>
> Esse cenário exige que usuários AWS Identity and Access Management (IAM) tenham acesso programático e credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários. As chaves de acesso podem ser atualizadas, se necessário. Para obter mais informações, consulte Atualização de chaves de acesso no Guia de usuário do IAM.

Pré-requisitos e limitações

Pré-requisitos

- Veeam Backup & Replication, incluindo o Veeam Availability Suite ou o Veeam Backup Essentials, instalado (você pode se inscrever para um teste gratuito)
- Licença do Veeam Backup & Replication com funcionalidade Enterprise ou Enterprise Plus, que inclui a Licença Universal da Veeam (VUL - Veeam Universal License)
- Um usuário ativo do IAM com acesso a um bucket do Amazon S3
- Um usuário ativo do IAM com acesso ao Amazon Elastic Compute Cloud (Amazon EC2) e ao Amazon Virtual Private Cloud (Amazon VPC), se estiver usando o nível de arquivamento
- Conectividade de rede local ou Serviços da AWS com largura de banda disponível para backup e restauração de tráfego por meio de uma conexão pública à Internet ou de uma interface virtual AWS Direct Connect pública (VIF)
- As seguintes portas de rede e endpoints foram abertos para garantir a comunicação adequada com os repositórios de armazenamento de objetos:
  - Armazenamento do Amazon S3 – TCP – porta 443: usada para se comunicar com o armazenamento do Amazon S3.
  - Armazenamento do Amazon S3 — endpoints na nuvem — `*.amazonaws.com` para Regiões da AWS e para AWS GovCloud (US) Regions, ou para as regiões da `*.amazonaws.com.cn` China: usado para se comunicar com o armazenamento do Amazon S3. Para obter uma lista completa dos endpoints de conexão, consulte os endpoints do Amazon S3 na documentação. AWS
  - Armazenamento Amazon S3 – TCP HTTP – porta 80: usada para verificar o status do certificado. Considere que os endpoints de verificação de certificados — servidores de lista de revogação de certificados (CRL) URLs e Online Certificate Status Protocol (OCSP) — estão sujeitos a alterações. A lista real de endereços pode ser encontrada no próprio certificado.
  - Armazenamento Amazon S3 — terminais de verificação de certificados —`*.amazontrust.com`: usado para verificar o status do certificado. Considere que os endpoints de verificação de certificados (servidores CRL URLs e OCSP) estão sujeitos a alterações. A lista real de endereços pode ser encontrada no próprio certificado.

Limitações

- A Veeam não suporta políticas de ciclo de vida do S3 em nenhum bucket do S3 usado como repositório de armazenamento de objetos da Veeam. Isso inclui políticas com transições de classe de armazenamento do Amazon S3 e regras de expiração do ciclo de vida do S3. A Veeam deve ser a única entidade que gerencia esses objetos. A ativação das políticas de ciclo de vida do S3 pode ter resultados inesperados, incluindo perda de dados.

Versões do produto

- Veeam Backup & Replication v9.5, atualização 4 ou superior (somente backup ou nível de capacidade)
- Veeam Backup & Replication v10 ou superior (nível de backup ou capacidade e Bloqueio de Objetos S3)
- Veeam Backup & Replication v11 ou superior (nível de backup ou capacidade, nível de arquivamento ou arquivamento e Bloqueio de Objetos S3)
- Veeam Backup & Replication v12 ou superior (nível de desempenho, nível de backup ou capacidade, nível de arquivamento ou arquivamento e Bloqueio de Objetos S3)
- S3 Standard
- S3 Standard – IA
- S3 One Zone-IA
- S3 Glacier Flexible Retrieval (somente v11 e versões posteriores)
- S3 Glacier Deep Archive (somente v11 e versões posteriores)
- S3 Glacier Instant Retrieval (somente v12 e versões posteriores)

Arquitetura

Pilha de tecnologia de origem

- Instalação on-premises do Veeam Backup & Replication com conectividade de um servidor de backup da Veeam ou de um servidor gateway da Veeam com o Amazon S3

Pilha de tecnologias de destino

- Amazon S3
- Amazon VPC e Amazon EC2 (se estiver usando o nível de arquivamento)

Arquitetura de destino: SOBR

O diagrama a seguir mostra a arquitetura do repositório de backup escalável (SOBR - scale-out backup repository).

O software Veeam Backup and Replication protege os dados contra erros lógicos, como falhas do sistema, erros de aplicativos ou exclusões acidentais. Neste diagrama, os backups são executados primeiro on-premises e uma cópia secundária é enviada diretamente para o Amazon S3. Um backup representa uma point-in-time cópia dos dados.

O fluxo de trabalho consiste em três componentes principais que são necessários para hierarquizar ou copiar backups para o Amazon S3 e um componente opcional:

- Veeam Backup & Replication (1) – O servidor de backup responsável por coordenar, controlar e gerenciar a infraestrutura de backup, configurações, tarefas, tarefas de recuperação e outros processos.
- Servidor gateway Veeam (não mostrado no diagrama) – Um servidor gateway on-premises opcional que é necessário se o servidor de backup da Veeam não tiver conectividade de saída com o Amazon S3.
- Repositório de backup de aumento de escala horizontalmente (2) – Sistema de repositório com suporte de escalabilidade horizontal para armazenamento de dados em várias camadas. O repositório de backup de aumento de escala horizontalmente consiste em um ou mais repositórios de backup que fornecem acesso rápido aos dados e podem ser expandidos com os repositórios de armazenamento de objetos do Amazon S3 para armazenamento de longo prazo (nível de capacidade) e arquivamento (nível de arquivamento). A Veeam usa o repositório de backup de aumento de escala horizontalmente para hierarquizar dados automaticamente entre armazenamento local (nível de desempenho) e armazenamento de objetos Amazon S3 (níveis de capacidade e arquivamento).

  > **Note**
  >
  > Começando com o Veeam Backup & Replication v12.2, o recurso Direct to S3 Glacier torna o nível de capacidade do S3 opcional. Um SOBR pode ser configurado com um nível de desempenho e um nível de arquivamento S3 Glacier. Essa configuração é útil para usuários que têm investimentos significativos em armazenamento local (local) para o nível de capacidade e que precisam apenas de retenção de arquivos de longo prazo na nuvem. Para obter mais informações, consulte a documentação do Veeam Backup & Replication.

- Amazon S3 (3) — serviço de armazenamento de AWS objetos que oferece escalabilidade, disponibilidade de dados, segurança e desempenho.

Arquitetura de destino: DTO

O diagrama a seguir mostra a arquitetura direct-to-object (DTO).

Neste diagrama, os dados de backup vão diretamente para o Amazon S3 sem serem armazenados primeiro on-premises. Cópias secundárias podem ser armazenadas no S3 Glacier.

Automação e escala

Você pode automatizar a criação de recursos do IAM e buckets do S3 usando os AWS CloudFormation modelos fornecidos no repositório. VeeamHub GitHub Os modelos incluem opções padrão e imutáveis.

Ferramentas

Ferramentas e Serviços da AWS

- O Veeam Backup & Replication é uma solução da Veeam para proteger, fazer backup, replicar e restaurar seus workloads físicas e virtuais.
- AWS CloudFormationajuda você a modelar e configurar seus AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em vários Contas da AWS e. Regiões da AWS
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você pode usar EC2 a Amazon para lançar quantos servidores virtuais precisar e pode expandir ou aumentar a escala.
- AWS Identity and Access Management (IAM) é um serviço da web para controlar com segurança o acesso a. Serviços da AWS Com o IAM, você pode gerenciar centralmente usuários, credenciais de segurança, como chaves de acesso, e permissões que controlam quais AWS recursos os usuários e aplicativos podem acessar.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objeto. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.
- O Amazon S3 Glacier (S3 Glacier) é um serviço seguro e durável para arquivamento de dados de baixo custo e backup de longo prazo.
- A Amazon Virtual Private Cloud (Amazon VPC) provisiona uma seção logicamente isolada da Nuvem AWS qual você pode lançar AWS recursos em uma rede virtual que você definiu. Essa

rede virtual se assemelha a uma rede tradicional que você operaria no seu data center, com os benefícios de usar a infraestrutura dimensionável da AWS.

Código

Use os CloudFormation modelos fornecidos no VeeamHub GitHub repositório para criar automaticamente os recursos do IAM e os buckets do S3 para esse padrão. Se você preferir criar esses recursos manualmente, siga as etapas na seção Épicos.

Práticas recomendadas

- De acordo com as melhores práticas do IAM, é altamente recomendável que você alterne regularmente as credenciais de usuário do IAM de longo prazo, como o usuário do IAM que você usa para gravar backups do Veeam Backup & Replication no Amazon S3. Para obter mais informações, consulte Práticas recomendadas de segurança na documentação do IAM.

Épicos

Configurar o armazenamento do Amazon S3 na sua conta

Tarefa	Descrição	Habilidades necessárias
Criar um usuário do IAM.	Siga as instruções na documentação do IAM para criar um usuário do IAM. Esse usuário não deve ter acesso ao AWS console e você precisará criar uma chave de acesso para esse usuário. A Veeam usa essa entidade para se autentica r e ler e gravar em seus buckets S3. AWS Você deve conceder o privilégio mínimo (ou seja, conceder somente as permissões necessárias para realizar uma tarefa) para	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	que o usuário não tenha mais autoridade do que precisa. Por exemplo, políticas do IAM para anexar ao seu usuário do IAM Veeam, consulte a seção Informações adicionais. **Note** Como alternativa, você pode usar os CloudFormation modelos fornecidos no VeeamHub GitHub repositório para criar um usuário do IAM e um bucket do S3 para esse padrão.	

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	1. Faça login no AWS Management Console e abra o console do Amazon S3. 2. Se você ainda não tiver um bucket do S3 existente para usar como armazenamento de destino, escolha Create bucket e especifique o nome do bucket e as configurações do bucket. Região da AWS • Recomendamos que você habilite a opção Bloquear acesso público para o bucket do S3 e configure as políticas de acesso e permissão de usuário para atender aos requisitos da sua organização. Para ver um exemplo, consulte a documentação do Amazon S3. • Recomendamos que você ative o Bloqueio de Objetos S3, mesmo que não pretenda usá-lo imediatamente. Essa configuração só pode ser ativada no momento da criação do bucket do S3.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte Criar um bucket na documentação do Amazon S3.	

Adicione Amazon S3 e S3 Glacier Flexible Retrieval (ou S3 Glacier Deep Archive) ao Veeam Backup & Replication

Tarefa	Descrição	Habilidades necessárias
Inicie o assistente para Novo repositório de objetos.	Antes de configurar o armazenamento de objetos e os repositórios de backup escaláveis na Veeam, você deve adicionar os repositórios de armazenamento Amazon S3 e S3 Glacier que você deseja usar para os níveis de capacidade e arquivamento. No próximo épico, você conectará esses repositórios de armazenamento ao seu repositório de backup de aumento da escala horizontalmente. 1. No console da Veeam, abra a visualização da Infraestrutura de backup. 2. No painel de inventário, escolha o nó Repositórios de backup e, em seguida, escolha Adicionar repositório.	Administrador da AWS, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	3. Na caixa de diálogo Adicionar repositório de backup, escolha Armazenamento de Objeto, Amazon S3.	

Tarefa	Descrição	Habilidades necessárias
Adicionar armazenamento do Amazon S3 para o nível de capacidade.	1. Na caixa de diálogo Amazon Cloud Storage Services, escolha Amazon S3. 2. Na etapa Nome do assistente, especifique o nome do armazenamento do objeto e uma breve descrição, como o criador e a data de criação. 3. Na etapa Conta do assistente, especifique a conta de armazenamento de objetos. • Em Credenciais, escolha o usuário do IAM que você criou no primeiro épico para acessar seu armazenamento de objetos do Amazon S3. • Para a região da AWS, escolha Região da AWS onde o bucket do S3 está localizado. 4. Na etapa Bucket do assistente, especifiq ue as configurações de armazenamento de objetos. • Para a região do data center, escolha Região da AWS onde o bucket do S3 está localizado.	Administrador da AWS, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	• Para o Bucket, escolha o bucket S3 criado o primeiro épico. • Em Pasta, crie ou selecione uma pasta na nuvem para mapear seu repositório de armazenamento de objetos. • Se você quiser ativar a imutabilidade, escolha Tornar os backups recentes imutáveis por X dias e defina o período durante o qual seus backups devem ser bloqueados. Observe que habilitar a imutabilidade resulta em aumento de custos devido ao aumento do número de chamadas de API da Veeam para o Amazon S3. 5. Na etapa Resumo do assistente, revise as informações de configuração e escolha Concluir.	

Tarefa	Descrição	Habilidades necessárias
Adicione armazenamento S3 Glacier para o nível de arquivamento.	Se você quiser criar uma camada de arquivamento, use as permissões do IAM detalhadas na seção Informações adicionais. 1. Inicie o assistente para Novo repositório de objetos conforme descrito anteriormente. 2. Na caixa de diálogo Amazon Cloud Storage Services, escolha Amazon S3 Glacier. 3. Na etapa Nome do assistente, especifique o nome do armazenamento do objeto e uma breve descrição, como o criador e a data de criação. 4. Na etapa Conta do assistente, especifique a conta de armazenamento de objetos. • Em Credenciais, escolha o usuário do IAM que você criou no primeiro épico para acessar seu armazenamento de objetos do S3 Glacier. • Para a região da AWS, escolha Região da AWS onde o bucket do S3 está localizado.	Administrador da AWS, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	5. Na etapa Bucket do assistente, especifiq ue as configurações de armazenamento de objetos. • Para a região do data center, escolha Região da AWS o. • Em Bucket, selecione um bucket S3 para armazenar seus dados de backup. Esse pode ser o mesmo bucket que você usou para o nível de capacidade. • Em Pasta, crie ou selecione uma pasta na nuvem para mapear seu repositório de armazenamento de objetos. • Se você quiser ativar a imutabilidade, escolha Tornar os backups recentes imutáveis durante toda a duração da política de retenção. Observe que habilitar a imutabilidade resulta em aumento de custos devido ao aumento do número de chamadas de API da Veeam para o Amazon S3.	

Tarefa	Descrição	Habilidades necessárias
	• Se você quiser usar o S3 Glacier Deep Archive como sua classe de armazenamento de arquivamento, escolha Usar a classe de armazenamento Deep Archive. 6. Na etapa do Proxy Appliance do assistente, configure a instância auxiliar usada para transferir os dados do Amazon S3 para o S3 Glacier. Você pode usar as configurações padrão ou definir cada configuração manualmente. Para definir as configurações manualmente: • Escolha Customize (Personalizar). • EC2 Por tipo de instância, escolha o tipo de instância para o dispositivo proxy, com base em seus requisitos de velocidade e custo para transferir os arquivos de backup para a camada de arquivamento do seu repositório de backup escalável.	

Tarefa	Descrição	Habilidades necessárias
	• Para a Amazon VPC, escolha a VPC para a instância de destino. • Em Sub-rede, selecione a sub-rede do dispositivo de proxy. • Em Security group, selecione o grupo de segurança a ser associado ao dispositivo proxy. • Para a porta Redirecto r, especifique a porta TCP para as solicitações de roteamento entre o dispositivo proxy e os componentes da infraestr utura de backup. • Escolha Ok para confirmar suas configura ções. 7. Na etapa Resumo do assistente, revise as informações de configura ção e escolha Concluir.	

Adicionar repositórios de backup

Tarefa	Descrição	Habilidades necessárias
Inicie o assistente do Novo repositório de backup de	1. No console da Veeam, abra a visualização da Infraestr utura de backup.	Proprietário do aplicativo, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
aumento da escala horizontalmente.	2. No painel de inventário, escolha Repositórios de aumento da escala horizontalmente e, em seguida, escolha Adicionar repositório de aumento da escala horizontalmente.	

Tarefa	Descrição	Habilidades necessárias
Adicione um repositório de backup de aumento da escala horizontalmente e configure a capacidade e os níveis de arquivamento.	1. Na etapa Nome do assistente, especifique o nome e uma breve descrição do repositório de backup de aumento da escala horizontalmente. 2. Se necessário, adicione extensões de desempenho. Você também pode usar seu repositório de backup local Veeam existente como seu nível de desempenho. A partir da versão 12 da Veeam, você pode adicionar um bucket S3 como uma extensão de desempenho para backups direct-to-object (DTO), ignorando um nível de desempenho local. 3. Escolha Avançado e especifique opções adicionais para o repositório de backup escalável. • Escolha Usar arquivos de backup por máquina para criar um arquivo de backup separado para cada máquina e gravar esses arquivos no repositório de backup em vários fluxos simultaneamente. Essa opção é recomendada para uma	Proprietário do aplicativo, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	melhor utilização dos recursos de armazenamento e computação. • Escolha Executar backup completo quando a extensão necessária estiver off-line para criar um arquivo de backup completo caso uma extensão que contenha pontos de restauração para um backup incremental fique off-line. Essa opção requer espaço livre no repositório de backup de aumento da escala horizontalmente para hospedar um arquivo de backup completo. 4. Na etapa Política do assistente, especifique a política de posicionamento de backup para o repositório. • Escolha Localidade de dados para armazenar arquivos de backup completos e incrementais que pertencem à mesma cadeia juntos, com a mesma extensão de desempenho. Você pode armazenar arquivos	

Tarefa	Descrição	Habilidades necessárias
	que pertencem a uma nova cadeia de backup na mesma extensão de desempenho ou em outra (a menos que você use um dispositivo de armazenamento com desduplicação como extensão de desempenho). • Escolha Desempenho para armazenar arquivos de backup completos e incrementais em diferentes níveis de desempenho. Essa opção requer uma conexão de rede rápida e confiável. Se você escolher Desempenho, poderá restringir os tipos de arquivos de backup a serem armazenados em cada extensão de desempenho. Por exemplo, você pode armazenar arquivos de backup completos em uma extensão e arquivos de backup incremental em outras extensões. Para escolher os tipos de arquivo: • Escolha Customize (Personalizar).	

Tarefa	Descrição	Habilidades necessárias
	• Na caixa de diálogo Configurações de Colocação de Backup, escolha uma extensão de desempenho e, em seguida, escolha Editar. • Escolha o tipo de arquivo de backup que você deseja armazenar na extensão. 5. Na etapa de Nível de capacidade do assistent e, configure o nível de armazenamento de longo prazo que você deseja anexar ao repositório de backup escalável. • Escolha Estender a capacidade escalável do repositório de backup com armazenamento de objetos. Para o repositór io de armazenamento de objetos, escolha o armazenamento Amazon S3 para o nível de capacidade que você adicionou no épico anterior. • Escolha Janela para selecionar uma janela de tempo para mover ou copiar dados.	

Tarefa	Descrição	Habilidades necessárias
	• Escolha Copiar backups para o armazenamento de objetos assim que forem criados para copiar todos os arquivos de backup criados recentemente ou somente os arquivos de backup criados recentemente até o limite da capacidade. • Escolha Mover backups para o armazenamento de objetos à medida que envelhecem, fora da janela de restaurações operacionais para transferir cadeias de backup inativas até o limite da capacidade. No campo Mover arquivos de backup com mais de X dias, especifique um período após o qual os arquivos de backup devem ser descarregados. (Para descarregar cadeias de backup inativas no dia em que foram criadas, especifique 0 dias.) Você também pode escolher Substituir para mover os arquivos de backup mais cedo se	

Tarefa	Descrição	Habilidades necessárias
	o repositório de backup escalável tiver atingido um limite especificado por você. • Escolha Criptografar dados enviados para o armazenamento de objetos e especifique uma senha para criptografar todos os dados e seus metadados para descarga. Escolha Adicionar ou Gerenciar senhas para especificar uma nova senha. 6. Na etapa Nível de arquivo do assistente, configure a camada de armazenamento de arquivamento que você deseja anexar ao repositório de backup escalável. (Essa etapa não aparece se você pulou a adição do armazenamento do Amazon S3 Glacier.) • Escolha Arquivar backups completos do GFS no armazenamento de objetos. Para o repositório de armazenamento de objetos, escolha o armazenamento Amazon S3 Glacier que você	

Tarefa	Descrição	Habilidades necessárias
	adicionou no épico anterior. • Para arquivar backups do GFS com mais de N dias, escolha uma janela de tempo para mover arquivos para a extensão de arquivamento. (Para arquivar cadeias de backup inativas no dia em que foram criadas, especifique 0 dias.) 7. Na etapa Resumo do assistente, revise a configuração do repositór io de backup expansível e escolha Concluir.	

Recursos relacionados

- Criação de um usuário do IAM em sua Conta da AWS (documentação do IAM)
- Criar um bucket (documentação do Amazon S3)
- Bloquear o acesso público ao armazenamento do Amazon S3 (documentação do Amazon S3)
- Usando o Bloqueio de Objetos S3 (documentação do Amazon S3)
- Documentação técnica do Veeam
- Como criar uma política do IAM segura para conexão com o armazenamento de objetos do S3 (documentação da Veeam)

Mais informações

As seções a seguir fornecem exemplos de políticas do IAM que você pode usar ao criar um usuário do IAM na seção Épicos desse padrão.

Política do IAM para nível de capacidade

> **Note**
>
> Altere o nome dos buckets S3 no exemplo de política de `<yourbucketname>` para o nome do bucket S3 que você deseja usar para backups de nível de capacidade da Veeam. Observe também que a política deve ser restrita aos recursos específicos usados pela Veeam (indicados pela `Resource` especificação na política a seguir) e que a primeira parte da política desativa a criptografia do lado do cliente, conforme discutido na postagem do AWS blog Prevenindo a criptografia não intencional de objetos do Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RestrictSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<your-bucket-name>/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "false"
                }
            }
        },
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectVersion",
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:PutObjectLegalHold",
                "s3:GetBucketVersioning",
                "s3:GetObjectLegalHold",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObject*",
                "s3:GetObject*",
                "s3:GetEncryptionConfiguration",
                "s3:PutObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
```

```
                "s3:DeleteObject*",
                "s3:DeleteObjectVersion",
                "s3:GetBucketLocation"

            ],
            "Resource": [
                "arn:aws:s3:::<yourbucketname>",
                "arn:aws:s3:::<yourbucketname>/*"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Política do IAM para o nível de arquivamento

> **Note**
>
> Altere o nome dos buckets S3 no exemplo de política de `<yourbucketname>` para o nome do bucket S3 que você deseja usar para backups da camada de arquivamento da Veeam.

Para usar sua VPC, sub-rede e grupos de segurança existentes:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
```

```
                "s3:RestoreObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "s3:PutObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket-name>",
                "arn:aws:s3:::<bucket-name>/*"
            ]
        }
    ]
}

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:RunInstances",
                "ec2:DeleteKeyPair",
                "ec2:DescribeVpcAttribute",
                "ec2:CreateTags",
                "ec2:DescribeSubnets",
                "ec2:TerminateInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs"
            ],
            "Resource": "arn:aws:ec2:<region>:<account-id>:*"
        }
```

```
    ]
}
```

Para criar novos VPC, sub-rede e grupos de segurança:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:RestoreObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "s3:PutObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket-name>",
                "arn:aws:s3:::<bucket-name>/*"
            ]
        }
    ]
}

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:DescribeInstances",
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:RunInstances",
                "ec2:DeleteKeyPair",
                "ec2:DescribeVpcAttribute",
                "ec2:CreateTags",
                "ec2:DescribeSubnets",
                "ec2:TerminateInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateRoute",
                "ec2:CreateInternetGateway",
                "ec2:AttachInternetGateway",
                "ec2:ModifyVpcAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstanceTypes"
            ],
            "Resource": "*"
        }
    ]
}
```

Configurar a Veritas NetBackup para VMware nuvem na AWS

Criado por Shubham Salani (AWS)

Resumo

Aviso: a partir de 30 de abril de 2024, o VMware Cloud on AWS não é mais revendido pela AWS ou por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu representante da AWS para obter detalhes.

Muitas empresas usam a Veritas NetBackup como uma solução de backup e recuperação para suas cargas de trabalho locais baseadas no VMware vSphere. Depois que as empresas migram suas cargas de trabalho para data centers definidos por software (SDDCs) na nuvem na infraestrutura da Amazon VMware Web Services (AWS), não há um procedimento claro de integração. lift-and-shift NetBackup Esse padrão descreve como você pode configurar a Veritas NetBackup em sua conta da AWS e configurá-la para fazer backup das cargas de trabalho em sua. VMware SDDCs

Esse padrão não inclui instruções para migrar suas cargas de trabalho. Para obter mais informações, consulte Migrar VMware SDDC para a VMware nuvem na AWS usando VMware o HCX. Ao configurar suas cargas de trabalho na VMware nuvem na AWS, use um cluster estendido (VMware documentação). Nessa configuração, seu cluster abrange duas zonas de disponibilidade da AWS em uma única região. Isso fornece alta disponibilidade e resiliência no caso de uma das zonas de disponibilidade ficar indisponível. O Elastic DRS e um host testemunha do vSAN VMware (documentação) copiam perfeitamente os dados para uma terceira zona de disponibilidade, conhecida como domínio de falhas. Essa solução de paridade poderá ajudá-lo a recuperar os dados em caso de falha. Como essa abordagem exige três zonas de disponibilidade, ao selecionar uma região da AWS para seu ambiente de VMware nuvem, certifique-se de que ela tenha três ou mais zonas de disponibilidade. Para ter mais informações, consulte Regiões e zonas de disponibilidade.

Nesse padrão, cada SDDC tem um host de backup, que é um servidor proxy. Usando instâncias do Amazon Elastic Compute Cloud (Amazon EC2), você configura os servidores NetBackup mestre e de mídia em uma nuvem privada virtual (VPC) separada, uma para cada SDDC. Como as interfaces de rede elástica fornecem alta largura de banda e baixa latência, você as usa para configurar a conectividade entre os hosts de backup e seus servidores NetBackup mestre e de mídia correspondentes. As EC2 instâncias direcionam os backups para os volumes do Amazon Elastic Block Store (Amazon EBS), que é o primeiro ponto de backup. Você pode usar DataSync a AWS para manter seus volumes do EBS SDDCs sincronizados.

Você também poderá usar o AWS Transit Gateway e um endpoint da VPC da interface para conectar os volumes do EBS a outro serviço de armazenamento, por exemplo, o Amazon Simple Storage Service (Amazon S3). De acordo com sua política de retenção, você poderá usar as classes de armazenamento S3 Intelligent-Tiering S3 Glacier para otimizar seus custos de armazenamento. Para obter mais informações, consulte Como usar as classes de armazenamento do Amazon S3 (Documentação do Amazon S3).

Pré-requisitos e limitações

Pré-requisitos

- Seu ambiente VMware Cloud on AWS usa um cluster estendido que abrange duas zonas de disponibilidade.
- O host de backup deve residir no SDDC VMware Cloud on AWS que tem acesso ao armazenamento de dados em que os arquivos do VMware Virtual Machine Disk File (VMDK) são implantados.
- HotAdd o modo de transporte deve estar ativado no NetBackup cliente para fazer backup e restaurar máquinas virtuais (VMs) e deve permitir restaurações a partir de arquivos e pastas direcionados ao usuário.

Limitações

- O servidor NetBackup mestre deve usar a resolução DNS para um endereço IP privado para o host de backup do vCenter no SDDC.
- Os arquivos hosts no servidor NetBackup mestre e no host de backup devem conter o seguinte:
  - O endereço IP privado e o nome DNS privado do servidor mestre
  - O endereço IP privado e o nome DNS privado do host de backup
- Se você estiver configurando um endpoint da VPC de interface para um bucket do S3, o firewall do SDDC Compute Gateway deverá ser configurado para permitir HTTPS de uma fonte de bloco de Encaminhamento Entre Domínios Sem Classificação (CIDR). Para obter mais informações, consulte Acessar um bucket do S3 usando um endpoint do S3 (documentação)VMware .
- VMware O Cloud on AWS não oferece suporte aos seguintes recursos de NetBackup:
  - Fazer backup ou restaurar modelos de VM
  - Usando o NetBackup vSphere Client (plug-in) HTML5
  - Bloqueio e desbloqueio VMs para backups ou restaurações

- Os backups não poderão ser armazenados em um datastore do vSAN
- Modos de transporte de dispositivo de blocos de rede (NBD), NBDSSL e SAN

Versões do produto

- VMware Cloud on AWS SDDC versão 1.0 ou posterior
- Veritas NetBackup versão 8.1.2 ou posterior
- Versão Linux 6.8 ou superior
- VMware vSphere versão 6.0 ou posterior

Arquitetura

O diagrama a seguir mostra a configuração do NetBackup for VMware Cloud on AWS. Os servidores NetBackup mestre e de mídia são implantados em uma VPC separada e conectados aos hosts de backup por meio de interfaces de SDDCs rede elástica. Os servidores NetBackup mestre e de mídia armazenam os backups nos volumes do Amazon EBS. Opcionalmente, você pode configurar armazenamento adicional nos buckets do Amazon S3 usando o AWS Transit Gateway e um endpoint VPC da PrivateLink interface da AWS.

Ferramentas

Ferramentas e serviços da AWS

- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (Amazon). EC2
- PrivateLinkA AWS ajuda você a criar conexões unidirecionais e privadas de suas nuvens privadas virtuais (VPCs) para serviços fora da VPC.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outros serviços

- VMware O Cloud on AWS é uma oferta de nuvem integrada desenvolvida em conjunto pela Amazon Web Services (AWS) e. VMware
- NetBackup para VMware backups e restaurações das máquinas VMware virtuais que são executadas em VMware ESXi hosts.

Épicos

Configurar os NetBackup servidores

Tarefa	Descrição	Habilidades necessárias
Atualize as regras do firewall.	Atualize as regras de firewall para estabelecer conectividade entre o SDDC VMware Cloud on AWS e os servidores NetBackup mestre e de mídia. Faça o seguinte: 1. Faça login na VMware nuvem na AWS em https://vmc.vmware.com/ 2. Na guia Rede e segurança, escolha Gateway Firewall. 3. Na página Gateway Firewall, escolha Compute Gateway. 4. Escolha ADICIONAR regra e, em seguida, crie uma nova regra com as configurações de porta de firewall necessárias. Para obter mais informações, consulte os requisitos de porta de NetBackup firewall (documentação da Veritas).	Administrador de rede, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Inicie os servidores NetBackup mestre e de mídia.	1. Faça login no AWS Management Console e abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/ 2. Inicie uma EC2 instância (EC2 documentação da Amazon) e use os seguintes detalhes de configuração: a. Para os servidores NetBackup mestre e de mídia, selecione a `NBU-Linux-GA-8-1-2-Setup-f032d23e-881b-4dee-ba70-b9ca3e915910-ami-072509a7ffc156938.4` Amazon Machine Image (AMI). Essa AMI pré-configurada está disponível por meio do AWS Marketplace. b. Selecione um tipo de instância. NetBackup recomendado `m5.2xlarge` para os servidores mestre e de mídia.	Administrador de nuvem, administrador de backup

Tarefa	Descrição	Habilidades necessárias
Configure o host de backup para NetBackup.	1. Faça login na VMware nuvem na AWS em https://vmc.vmware.com/ 2. Selecione o SDDC 3. Escolha a guia Abrir VCENTER. Isso abre o SDDC vCenter. 4. Anote o nome de domínio totalmente qualificado (FQDN) do host de backup. 5. Faça login no console de NetBackup administração. Para obter mais informaçõ es, consulte Como fazer login no console NetBackup administrativo (document ação da Veritas). 6. Selecione os servidores mestre e de mídia e, em seguida, escolha VMware Access Hosts. 7. Adicione o FQDN do host de backup. 8. Escolha Apply e, em seguida, escolha OK.	Administrador de nuvem, administrador de backup

(Opcional) Configure o armazenamento do Amazon S3

Tarefa	Descrição	Habilidades necessárias
Configure o armazenamento no Amazon S3.	1. Analise as opções de armazenamento em nuvem do Amazon S3	Administrador AWS, Geral AWS

Tarefa	Descrição	Habilidades necessárias
	(Documentação da Veritas) e selecione a classe de armazenamento adequada para suas necessidades. 2. Configure NetBackup para usar o Amazon S3 para armazenamento em nuvem de acordo com as instruções em Configuração do armazenamento em nuvem em NetBackup (documentação da Veritas).	

Recursos relacionados

Documentação da AWS

- Crie uma interface VPC endpoint (documentação da AWS) PrivateLink

Documentação da Veritas

- NetBackup requisitos de porta de firewall

VMware documentação

- Implantar uma VM a partir de um modelo OVF em uma biblioteca de conteúdo
- VMware Cobranças de transferência de dados na nuvem na AWS: como funciona? (postagem VMware no blog)
- VMware Nuvem na AWS: clusters estendidos

Copiar dados de um bucket do S3 para outra conta e região usando a AWS CLI

Criado por Appasaheb Bagali (AWS) e Purushotham G K (AWS)

Resumo

Este padrão descreve como migrar dados de um bucket do Amazon Simple Storage Service (Amazon S3) em uma conta de origem da AWS para um bucket do S3 de destino em outra conta da AWS, na mesma região da AWS ou em uma região diferente.

O bucket do S3 de origem permite acesso ao AWS Identity and Access Management (IAM) usando uma política de recursos anexada. Um usuário na conta de destino precisa assumir uma função que tenha permissões `PutObject` e `GetObject` para o bucket de origem. Por fim, você executa os comandos `copy` e `sync` para transferir dados do bucket do S3 de origem para o bucket do S3 de destino.

As contas são proprietárias dos objetos que carregam nos buckets do S3. Se você copiar objetos entre contas e regiões, concederá à conta de destino a propriedade dos objetos copiados. Você pode alterar a propriedade de um objeto alterando sua lista de controle de acesso (ACL) para `bucket-owner-full-control`. No entanto, recomendamos que você conceda permissões programáticas entre contas à conta de destino, pois ACLs pode ser difícil gerenciar vários objetos.

> **Warning**
>
> Esse cenário exige que os usuários do IAM tenham acesso programático e credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessári as para realizar a tarefa e que você os remova quando não forem mais necessários. As chaves de acesso podem ser atualizadas, se necessário. Para obter mais informações, consulte Atualização de chaves de acesso no Guia de usuário do IAM.

Esse padrão abrange a migração única. Para cenários que exigem migração contínua e automática de novos objetos de um bucket de origem para um bucket de destino, você pode usar o S3 Batch Replication em vez disso, conforme descrito no padrão Copiar dados de um bucket do S3 para outra conta e região usando o S3 Batch Replication.

Pré-requisitos e limitações

- Duas contas da AWS ativas na mesma ou em diferentes regiões da AWS.
- Um bucket do S3 existente na conta de origem.
- Se o bucket do Amazon S3 de origem ou destino tiver a criptografia padrão habilitada, você deverá modificar as permissões da chave do AWS Key Management Service (AWS KMS). Para obter mais informações, consulte o artigo AWS ref: Publicação sobre este tópico.
- Familiaridade com permissões entre contas.

Arquitetura

Ferramentas

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir com serviços da AWS através de comandos na sua shell da linha de comando.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

Práticas recomendadas

- Práticas recomendadas de segurança no IAM (documentação do IAM)
- aplicativo de permissões com privilégios mínimos (documentação do IAM)

Épicos

Criar um usuário e um perfil do IAM na conta da AWS de destino

Tarefa	Descrição	Habilidades necessárias
Criar um usuário do IAM e obter a chave de acesso.	1. Cadastre-se no Console de Gerenciamento da	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	AWS e crie um usuário do IAM que tenha acesso programático. Para ver as etapas detalhadas, consulte Criação de usuários do IAM na documentação do IAM. Não há necessidade de anexar nenhuma política para esse usuário. 2. Gere uma chave de acesso e uma chave secreta para esse usuário. Para obter instruções, consulte Conta e chaves de acesso da AWS na documentação da AWS.	

Tarefa	Descrição	Habilidades necessárias
Criar uma política do IAM baseada em identidade.	Crie uma política baseada em identidade do IAM nomeada `S3MigrationPolicy` usando as seguintes permissões. Para ver as etapas detalhadas, consulte Criação de políticas do IAM na documentação do IAM. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:ListBucket", "s3:GetObject", "s3:GetObjectTagging", "s3:GetObjectVersion", "s3:GetObjectVersionTagging" ], "Resource": [ "arn:aws:s3:::amazon-s3-demo-source-bucket",`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>"arn:aws:s3:::amazon-s3-demo-source-bucket/*"
	            ]
	        },
	        {
	            "Effect": "Allow",
	            "Action": [
	"s3:ListBucket",
	"s3:PutObject",
	"s3:PutObjectAcl",
	"s3:PutObjectTagging",
	"s3:GetObjectTagging",
	"s3:GetObjectVersion",
	"s3:GetObjectVersionTagging"
	            ],
	            "Resource": [
	"arn:aws:s3:::amazon-s3-demo-destination-bucket",
	"arn:aws:s3:::amazon-s3-demo-destination-bucket/*"
	            ]
	        }
	    ]</pre>	

Tarefa	Descrição	Habilidades necessárias
	} **Note** Modifique os nomes dos buckets de origem e destino de acordo com seu caso de uso. Essa política baseada em identidade permite que o usuário que está assumindo essa função acesse o bucket de origem e o bucket de destino.	

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM.	Crie um perfil do IAM denominado `S3MigrationRole` usando a seguinte política de confiança e então anexe a `S3MigrationPolicy` criada anteriormente. Para obter as etapas detalhadas, consulte Criar um perfil para delegar permissões a um usuário do IAM na documentação do IAM. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<destination_account>:user/<user_name>" }, "Action": "sts:AssumeRole", "Condition": {} } ] }` **Note** Modifique o Amazon Resource Name	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	(ARN) da função do IAM de destino ou nome de usuário na política de confiança de acordo com seu caso de uso. Essa política de confiança permite que o usuário do IAM recém-criado assuma `S3MigrationRole` .	

Criar e anexar a política de bucket do S3 na conta de origem

Tarefa	Descrição	Habilidades necessárias
Criar e anexar uma política de bucket do S3.	Faça login no Console de Gerenciamento da AWS da sua origem e abra o console do Amazon S3. Escolha sua origem do bucket do S3 e selecione Permissões. Em Política de bucket, selecione Editar e cole a seguinte política de bucket. Escolha Salvar. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "DelegateS3Access",`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

```
            "Effect":
 "Allow",
            "Principa
l": {"AWS": "arn:aws:
iam::<destination_
account>:role/<Rol
eName>"},
            "Action":
 ["s3:ListBucket",

 "s3:GetObject",

  "s3:GetObjectTaggi
ng",

  "s3:GetObjectVersi
on",

  "s3:GetObjectVersi
onTagging"

 ],
            "Resource":
 [

 "arn:aws:s3:::amazon-
s3-demo-source-bucket/
*",

 "arn:aws:s3:::amazon-
s3-demo-source-bucket"
            ]
        }
    ]
}
```

> **Note**
>
> Certifique-se de incluir o ID da conta da AWS para a conta de

Tarefa	Descrição	Habilidades necessárias
	destino e configurar o modelo de política de bucket de acordo com seus requisitos. Essa política baseada em recursos permite que a função `S3MigrationRole` de destino acesse objetos do S3 na conta de origem.	

Configurar o bucket do S3 de destino

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3 de destino.	Faça login no Console de Gerenciamento da AWS da sua origem, abra o console do Amazon S3 e selecione Criar bucket. Criar um bucket do S3 de acordo com suas necessidades. Para obter mais informações, consulte Criar um bucket na documentação do Amazon S3.	Administrador de nuvem

Copiar dados para o bucket do S3 de destino

Tarefa	Descrição	Habilidades necessárias
Configurar a AWS CLI com as credenciais de usuário recém-criadas.	1. Instale a versão mais recente da AWS CLI. Para obter instruções, consulte	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Instalar ou atualizar a versão mais recente da AWS CLI na documentação da AWS CLI. 2. Execute `$ aws configure` e atualize a CLI com a chave de acesso da AWS do usuário que você criou. Para obter mais informações, consulte Arquivos de configuração e credencial na documentação da AWS CLI.	

Tarefa	Descrição	Habilidades necessárias
Assumir a função de migração do S3.	1. Usar a AWS CLI para assumir `S3MigrationRole` : `aws sts assume-role \ --role-arn "arn:aws:iam::<destination_account>:role/S3MigrationRole" \ --role-session-name AWSCLI-Session` Esse comando gera várias informações. Dentro do bloco de credenciais, você precisa de `AccessKeyId` , `SecretAccessKey` , e `SessionToken` . Este exemplo usa as variáveis de ambiente `RoleAccessKeyID` , `RoleSecretKey` e `RoleSessionToken` . Observe que o timestamp do campo de expiração está no fuso horário UTC. O timestamp indica quando as credenciais temporárias do perfil do IAM expiram. Se as credenciais temporárias expirarem, você deverá chamar a API `sts:AssumeRole` novamente.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	2. Criar três variáveis de ambiente para assumir o perfil do IAM. Essas variáveis de ambiente são preenchidas com a seguinte saída:
	
	`# Linux`
	`export AWS_ACCES S_KEY_ID=RoleAcces sKeyID`
	`export AWS_SECRE T_ACCESS_KEY=RoleS ecretKey`
	`export AWS_SESSI ON_TOKEN=RoleSessi onToken`
	`# Windows`
	`set AWS_ACCES S_KEY_ID=RoleAcces sKeyID`
	`set AWS_SECRE T_ACCESS_KEY=RoleS ecretKey`
	`set AWS_SESSI ON_TOKEN=RoleSessi onToken`
	
	3. Confira se você assumiu o perfil do IAM digitando o seguinte comando:
	
	`aws sts get-caller-identity`
	
	Para obter mais informaçõ es, consulte o Centro de Conhecimentos da AWS.	

Tarefa	Descrição	Habilidades necessárias

Copiar e sincronizar dados do bucket do S3 de origem para o bucket do S3 de destino.	Depois de assumir a função `S3MigrationRole` , você pode copiar os dados usando o comando copy (cp) ou synchronize (sync).
	
	Copiar (consulte a Referência de comandos da CLI para obter detalhes):
	
	`aws s3 cp s3://amazon-s3-demo-source-bucket/ \ s3://amazon-s3-demo-destination-bucket/ \ --recursive --source-region SOURCE-REGION-NAME --region DESTINATION-REGION-NAME`
	
	Sincronizar (consulte a Referência de comandos da CLI para obter detalhes):
	
	`aws s3 sync s3://amazon-s3-demo-source-bucket/ \ s3://amazon-s3-demo-destination-bucket/ \ --source-region SOURCE-REGION-NAME --region DESTINATION-REGION-NAME`
		Administrador de nuvem

Solução de problemas

Problema	Solução
Ocorreu um erro (`AccessDenied`) ao chamar a operação `ListObjects`: acesso negado	• Certifique-se de ter assumido a função`S3MigrationRole`. • Execute `aws sts get-caller-identity` para verificar a função usada. Se a saída não exibir o ARN para `S3MigrationRole`, assuma a função novamente e tente novamente.

Recursos relacionados

- Criar um bucket do S3 (documentação do Amazon S3)
- Políticas e políticas de usuário do bucket do S3 (documentação do Amazon S3)
- Identidades do IAM (usuários, grupos e perfis) (documentação do IAM)
- comando cp (documentação da AWS CLI)
- comando sync (documentação da AWS CLI)

Copie dados de um bucket do S3 para outra conta e região usando o S3 Batch Replication

Criado por Appasaheb Bagali (AWS), Lakshmikanth B D (AWS), Purushotham G K (AWS), Shubham Harsora (AWS) e Suman Rajotia (AWS)

Resumo

Esse padrão explica como você pode usar a replicação em lote do Amazon Simple Storage Service (Amazon S3) para copiar automaticamente o conteúdo de um bucket do S3 para outro bucket do S3, sem qualquer intervenção manual, depois de configurar os buckets. Os buckets de origem e destino podem estar na mesma região ou em regiões diferentes Contas da AWS .

O S3 Batch Replication oferece uma maneira de replicar objetos do Amazon S3 que existiam antes de uma configuração de replicação estar em vigor, objetos que foram replicados anteriormente e objetos que falharam na replicação. Esse método usa um trabalho de operações em lote do S3. Quando o trabalho for concluído, você receberá um relatório de conclusão.

Você pode usar o S3 Batch Replication em cenários que exigem migração contínua e automática de novos objetos de um bucket de origem para um bucket de destino. Para uma migração única, você pode usar o AWS Command Line Interface (AWS CLI) em vez disso, conforme descrito no padrão Copiar dados de um bucket do S3 para outra conta e região usando o. AWS CLI

Pré-requisitos e limitações

- Uma fonte Conta da AWS.
- Um destino Conta da AWS.
- Um bucket do S3 na conta de origem com alguns objetos (arquivos ou pastas).
- Um ou mais buckets S3 na conta de destino.
- Versionamento do S3 ativado nos buckets de origem e destino.
- AWS Identity and Access Management Permissões (IAM) para criar uma política do IAM, uma função do IAM e uma política de bucket do S3 nas contas de origem e destino.
- As regras de ciclo de vida do Amazon S3 estão desativadas enquanto a tarefa de replicação em lote do S3 está ativa. Isso garante a paridade entre os buckets de origem e destino. Caso contrário, o bucket de destino pode não ser uma réplica exata do bucket de origem.

Arquitetura

Ferramentas

AWS serviços

- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Práticas recomendadas

O vídeo a seguir do AWS re:Invent 2022 discute as melhores práticas para usar a replicação do Amazon S3 para conformidade regulatória, proteção de dados e maior desempenho de aplicativos.

https://www.youtube-nocookie.com/embed/seu JEb ISBL04? controles = 0

Épicos

Crie uma política e uma função do IAM para replicação entre contas na conta de origem

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM para replicação entre contas.	Na conta AWS de origem: 1. Abra o console do IAM. 2. Crie uma nova política do IAM. 3. Na seção Editor de políticas , escolha JSON e cole o código a seguir. `{ "Version": "2012-10-17", "Statement": [`	Administrador de nuvem, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	{ "Sid": "GetSourceBucketConfiguration", "Effect": "Allow", "Action": ["s3:ListBucket", "s3:GetBucketLocation", "s3:GetBucketAcl", "s3:GetReplicationConfiguration", "s3:GetObjectVersionForReplication", "s3:GetObjectVersionAcl", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::source-bucket-name", "arn:aws:s3:::source-bucket-name/*"] }, { "Sid": "ReplicateToDestinationBuckets",	

Tarefa	Descrição	Habilidades necessárias
	"Effect": "Allow", "Action": ["s3:List*", "s3:*Object", "s3:ReplicateObject", "s3:ReplicateDelete", "s3:ReplicateTags"], "Resource": ["arn:aws:s3:::destination-bucket-name*", "arn:aws:s3:::destination-bucket-name/*"] }, { "Sid": "PermissionToOverrideBucketOwner", "Effect": "Allow", "Action": ["s3:ObjectOwnerOverrideToBucketOwner"],	

Tarefa	Descrição	Habilidades necessárias
	"Resource": ["arn:aws:s3:::destination-bucket-name*", "arn:aws:s3:::destination-bucket-name/*"] }] } Essa política inclui três declarações: • `GetSourceBucketConfiguration` fornece acesso à configuração de replicação e à versão do objeto para replicação no bucket de origem. • `ReplicateToDestinationBuckets` fornece acesso para replicar no bucket de destino. Você pode especificar vários buckets de destino na matriz. • `PermissionToOverrideBucketOwner` fornece acesso para `ObjectOwnerOverrid`	

Tarefa	Descrição	Habilidades necessárias
	`eToBucketOwner` que o bucket de destino possa possuir os objetos na conta de destino que foram replicados da conta de origem. 4. Escolha Avançar, forneça um nome de política como `ecross-account-bucket-replication-policy` , em seguida, escolha Criar política. Para obter mais informações, consulte Criar políticas do IAM na documentação do IAM.	

Tarefa	Descrição	Habilidades necessárias
Crie uma função do IAM para replicação entre contas.	Na conta AWS de origem: 1. No console do IAM, crie uma função do IAM com as seguintes informações: a. Em Tipo de entidade confiável, escolha Serviços da AWS. b. Para manutenção, escolha S3. c. Para o caso de uso, escolha S3 Batch Operations. d. Escolha a política que você criou na etapa anterior. 2. Forneça um nome de função, como cross-account-bucket-replication-role, e escolha Create role. Para obter mais informações, consulte Criação de funções do IAM na documentação do IAM.	Administrador de nuvem, administrador da AWS

Crie uma regra de replicação na conta de origem

Tarefa	Descrição	Habilidades necessárias
Crie uma regra de replicação em relação ao bucket de origem na conta de origem.	Na conta AWS de origem: 1. Abra o console Amazon S3.	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	2. Navegue até o bucket de origem e escolha a guia Gerenciamento. 3. Crie uma regra de replicação com a seguinte configuração: a. Forneça um nome de regra, como `s3-replication-rule`. b. Em Status, escolha Enabled. c. Para o escopo da regra, escolha Aplica-se a todos os objetos no bucket. d. Em Destino, escolha Especificar um compartimento em outra conta e, em seguida, insira o Conta da AWS número do destino e o nome do compartimento. e. Escolha a opção de alterar a propriedade do objeto para o proprietário do bucket de destino. f. Para a função do IAM, escolha a função que você criou anteriormente na conta de origem. g. Para opções adicionais de replicação, selecione todas as opções	

Tarefa	Descrição	Habilidades necessárias
	disponíveis. Eles fornecem a capacidad e de replicar conteúdo rapidamente, monitorar o progresso da replicação por meio de CloudWatc h métricas da Amazon, replicar marcadores de exclusão e replicar alterações de metadados . h. Escolha Salvar. 4. Se você tiver vários buckets de destino, crie regras adicionais de replicação. Para obter mais informaçõ es, consulte Como configura r a replicação quando os buckets de origem e destino pertencem a contas diferentes na documentação do Amazon S3.	

Aplique uma política de bucket ao bucket de destino

Tarefa	Descrição	Habilidades necessárias
Aplique uma política de bucket ao bucket de destino.	Essa etapa deve ser executada para cada bucket de destino individualmente nas contas de AWS destino. Na conta AWS de destino:	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
	1. Abra o console do Amazon S3, navegue até o bucket de destino e escolha a guia Permissões. 2. Edite a política do bucket fornecendo o seguinte código JSON e salve a política: `{ "Version": "2012-10-17", "Id": "PolicyForDestinationBucket", "Statement": [{ "Sid": "Permissions on objects and buckets", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::SourceAWSAccountNumber:role/IAM-Role-created-in-step1-in-source-account" }, "Action": ["s3:List*", "s3:GetBucketVersioning", "s3:PutBucketVersioning",`	

Tarefa	Descrição	Habilidades necessárias

	"s3:ReplicateDelete",
	"s3:ReplicateObject"
	],
	"Resource":
	[
	"arn:aws:s3:::dest
	ination-bucket",
	"arn:aws:s3:::dest
	ination-bucket/*"
	]
	},
	{
	"Sid":
	"Permission to
	override bucket owner",
	"Effect":
	"Allow",
	"Principa
	l": {
	"AWS":
	"arn:aws:iam::Sour
	ceAWSAccountNumber
	:role/IAM-Role-cre
	ated-in-step1-in-s
	ource-account"
	},
	"Action":
	"s3:ObjectOwnerOve
	rrideToBucketOwner",
	"Resource
	": "arn:aws:s3:::dest
	ination-bucket/*"
	}
	]
	}	

Tarefa	Descrição	Habilidades necessárias
	Essa política inclui duas declarações: • `Permissions on objects and bucketsindica` que o bucket de destino pode replicar o conteúdo com base na função definida na conta de origem. A função fornece permissões para o bucket de origem. • `Permission to override bucket ownerindica` que o bucket de destino tem permissões para substituir a proprieda de da conta de origem.	

Teste a replicação entre contas do Amazon S3

Tarefa	Descrição	Habilidades necessárias
Verifique se a replicação funciona corretamente.	1. Adicione um objeto ao bucket de origem. 2. Verifique se o novo objeto aparece nos buckets do S3 nas contas de destino. 3. Veja CloudWatch as métricas: a. No bucket de origem, escolha a guia Métricas.	Administrador da AWS, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	b. Na seção Métricas de replicação, selecione uma regra de replicação. c. Escolha Display charts (Exibir gráficos). Os gráficos refletem o estado da replicação exibindo as operações que estão pendentes de replicação, a latência da replicação e os bytes pendentes de replicação. Para obter mais informaçõ es, consulte Métricas de monitoramento com a Amazon CloudWatch na documentação do Amazon S3.	

Recursos relacionados

- Quando eu uso o IAM? (Documentação do IAM)
- Como o IAM funciona (documentação do IAM)
- Criação de funções do IAM (documentação do IAM)
- Criação de políticas do IAM (Documentação do IAM)
- Visão geral do gerenciamento de acesso: permissões e políticas (documentação do IAM)
- Criação, configuração e trabalho com buckets do Amazon S3 (documentação do Amazon S3)
- Carregar, baixar e trabalhar com objetos no Amazon S3 (documentação do Amazon S3)
- Replicação de objetos (documentação do Amazon S3)

Migre dados de um ambiente Hadoop local para o Amazon S3 usando com a AWS para o Amazon S3 DistCp PrivateLink

Criado por Jason Owens (AWS), Andres Cantor (AWS), Jeff Klopfenstein (AWS), Bruno Rocha Oliveira (AWS) e Samuel Schmidt (AWS)

Resumo

Esse padrão demonstra como migrar praticamente qualquer quantidade de dados de um ambiente Apache Hadoop local para a nuvem da Amazon Web Services (AWS) usando a ferramenta de código aberto Apache com a DistCpAWS PrivateLink para o Amazon Simple Storage Service (Amazon S3). Em vez de usar a Internet pública ou uma solução de proxy para migrar dados, você pode usar a AWS PrivateLink para Amazon S3 para migrar dados para o Amazon S3 por meio de uma conexão de rede privada entre seu datacenter local e uma Amazon Virtual Private Cloud (Amazon VPC). Se você usar entradas de DNS no Amazon Route 53 ou adicionar entradas no arquivo /etc/hosts em todos os nós do seu cluster Hadoop on-premises, você será automaticamente direcionado para o endpoint correto da interface.

Este guia fornece instruções de uso DistCp para migrar dados para a nuvem da AWS. DistCp é a ferramenta mais usada, mas outras ferramentas de migração estão disponíveis. Por exemplo, você pode usar ferramentas off-line da AWS, como AWS Snowball ou AWS Snowmobile, ou ferramentas online da AWS, como AWS Storage Gateway ou AWS. DataSync Além disso, você pode usar outras ferramentas de código aberto, como o NiFiApache.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa com uma conexão de rede privada entre seu datacenter on-premises e a Nuvem AWS
- Hadoop, instalado localmente com DistCp
- Um usuário do Hadoop com acesso aos dados de migração no Sistema de Arquivos Distribuído do Hadoop (HDFS)
- AWS Command Line Interface (AWS CLI), instalada e configurada
- Permissões para colocar objetos em um bucket do S3

Limitações

As limitações da nuvem privada virtual (VPC) se aplicam à AWS PrivateLink para o Amazon S3. Para obter mais informações, consulte Propriedades e limitações do endpoint da interface e PrivateLink cotas da AWS (PrivateLink documentação da AWS).

A AWS PrivateLink para Amazon S3 não oferece suporte ao seguinte:

- Endpoints do Federal Information Processing Standard (FIPS – Padrões Federais de Processamento de Informações)
- Endpoints de site
- Endpoints globais herdados

Arquitetura

Pilha de tecnologia de origem

- Cluster Hadoop com instalação DistCp

Pilha de tecnologias de destino

- Amazon S3
- Amazon VPC

Arquitetura de destino

O diagrama mostra como o administrador do Hadoop usa DistCp para copiar dados de um ambiente local por meio de uma conexão de rede privada, como o AWS Direct Connect, para o Amazon S3 por meio de um endpoint de interface do Amazon S3.

Ferramentas

Serviços da AWS

- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- O Apache Hadoop DistCp (cópia distribuída) é uma ferramenta usada para copiar grandes interclusters e intra-clusters. DistCp usa o Apache MapReduce para distribuição, tratamento e recuperação de erros e geração de relatórios.

Épicos

Migre dados para a Nuvem AWS

Tarefa	Descrição	Habilidades necessárias
Crie um endpoint para a AWS PrivateLink para o Amazon S3.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. 2. No painel de navegação, selecione Endpoints e Criar endpoint. 3. Para Service category (Categoria de serviço), escolha AWS Services (Serviços da AWS). 4. Na caixa de pesquisa, digite s3 e pressione Enter. 5. Nos resultados da pesquisa, escolha com.amazonaws. < your-aws-region >.s3 nome do serviço em que o valor na coluna Tipo é Interface.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	6. Em VPC, escolha sua VPC. Em Sub-redes, escolha sua sub-rede. 7. Para Grupo de segurança , escolha ou crie um grupo de segurança que permite TCP 443. 8. Adicione tags com base em seus requisitos e escolha Criar endpoint.	
Verifique os endpoints e encontre as entradas de DNS.	1. Abra o console do Amazon VPC, escolha Endpoints e selecione o endpoint que você criou anteriormente. 2. Na guia Detalhes, encontre a primeira entrada de DNS para nomes DNS. Essa é a entrada do DNS regional. Quando você usa esse nome de DNS, as solicitaç ões alternam entre as entradas de DNS específic as das Zonas de Disponibi lidade. 3. Escolha a guia Sub-redes . Você pode encontrar o endereço da interface de rede elástica do endpoint em cada zona de disponibi lidade.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Verifique as regras do firewall e as configurações de roteamento.	Para confirmar se suas regras de firewall estão abertas e se sua configuração de rede está configurada corretamente, use o Telnet para testar o endpoint na porta 443. Por exemplo:
	`$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443`
	`Trying 10.104.88.6...`
	`Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.`
	`...`
	`$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443`
	`Trying 10.104.71.141...`
	`Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.`
	Note
	Se você usar a entrada Regional, um teste bem-sucedido
		Administrador de rede, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	mostra que o DNS está alternando entre os dois endereços IP que você pode ver na guia Sub-redes do seu endpoint selecionado no console da Amazon VPC.	

Tarefa	Descrição	Habilidades necessárias
Configure a resolução de nomes.	Você deve configurar a resolução de nomes para permitir que o Hadoop acesse o endpoint da interface Amazon S3. Não é possível usar o nome do endpoint em si. Em vez disso, você deve resolver `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com` ou `*.s3.<your-aws-region>.amazonaws.com`. Para obter mais informações sobre essa limitação de nomenclatura, consulte Apresentando o cliente Hadoop S3A (site do Hadoop). Escolha uma das seguintes opções de configuração: • Use o DNS on-premises para resolver o endereço IP privado do endpoint. Você pode substituir o comportamento de todos os compartimentos ou dos compartimentos selecionados. Para obter mais informações, consulte “Opção 2: acessar o Amazon S3 usando zonas de política de resposta do sistema de nomes de domínio (DNS RPZ)” em	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Acesso híbrido seguro ao Amazon S3 usando a AWS (postagem no blog da PrivateLink AWS). • Configure o DNS on-premises para encaminhar condicionalmente o tráfego para os endpoints de entrada do resolvedor na VPC. O tráfego é encaminhado para a Route 53. Para obter mais informações, consulte "Opção 3: Encaminhar solicitações de DNS do local usando os endpoints de entrada do Amazon Route 53 Resolver" em Acesso híbrido seguro ao Amazon S3 usando a AWS (postagem no blog da AWS) PrivateLink. • Edite o arquivo /etc/hosts em todos os nós do seu cluster do Hadoop. Essa é uma solução temporária para testes e não é recomendada para produção. Para editar o arquivo /etc/hosts, adicione uma entrada para `<your-bucket-name>.s3.<your-aws-region>.amazo`	

Tarefa	Descrição	Habilidades necessárias
	`naws.com` ou `s3.<your-aws-region>.amazonaws.com` . O arquivo /etc/hosts não pode ter vários endereços IP para uma entrada. Você deve escolher um único endereço IP de uma das zonas de disponibilidade, que então se torna um único ponto de falha.	

Tarefa	Descrição	Habilidades necessárias
Configure a autenticação para o Amazon S3.	Para se autenticar no Amazon S3 por meio do Hadoop, recomendamos que você exporte credenciais de função temporárias para o ambiente do Hadoop. Para obter mais informações, consulte Autenticação com o S3 (site do Hadoop). Para trabalhos de longa duração, você pode criar um usuário e atribuir uma política que tenha permissões para colocar dados somente em um bucket do S3. A chave de acesso e a chave secreta podem ser armazenadas no Hadoop, acessíveis somente para o DistCp trabalho em si e para o administrador do Hadoop. Para obter mais informações sobre como armazenar segredos, consulte Armazenamento de segredos com provedores de credenciais do Hadoop (site do Hadoop). Para obter mais informações sobre outros métodos de autenticação, consulte Como obter credenciais de um perfil do IAM para uso com acesso da CLI a uma conta da AWS IAM na documentação do Centro de Identidade do AWS IAM	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	(sucessor do AWS Single Sign-On).
	
	Para usar credenciais temporárias, adicione as credenciais temporárias ao seu arquivo de credencia is ou execute os seguintes comandos para exportar as credenciais para o seu ambiente:
	
	`export AWS_SESSI ON_TOKEN=SECRET-SE SSION-TOKEN`
	`export AWS_ACCES S_KEY_ID=SESSION-A CCESS-KEY`
	`export AWS_SECRE T_ACCESS_KEY=SESSION- SECRET-KEY`
	
	Se você tiver uma combinaçã o tradicional de chave de acesso e chave secreta, execute os seguintes comandos:
	
	`export AWS_ACCES S_KEY_ID=my.aws.key`
	`export AWS_SECRE T_ACCESS_KEY=my.se cret.key`	

Tarefa	Descrição	Habilidades necessárias
	Note Se você usar uma combinação de chave de acesso e chave secreta, altere o provedor de credenciais nos DistCp comandos de `"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider"` para `"org.apache.hadoop.fs.s3a.SimpleAWSCredentialsProvider"` .	

Tarefa	Descrição	Habilidades necessárias
Transfira dados usando DistCp.	Para usar DistCp para transferir dados, execute os seguintes comandos: `hadoop distcp -Dfs.s3a.aws.credentials.provider=\"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider" \ -Dfs.s3a.access.key="${AWS_ACCESS_KEY_ID}" \ -Dfs.s3a.secret.key="${AWS_SECRET_ACCESS_KEY}" \ -Dfs.s3a.session.token="${AWS_SESSION_TOKEN}" \ -Dfs.s3a.path.style.access=true \ -Dfs.s3a.connection.ssl.enabled=true \ -Dfs.s3a.endpoint=s3.<your-aws-region>.amazonaws.com \ hdfs:///user/root/ s3a://<your-bucket-name>` **Note** A região da AWS do endpoint não é descoberta automaticamente quando você usa o DistCp comando	Engenheiro de migração, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	com a AWS PrivateLink para o Amazon S3. O Hadoop 3.3.2 e versões posteriores resolvem esse problema habilitando a opção de definir explicitamente a região da AWS do bucket S3. Para obter mais informações, consulte S3A para adicionar a opção fs.s3a.endpoint.region para definir a região da AWS (site do Hadoop). Para obter mais informações sobre provedores S3A adicionais, consulte Configuração geral do cliente S3A (site do Hadoop). Por exemplo, se você usa criptografia, pode adicionar a seguinte opção à série de comandos acima, dependendo do seu tipo de criptografia: `-Dfs.s3a.server-side-encryption-algorithm=AES-256 [or SSE-C or SSE-KMS]`	

Tarefa	Descrição	Habilidades necessárias
	Note Para usar o endpoint da interface com o S3A, você deve criar uma entrada de alias de DNS para o nome regional do S3 (por exemplo, `s3.<your-aws-region>.amazonaws.com`) no endpoint da interface. Consulte a seção Configurar autenticação para o Amazon S3 para obter instruções. Essa solução alternativa é necessária para o Hadoop 3.3.2 e versões anteriores. Versões futuras do S3A não exigirão essa solução alternativa. Se você tiver problemas de assinatura com o Amazon S3, adicione uma opção de usar a Signature Version 4 (SigV4): `-Dmapreduce.map.java.opts="-Dcom.amazonaws.services.s3.enableV4=true"`	

Mais padrões

- Acesse Serviços da AWS a partir do IBM z/OS instalando o AWS CLI
- Automatize backups orientados por eventos para o Amazon CodeCommit S3 usando e Eventos CodeBuild CloudWatch
- Arquivar automaticamente itens no Amazon S3 usando o DynamoDB TTL
- Faça backup automático dos bancos de dados SAP HANA usando o Systems Manager e EventBridge
- Faça backup e arquive dados de mainframe no Amazon S3 usando o BMC AMI Cloud Data
- Criar um pipeline de serviços de ETL para carregar dados incrementalmente do Amazon S3 ao Amazon Redshift usando o AWS Glue
- Configure o registro de invocação de modelo no Amazon Bedrock usando AWS CloudFormation
- Converta e descompacte dados EBCDIC em ASCII na AWS usando Python
- Converter VARCHAR2 (1) tipo de dados para Oracle para tipo de dados booleano para Amazon Aurora PostgreSQL
- Crie uma definição de tarefa do Amazon ECS e monte um sistema de arquivos em EC2 instâncias usando o Amazon EFS
- Entregue registros do DynamoDB para o Amazon S3 usando o Kinesis Data Streams e o Firehose com AWS CDK
- Implemente um sistema de arquivos Lustre para processamento de dados de alto desempenho usando o Terraform e o DRA
- Estime os custos de armazenamento de uma tabela do Amazon DynamoDB
- Identifique buckets públicos do Amazon S3 usando o Security AWS Organizations Hub
- Migre instâncias do banco de dados Amazon RDS para Oracle para outras contas que usam AMS
- Migrar um servidor SFTP local para usar AWSAWS Transfer for SFTP
- Migre uma tabela particionada do Oracle para o PostgreSQL usando o AWS DMS
- Migre dados do Microsoft Azure Blob para o Amazon S3 usando o Rclone
- Migrar valores do Oracle CLOB para linhas individuais no PostgreSQL na AWS
- Migrar sistemas de arquivos compartilhados em uma grande migração da AWS
- Migre pequenos conjuntos de dados on-premises para o Amazon S3 usando o AWS SFTP
- Monitore o Amazon Aurora em busca de instâncias sem criptografia
- Mova arquivos de mainframe diretamente para o Amazon S3 usando o Transfer Family

- Remova EC2 as entradas da Amazon na mesma forma Conta da AWSAWS Managed Microsoft AD usando a AWS Lambda automação
- Executar workloads monitoradas com armazenamento de dados persistente usando o Amazon EFS no Amazon EKS com o AWS Fargate
- Importe com sucesso um bucket do S3 como uma pilha da AWS CloudFormation
- Sincronize dados entre sistemas de arquivos Amazon EFS em diferentes regiões da AWS usando a AWS DataSync
- Ver os detalhes do snapshot do EBS para sua conta ou organização da AWS

Ferramentas de desenvolvedor

Tópicos

- DevOps
- Infraestrutura
- Aplicativos para web e dispositivos móveis

DevOps

Tópicos

- Automatize as operações de AWS infraestrutura usando o Amazon Bedrock
- Automatize CloudFront as atualizações quando os endpoints do balanceador de carga mudarem usando o Terraform
- Automatize as CodeGuru avaliações da Amazon para aplicativos AWS CDK Python usando Actions GitHub
- Automatize a avaliação de recursos da AWS
- Instale sistemas SAP automaticamente usando ferramentas de código aberto
- Automatize o portfólio e a implantação de produtos do AWS Service Catalog usando o AWS CDK
- Automatize backups orientados por eventos para o Amazon CodeCommit S3 usando e Eventos CodeBuild CloudWatch
- Automatize a exclusão de AWS CloudFormation pilhas e recursos associados
- Automatize o gerenciamento dinâmico de pipelines para implantar soluções de hotfix em ambientes Gitflow usando e AWS Service CatalogAWS CodePipeline
- Automatize a ingestão e a visualização de métricas personalizadas do Amazon MWAA no Amazon Managed Grafana usando o Terraform
- Simplifique o desenvolvimento e a implantação de bots do Amazon Lex usando um fluxo de trabalho automatizado
- Automatize a implantação de conjuntos de pilhas usando a AWS e a AWS CodePipeline CodeBuild
- Anexe automaticamente uma política gerenciada da AWS para Systems Manager aos perfis de EC2 instância usando o Cloud Custodian e o AWS CDK
- Compile automaticamente pipelines de CI/CD e clusters do Amazon ECS para microsserviços usando o AWS CDK
- Crie uma arquitetura pouco acoplada com microsserviços usando DevOps práticas e o AWS Cloud9
- Crie e envie imagens do Docker para o Amazon ECR usando GitHub Actions e Terraform
- Crie e teste aplicativos iOS com AWS CodeCommit CodePipeline, AWS e AWS Device Farm
- Verifique os aplicativos ou CloudFormation modelos do AWS CDK para obter as melhores práticas usando pacotes de regras cdk-nag
- Configurar a autenticação de TLS mútuo para aplicativos em execução no Amazon EKS

- Automatize a criação de recursos AppStream 2.0 usando a AWS CloudFormation
- Crie um analisador de log personalizado para o Amazon ECS usando um roteador de log Firelens
- Crie um pipeline e uma AMI usando CodePipeline um HashiCorp Packer
- Crie um pipeline e implante atualizações de artefatos em instâncias locais usando EC2 CodePipeline
- Criar pipelines dinâmicos de CI para projetos Java e Python automaticamente
- Implante canários CloudWatch Synthetics usando o Terraform
- Implementar um pipeline de CI/CD para microsserviços Java no Amazon ECS
- Implemente uma ChatOps solução para gerenciar os resultados do escaneamento SAST usando o Amazon Q Developer em aplicativos de bate-papo, ações personalizadas e AWS CloudFormation
- Implante um firewall usando o AWS Network Firewall e o AWS Transit Gateway
- Implante um trabalho do AWS Glue com um pipeline de CodePipeline CI/CD da AWS
- Implante um cluster Amazon EKS a partir do AWS Cloud9 usando um perfil de instância EC2
- Implante código em várias regiões da AWS usando AWS CodePipeline CodeCommit, AWS e AWS CodeBuild
- Execute consultas SQL do Amazon Redshift usando o Terraform
- Exporte relatórios do AWS Backup de toda a organização no AWS Organizations como um arquivo CSV
- Exportar tags de uma lista de EC2 instâncias da Amazon para um arquivo CSV
- Gere um CloudFormation modelo da AWS contendo regras gerenciadas do AWS Config usando o Troposphere
- Conceda às instâncias do SageMaker notebook acesso temporário a um CodeCommit repositório em outra conta da AWS
- Implemente uma estratégia GitHub de ramificação do Flow para ambientes com várias contas DevOps
- Implemente uma estratégia de ramificação do Gitflow para ambientes com várias contas DevOps
- Implemente uma estratégia de ramificação de troncos para ambientes com várias contas DevOps
- Implemente o escaneamento Checkov personalizado e centralizado para aplicar a política antes de implantar a infraestrutura AWS
- Detecte alterações automaticamente e inicie diferentes CodePipeline pipelines para um monorepo em CodeCommit
- Integre um repositório Bitbucket com o AWS Amplify usando a AWS CloudFormation

- Lance um CodeBuild projeto em várias contas da AWS usando Step Functions e uma função de proxy Lambda
- Gerencie o failover Multi-AZ para clusters do EMR usando o Application Recovery Controller
- Gerencie implantações azul/verdes de microsserviços em várias contas e regiões usando os serviços de código da AWS e as chaves multirregionais do AWS KMS
- Monitore os repositórios do Amazon ECR para obter permissões curinga usando o AWS e o AWS Config CloudFormation
- Otimize implantações sem servidor de várias contas usando os fluxos de trabalho e Actions AWS CDK GitHub
- Execute ações personalizadas a partir de CodeCommit eventos da AWS
- Provisione AWS Service Catalog produtos com base em AWS CloudFormation modelos usando GitHub Ações
- Provisione funções do IAM com privilégios mínimos implantando uma solução de máquina de venda automática de funções
- Publique CloudWatch métricas da Amazon em um arquivo CSV
- Remova EC2 as entradas Contas da AWS da Amazon em frente AWS Managed Microsoft AD usando a AWS Lambda automação
- Remova EC2 as entradas da Amazon na mesma forma Conta da AWSAWS Managed Microsoft AD usando a AWS Lambda automação
- Execute testes de unidade para trabalhos de ETL do Python AWS Glue usando a estrutura pytest
- Configurar um repositório de chart do Helm v3 no Amazon S3
- Configure um pipeline de CI/CD usando a AWS e o CodePipeline AWS CDK
- Configure o registro centralizado em escala corporativa usando o Terraform
- Configure a end-to-end criptografia para aplicativos no Amazon EKS usando cert-manager e Let's Encrypt
- Simplifique a implantação de aplicativos multilocatários do Amazon EKS usando o Flux
- Assinar vários endpoints de e-mail em um tópico do SNS usando um recurso personalizado
- Coordene a dependência de recursos e a execução de tarefas usando a AWS Fargate WaitCondition construção de gancho
- Use repositórios de origem Git de terceiros na AWS CodePipeline
- Crie um pipeline de CI/CD para validar as configurações do Terraform usando a AWS CodePipeline

- Mais padrões

Automatize as operações de AWS infraestrutura usando o Amazon Bedrock

Criado por Ishwar Chauthaiwale (AWS) e Anand Bukkapatnam Tirumala (AWS)

Resumo

Em soluções nativas em nuvem, a automação de operações comuns de infraestrutura desempenha um papel vital na manutenção de ambientes eficientes, seguros e econômicos. O manuseio manual das operações é demorado e propenso a erros humanos. Além disso, membros da equipe com diferentes níveis de AWS especialização precisam realizar essas tarefas e, ao mesmo tempo, garantir a conformidade com os protocolos de segurança. Esse padrão demonstra como usar o Amazon Bedrock para automatizar operações comuns de AWS infraestrutura por meio do processamento de linguagem natural (NLP).

Esse padrão pode ajudar as organizações a desenvolver código reutilizável, modular e seguro para implantar uma infraestrutura generativa baseada em IA em vários ambientes. Por meio de seu foco na infraestrutura como código (IaC) e na automação, ela oferece DevOps os principais benefícios, incluindo controle de versão, implantações consistentes, redução de erros, provisionamento mais rápido e colaboração aprimorada.

O padrão implementa uma arquitetura segura que permite que as equipes gerenciem operações relacionadas à chave Serviços da AWS , incluindo:

- Gerenciamento de versão de buckets do Amazon Simple Storage Service (Amazon S3)
- Criação de snapshot do Amazon Relational Database Service (Amazon RDS)
- Gerenciamento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2)

A arquitetura emprega endpoints e redes privadas da Amazon Virtual Private Cloud (Amazon VPC) para comunicação segura, AWS Lambda com funções operando como executores de tarefas em sub-redes privadas. O Amazon S3 fornece gerenciamento de dados e implementa funções e permissões abrangentes AWS Identity and Access Management (IAM) para garantir controles de acesso adequados. Essa solução não inclui um recurso de histórico de bate-papo e o bate-papo não é armazenado.

Pré-requisitos e limitações

- Um ativo Conta da AWS.

- Medidas adequadas de controle de acesso devem estar em vigor para ajudar a proteger e controlar o acesso. Exemplos de controle de acesso incluem o uso de acesso a modelos básicos AWS Systems Manager, uma função do IAM para implantação e funções baseadas em serviços, a desativação do acesso público aos buckets do Amazon S3 e a configuração de uma fila de mensagens mortas.
- Uma chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente.
- AWS Command Line Interface (AWS CLI) versão 2 ou posterior, instalada e configurada no ambiente de implantação.
- Terraform AWS Provider versão 4 ou posterior instalado e configurado.
- Terraform versão 1.5.7 ou posterior instalado e configurado.
- Analise e defina esquemas de OpenAPI para os grupos de ação do seu agente no Amazon Bedrock para ajudar a proteger contra acesso não autorizado e manter a integridade dos dados.
- Acesso habilitado em seu Conta da AWS para os modelos Amazon Titan Text Embeddings v2 necessários e para os modelos Claude 3.5 Sonnet ou Claude 3 Haiku Foundation. Para evitar falhas na implantação, confirme se a implantação de destino é Região da AWS compatível com os modelos necessários.
- Uma nuvem privada virtual (VPC) configurada que segue as melhores práticas do AWS Well Architected Framework.
- Revisão concluída da política de IA responsável da Amazon.

Versões do produto

- Incorporações de texto Amazon Titan v2
- Soneto Antrópico Claude 3.5 ou Claude 3 Haiku
- Terraform AWS Provider versão 4 ou posterior
- Terraform versão 1.5.7 ou posterior

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

A arquitetura da solução consiste em várias camadas que trabalham juntas para processar solicitações de linguagem natural e executar AWS as operações correspondentes:

1. O usuário faz solicitações de operações por meio do console de bate-papo do Amazon Bedrock.
2. O chatbot usa as bases de conhecimento Amazon Bedrock para processamento de solicitações. Ele implementa o modelo Amazon Titan Text Embeddings v2 para processamento de linguagem natural.
3. Se o prompt do usuário incluir uma solicitação de ação, o grupo de ação Amazon Bedrock usa o modelo Anthropic Claude 3 Haiku ou o modelo Claude 3.5 Sonnet (dependendo da sua escolha) para a lógica de execução e define as operações por meio de um esquema OpenAPI.
4. O grupo de ação alcança os endpoints da Amazon VPC usando AWS PrivateLink para comunicação segura de serviços.
5. A AWS Lambda função é alcançada por meio de endpoints Amazon VPC para serviços Amazon Bedrock.
6. As funções Lambda são o principal mecanismo de execução. Com base na solicitação, a função Lambda chama a API para realizar ações no. Serviços da AWS A função Lambda também gerencia o roteamento e a execução da operação.
7. A solicitação Serviços da AWS get the API da função Lambda e as operações correspondentes são executadas.
8. A função Lambda calcula uma carga de saída que é compreendida pelo Amazon Bedrock.
9. Essa carga é enviada para o Amazon Bedrock usando uma comunicação segura PrivateLink de serviços. O modelo de linguagem grande (LLM) usado pelo Amazon Bedrock compreende essa carga útil e a converte em um formato compreensível para humanos.
10. Em seguida, a saída é mostrada ao usuário no console de bate-papo do Amazon Bedrock.

A solução permite as seguintes operações primárias:

- Amazon S3 — Habilite o controle de versão do bucket para controle de versão.
- Amazon RDS — Crie instantâneos de banco de dados para backup.
- Amazon EC2 — Liste as instâncias e controle o início e a parada das instâncias.

Ferramentas

Serviços da AWS

- O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada.

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon OpenSearch Serverless é uma configuração sem servidor sob demanda para o Amazon Service. OpenSearch
- AWS PrivateLinkajuda você a criar conexões unidirecionais e privadas de suas nuvens privadas virtuais (VPCs) para serviços fora da VPC.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional no. Nuvem AWS
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- O Git é um sistema de controle de versão distribuído e de código aberto.
- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Repositório de código

O código desse padrão está disponível no repositório GitHub infra-ops-orchestratoraws-samples/.

Práticas recomendadas

- Monitore os registros de execução do Lambda regularmente. Para obter mais informações, consulte Monitorar e solucionar problemas de funções do Lambda. Para obter mais informações sobre as melhores práticas, consulte Práticas recomendadas para trabalhar com AWS Lambda funções.
- Revise as configurações de segurança periodicamente para garantir a conformidade com os requisitos da sua organização. Para obter mais informações, consulte Práticas recomendadas de segurança.
- Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Implante a solução

Tarefa	Descrição	Habilidades necessárias

Clonar o repositório.	Para clonar o repositório em sua máquina local, execute o seguinte comando:
	`git clone "git@github.com:aws-samples/infra-ops-orchestrator.git"`
	`cd infra-ops-orchestrator`
		AWS DevOps, DevOps engenheiro

Edite as variáveis de ambiente.	Edite o `terraform.tfvars` arquivo. no diretório raiz do repositório clonado. Revise os espaços reservados indicados	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	por `[XXXXX]` e atualize-os de acordo com seu ambiente.	

Crie a infraestrutura.	Para criar a infraestrutura, execute os seguintes comandos:
	`terraform init`
	`terraform plan`
	Revise o plano de execução com cuidado. Se as alteraçõe s planejadas forem aceitáveis, execute o seguinte comando:
	`terraform apply --auto-approve`
		AWS DevOps, DevOps engenheiro

Acesse a solução

Tarefa	Descrição	Habilidades necessárias
Acesse a solução.	Após a implantação bem-sucedida, siga estas etapas para usar a interface baseada em bate-papo: 1. Para acessar o Infrastru cture Orchestrator Assistant , faça login na função AWS Management Console usando uma [função do IAM com as permissõe	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	s do Amazon Bedrock e abra o console do Amazon Bedrock em. https://console.aws.amazon.com/bedrock/ No painel de navegação à esquerda, selecione Agentes. Em seguida, escolha o Infrastructure Orchestrator Assistant na seção Agentes. 2. Verifique se os recursos de destino existem em seu AWS ambiente para obter as sugestões a seguir e, em seguida, tente estes exemplos de operações: • Crie um backup instantâneo de uma instância do Amazon RDS perguntando: 'Crie um instantâneo da instância do RDS [nome da instância] ' • Ative o controle de versão em um bucket do Amazon S3 perguntando: “Habilitar o versionamento para o bucket [nome do bucket]” • Liste EC2 as instâncias da Amazon perguntando: “Listar todas as EC2 instâncias” • Inicie ou interrompa uma EC2 instância da Amazon	

Tarefa	Descrição	Habilidades necessárias
	perguntando: 'Start EC2 instance [instance-id] 'ou 'Stop EC2 instance [instance-id]' Observação: substitua os valores entre colchetes pelos nomes reais dos recursos ou IDs do seu AWS ambiente.	

Limpar recursos

Tarefa	Descrição	Habilidades necessárias

Exclua os recursos criados.	Para excluir toda a infraestr utura criada por esse padrão, execute o seguinte comando:
	
	`terraform plan -destroy`
	
	Revise o plano de destruição com cuidado. Se as exclusões planejadas forem aceitáveis, execute o seguinte comando:
	
	`terraform destroy`
	
	Nota: Esse comando excluirá permanentemente todos os recursos criados por esse padrão. O comando solicitar á a confirmação antes de remover qualquer recurso.
		AWS DevOps, DevOps engenheiro

Solução de problemas

Problema	Solução
Comportamento do agente	Para obter informações sobre esse problema, consulte Testar e solucionar problemas de comportamento do agente na documentação do Amazon Bedrock.
Problemas de rede Lambda	Para obter informações sobre esses problemas , consulte Solucionar problemas de rede no Lambda na documentação do Lambda.
permissões do IAM	Para obter informações sobre esses problemas , consulte Solucionar problemas do IAM na documentação do IAM.

Recursos relacionados

- Criação de um DB snapshot para uma instância de banco de dados Single-AZ para o Amazon RDS
- Defina esquemas de OpenAPI para os grupos de ação do seu agente no Amazon Bedrock
- Ativando o controle de versão em buckets
- Como o Amazon Bedrock Agents funciona
- Recupere dados e gere respostas de IA com as bases de conhecimento Amazon Bedrock
- Acesse com segurança os serviços em AWS PrivateLink
- Pare e inicie EC2 instâncias da Amazon
- Use grupos de ação para definir ações para seu agente realizar

Automatize CloudFront as atualizações quando os endpoints do balanceador de carga mudarem usando o Terraform

Criado por Tamilselvan P (AWS), Mohan Annam (AWS) e Naveen Suthar (AWS)

Resumo

Quando os usuários do Amazon Elastic Kubernetes Service (Amazon EKS) excluem e reinstalam sua configuração de entrada por meio de gráficos do Helm, um novo Application Load Balancer (ALB) é criado. Isso cria um problema porque CloudFront a Amazon continua referenciando o antigo registro DNS do ALB. Como resultado, os serviços destinados a esse endpoint não estarão acessíveis. (Para obter mais detalhes sobre esse fluxo de trabalho problemático, consulte Informações adicionais.)

Para resolver esse problema, esse padrão descreve o uso de uma AWS Lambda função personalizada desenvolvida com Python. Essa função Lambda detecta automaticamente quando um novo ALB é criado por meio das regras da Amazon. EventBridge Usando o AWS SDK para Python (Boto3), a função então atualiza a CloudFront configuração com o novo endereço DNS do ALB, garantindo que o tráfego seja roteado para o endpoint correto.

Essa solução automatizada mantém a continuidade do serviço sem roteamento ou latência adicionais. O processo ajuda a garantir que CloudFront sempre faça referência ao endpoint DNS correto do ALB, mesmo quando a infraestrutura subjacente muda.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Um exemplo de aplicativo web para teste e validação que é implantado no Amazon EKS usando o Helm. Para obter mais informações, consulte Implantar aplicativos com o Helm no Amazon EKS na documentação do Amazon EKS.
- Configure CloudFront para rotear chamadas para um ALB criado por um controlador de entrada do Helm. Para obter mais informações, consulte Instalar o controlador AWS Load Balancer com o Helm na documentação do Amazon EKS e Restringir o acesso aos Application Load Balancers na documentação. CloudFront
- Terraform instalado e configurado em um espaço de trabalho local.

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- Terraform versão 1.0.0 ou posterior
- Terraform AWS Provider versão 4.20 ou posterior

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

Essa solução executa as seguintes etapas:

1. O controlador de entrada do Amazon EKS cria um novo Application Load Balancer (ALB) sempre que há uma reinicialização ou implantação do Helm.
2. EventBridge procura eventos de criação de ALB.
3. O evento de criação do ALB aciona a função Lambda.
4. A função Lambda foi implantada com base no python 3.9 e usa a API boto3 para fazer chamadas. Serviços da AWS A função Lambda atualiza a CloudFront entrada com o nome DNS mais recente do balanceador de carga, que é recebido dos eventos de criação do balanceador de carga.

Ferramentas

Serviços da AWS

- A Amazon CloudFront acelera a distribuição do seu conteúdo da web entregando-o por meio de uma rede mundial de data centers, o que reduz a latência e melhora o desempenho.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS

- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS

Outras ferramentas

- Python é uma linguagem de programação de computador de uso geral.
- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Repositório de código

O código desse padrão está disponível no repositório GitHub aws-cloudfront-automation-terraform-samples.

Épicos

Configurar estação de trabalho local

Tarefa	Descrição	Habilidades necessárias
Configure e configure a CLI do Git.	Para instalar e configurar a interface de linha de comando (CLI) do Git em sua estação de trabalho local, siga as instruções de Introdução — Instalação do Git na documentação do Git.	DevOps engenheiro
Crie a pasta do projeto e adicione os arquivos.	1. Vá até o GitHub repositório do padrão e escolha o botão Código. 2. Na caixa de diálogo Clonar, escolha a guia HTTPS. Em	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Clonar usando o URL da web, copie o URL exibido. 3. Crie uma pasta na sua máquina local. Nomeie com o nome do seu projeto. 4. Abra um terminal em sua máquina local e navegue até essa pasta. 5. Para clonar o repositório git desse padrão, execute o seguinte comando: `git clone https://github.com/aws-samples/aws-cloudfront-automation-terraform-samples` 6. Depois que o repositório for clonado, use o comando a seguir para acessar o diretório clonado: `cd <directory name>/cloudfront-update` Abra este projeto em um Ambiente de Desenvolvimento Integrado (IDE) de sua escolha.	

Provisione a arquitetura de destino usando a configuração do Terraform

Tarefa	Descrição	Habilidades necessárias

Implante a solução.	Para implantar recursos no destino Conta da AWS, use as seguintes etapas:
	1. Acesse a pasta `cloudfront-update` .
	2. Atualize o `terraform.tfvars` arquivo com `cloudfront_distribution_id` o.
	3. Para definir o Região da AWS para o seu AWS perfil, execute o seguinte comando:
	`export AWS_REGION={{ REGION }}`
	4. Para inicializar o Terraform , execute o seguinte comando:
	`terraform init`
	5. Para validar o Terraform , execute o seguinte comando:
	`terraform validate`
	6. Para criar um plano de execução do Terraform , execute o seguinte comando:
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`terraform plan`
	7. Para aplicar as ações `deterraform plan`, execute o seguinte comando:
	`terraform apply`	

Verificar a implantação

Tarefa	Descrição	Habilidades necessárias
Valide a implantação.	1. Faça login no AWS Management Console e abra o CloudFront console da Amazon em https://console.aws.amazon.com/cloudfront/v4/home. 2. No painel de navegação esquerdo, escolha Distribuições e abra a CloudFront distribuição. 3. Na guia Origens, verifique se o nome da origem e o mapeamento de origem têm o registro DNS do ALB atualizado.	DevOps engenheiro

Limpe a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Limpe a infraestrutura.	Para limpar a infraestrutura que você criou anteriormente, use as seguintes etapas: 1. Execute o seguinte comando: `terraform destroy` 2. Para confirmar o comando destroy, digite `yes`.	DevOps engenheiro

Solução de problemas

Problema	Solução
Erro ao validar as credenciais do provedor	Ao executar o Terraform `apply` ou `destroy` os comandos da sua máquina local, você pode encontrar um erro semelhante ao seguinte: `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Esse erro é causado pela expiração do token de segurança das credenciais usadas na configuração da sua máquina local.

Problema	Solução
	Para resolver o erro, consulte Definir e visualizar as configurações na documentação AWS Command Line Interface (AWS CLI).

Recursos relacionados

AWS recursos

- Restrinja o acesso aos Application Load Balancers
- Roteie o tráfego da Internet com o AWS Load Balancer Controller

Documentação do Terraform

- AWS Provedor
- Instalar o Terraform
- Estado remoto

Mais informações

Fluxo de trabalho problemático

O diagrama mostra o seguinte fluxo de trabalho:

1. Quando o usuário acessa o aplicativo, a chamada vai para CloudFront.
2. CloudFront encaminha as chamadas para o respectivo Application Load Balancer (ALB).
3. O ALB inclui os endereços IP de destino, que são os endereços IP do pod do aplicativo. A partir daí, o ALB fornece os resultados esperados para o usuário.

No entanto, esse fluxo de trabalho demonstra um problema. As implantações de aplicativos estão acontecendo por meio de gráficos do Helm. Sempre que houver uma implantação ou se alguém reiniciar o Helm, a respectiva entrada também será recriada. Como resultado, o controlador externo do balanceador de carga recria o ALB. Além disso, durante cada recriação, o ALB é recriado com um nome DNS diferente. Por causa disso, CloudFront terá uma entrada obsoleta nas configurações

de origem. Por causa dessa entrada obsoleta, o aplicativo não estará acessível para o usuário. Esse problema resulta em tempo de inatividade para os usuários.

Solução alternativa

Outra solução possível é criar um DNS externo para o ALB e, em seguida, direcioná-lo para o endpoint de zona hospedada privada do Amazon Route 53. CloudFront No entanto, essa abordagem adiciona outro salto no fluxo do aplicativo, o que pode causar latência do aplicativo. A solução de função Lambda desse padrão não interrompe o fluxo de corrente.

Automatize as CodeGuru avaliações da Amazon para aplicativos AWS CDK Python usando Actions GitHub

Criado por Vanitha Dontireddy (AWS) e Sarat Chandra Pothula (AWS)

Resumo

Esse padrão mostra a integração das análises de código CodeGuru automatizadas da Amazon para aplicativos AWS Cloud Development Kit (AWS CDK) Python, GitHub orquestradas por meio de ações. A solução implanta uma arquitetura sem servidor definida em Python. AWS CDK Ao automatizar a análise de código especializada no pipeline de desenvolvimento, essa abordagem pode fazer o seguinte para projetos em Python AWS CDK :

- Melhore a qualidade do código.
- Simplifique os fluxos de trabalho.
- Maximize os benefícios da computação sem servidor.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Command Line Interface (AWS CLI) versão 2.9.11 ou posterior, instalada e configurada.
- Uma GitHub conta ativa e um GitHub repositório com permissões de fluxo de trabalho de leitura e gravação e criação de pull requests (PR) pela GitHub Actions para garantir que o fluxo de trabalho de PR funcione corretamente.
- Uma função do OpenID Connect (OIDC) em GitHub Ações para implantar a solução no. Conta da AWS Para criar a função, use a AWS CDK construção.

Limitações

- O Amazon CodeGuru Profiler oferece suporte a aplicativos escritos em todas as linguagens de máquina virtual Java (JVM) (como Scala e Kotlin) e tempos de execução e Python 3.6 ou posterior.
- O Amazon CodeGuru Reviewer oferece suporte a associações com repositórios de código Java e Python somente dos seguintes provedores de origem AWS CodeCommit: Bitbucket GitHub

GitHub , Enterprise Cloud e Enterprise Server. GitHub Além disso, os repositórios do Amazon Simple Storage Service (Amazon S3) só são suportados por meio de ações. GitHub

- Não há uma maneira automatizada de imprimir as descobertas durante o pipeline de integração contínua e implantação contínua (CI/CD). Em vez disso, esse padrão usa GitHub Ações como um método alternativo para manipular e exibir as descobertas.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte os serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra a arquitetura dessa solução.

Conforme mostrado no diagrama, quando um desenvolvedor cria uma pull request (PR) para análise, o GitHub Actions aciona as seguintes etapas:

1. Suposição da função do IAM — O pipeline usa a função do IAM especificada em GitHub Segredos para realizar tarefas de implantação.
2. Análise de código
   - CodeGuru O revisor analisa o código armazenado no bucket do Amazon S3. Ele identifica defeitos e fornece recomendações para correções e otimizações.
   - CodeGuru Verificações de segurança em busca de violações e vulnerabilidades de políticas.
3. Revisão dos resultados
   - O pipeline imprime um link para o painel de descobertas na saída do console.
   - Se descobertas críticas forem detectadas, o pipeline falhará imediatamente.
   - Para constatações de severidade alta, normal ou baixa, o pipeline continua na próxima etapa.
4. Aprovação de PR
   - Um revisor deve aprovar manualmente o PR.
   - Se o PR for negado, o pipeline falhará e interromperá outras etapas de implantação.
5. Implantação do CDK — Após a aprovação do PR, o processo de implantação do CDK começa. Ele configura o seguinte Serviços da AWS e os recursos:
   - CodeGuru Perfilador
   - AWS Lambda função

- Fila do Amazon Simple Queue Service (Amazon SQS)

6. Geração de dados de perfil — Para gerar dados de perfil suficientes para CodeGuru o Profiler:
   - O pipeline invoca a função Lambda várias vezes enviando mensagens para a fila do Amazon SQS periodicamente.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- O CDK Toolkit é um kit de desenvolvimento em nuvem de linha de comando que ajuda você a interagir com seu AWS CDK aplicativo.
- O Amazon CodeGuru Profiler coleta dados de desempenho de tempo de execução de seus aplicativos ativos e fornece recomendações que podem ajudá-lo a ajustar o desempenho do seu aplicativo.
- O Amazon CodeGuru Reviewer usa análise de programas e aprendizado de máquina para detectar possíveis defeitos difíceis de serem encontrados pelos desenvolvedores. Em seguida, o CodeGuru Profiler oferece sugestões para melhorar seu código Java e Python.
- O Amazon CodeGuru Security é uma ferramenta estática de segurança de aplicativos que usa aprendizado de máquina para detectar violações e vulnerabilidades de políticas de segurança. Ele fornece sugestões para lidar com os riscos de segurança e gera métricas para que você possa acompanhar a postura de segurança de seus aplicativos.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- GitHub O Actions é uma plataforma de integração contínua e entrega contínua (CI/CD) totalmente integrada aos GitHub repositórios. Você pode usar o GitHub Actions para automatizar seu pipeline de criação, teste e implantação.

Repositório de código

O código desse padrão está disponível no repositório GitHub amazon-codeguru-suite-cdk-python.

Práticas recomendadas

- Siga as melhores práticas para desenvolver e implantar infraestrutura em nuvem com o. AWS CDK
- Siga as melhores práticas de segurança no IAM ao usar os fluxos Serviços da AWS de trabalho do GitHub Actions, incluindo:
  - Não armazene credenciais no código do seu repositório.
  - Assuma uma função do IAM para receber credenciais temporárias e use credenciais temporárias sempre que possível.
  - Conceda o menor privilégio à função do IAM usada nos fluxos de trabalho do GitHub Actions. Conceda somente as permissões necessárias para realizar as ações em seus fluxos de trabalho de GitHub ações.
  - Monitore a atividade da função do IAM usada nos fluxos de trabalho do GitHub Actions.
  - Alterne periodicamente todas as credenciais de longo prazo que você usa.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Configure as AWS credencia is.	Para exportar as variáveis que definem Conta da AWS e Região da AWS onde você está implantando a pilha, execute os seguintes comandos:	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	
	`export CDK_DEFAU LT_REGION=<AWS Region>`
	
	As AWS credenciais do AWS CDK são fornecidas por meio de variáveis de ambiente.	

Clonar o repositório.	Para clonar o repositório em sua máquina local, execute o seguinte comando: `git clone https://g ithub.com/aws-samp les/amazon-codeguru- suite-cdk-python.git`	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Instale o CDK Toolkit.	Para confirmar se o CDK Toolkit está instalado e verificar a versão, execute o seguinte comando:
	`cdk --version`
	Se a versão do CDK Toolkit for anterior à 2.27.0, digite o seguinte comando para atualizá-la para a versão 2.27.0:
	`npm install -g aws-cdk@2.27.0`
	Se o CDK Toolkit não estiver instalado, execute o seguinte comando para instalá-lo:
	`npm install -g aws-cdk@2.27.0 --force`
		AWS DevOps, DevOps engenheiro

Instale as dependências necessárias.	Para instalar as dependências necessárias do projeto, execute o seguinte comando:
	`python -m pip install --upgrade pip`
	`pip install -r requirements.txt`
		AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Inicialize o ambiente CDK.	Para inicializar um ambiente de CDK da AWS, execute os seguintes comandos:
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Depois de inicializar o ambiente com sucesso, a seguinte saída deve ser exibida:
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
		AWS DevOps, DevOps engenheiro

Implemente o aplicativo CDK

Tarefa	Descrição	Habilidades necessárias
Sintetize o aplicativo. AWS CDK	Para sintetizar um AWS CDK aplicativo, execute o seguinte comando: `cdk synth` Para obter mais informações sobre esse comando, consulte cdk synthesize na documentação. AWS CDK	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Implantar os recursos	Para implantar os recursos, execute o seguinte comando: `cdk deploy --require-approval never` **Note** A `--require-approval never` bandeira significa que o CDK aprovará e executará todas as alterações automaticamente. Isso inclui mudanças que o CDK normalmente sinalizaria como necessitando de revisão manual (como mudanças na política do IAM ou remoção de recursos). Certifique-se de que seu código CDK e seu pipeline de CI/CD estejam bem testados e seguros antes de usar a `--require-approval never` bandeira em ambientes de produção.	AWS DevOps, DevOps engenheiro

Crie GitHub segredos e token de acesso pessoal

Tarefa	Descrição	Habilidades necessárias
Crie os segredos necessários em GitHub.	Para permitir que os fluxos de trabalho do GitHub Actions acessem AWS recursos com segurança sem expor informações confidenciais no código do seu repositório, crie segredos. Para criar os segredos em GitHub for`ROLE_TO_ASSUME` ,, e `CodeGuruReviewArtifactBucketName` `AWS_ACCOUNT_ID` , siga as instruções em Criação de segredos para um repositório na documentação de GitHub Ações. Veja a seguir mais informações sobre as variáveis: • `AWS_ACCOUNT_ID` — O Conta da AWS ID em que o pipeline é executado. • `CodeGuruReviewArtifactBucketName` — O nome do bucket do S3 em que os artefatos do CodeGuru Reviewer são armazenados. Esse padrão usa o nome do bucket`codeguru-reviewer-build-art`	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`ifacts-<ACCOUNT_ID>-<REGION>` . • `AWS_REGION` — Região da AWS Onde os recursos estão localizados. • `ROLE_TO_ASSUME` — O nome da função do IAM que o pipeline assume. Esse padrão usa o nome da função`githubActionsDeployRole` .	
Crie um token de acesso GitHub pessoal.	Para configurar uma forma segura de autenticar e interagir com seus fluxos de trabalho do GitHub Actions GitHub, faça o seguinte: 1. Para criar um token de acesso GitHub pessoal que tenha acesso de leitura e gravação ao seu repositór io, siga as instruções em Gerenciando seus tokens de acesso pessoal na GitHub documentação. 2. Para salvar esse token como um segredo do repositório para GitHub Ações, siga as instruções em Criação de segredos para um repositório na documentação de GitHub Ações.	AWS DevOps, DevOps engenheiro

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpar os recursos	Para limpar seu aplicativo AWS CDK Python, execute o seguinte comando: `cdk destroy --all`	DevOps engenheiro

Solução de problemas

Problema	Solução
Exibir link para as descobertas do painel.	Não há como imprimir as descobertas durante o pipeline de CI/CD. Em vez disso, esse padrão usa GitHub Ações como um método alternativo para manipular e exibir as descobert as.

Recursos relacionados

AWS recursos

- AWS Kit de desenvolvimento em nuvem
- CodeGuru Documentação da Amazon
- Amazon S3
- AWS Identity and Access Management
- Amazon Simple Queue Service
- O que é AWS Lambda?

GitHub documentação

- Configurando o OpenID Connect na Amazon Web Services

- GitHub Ações
- Reutilização de fluxos de trabalho
- Acionando um fluxo de trabalho

Automatize a avaliação de recursos da AWS

Criado por Naveen Suthar (AWS), Arun Bagal (AWS), Manish Garg (AWS) e Sandeep Gawande (AWS)

Resumo

Esse padrão descreve uma abordagem automatizada para configurar recursos de avaliação de recursos usando o AWS Cloud Development Kit (AWS CDK). Ao usar esse padrão, as equipes de operações coletam detalhes de auditoria de recursos de forma automatizada e visualizam os detalhes de todos os recursos implantados em uma conta da AWS em um único painel. Isso é útil nos seguintes casos de uso:

- Identificação de ferramentas de infraestrutura como código (IaC) e isolamento de recursos criados por diferentes soluções de IaC, como HashiCorp Terraform, AWS CloudFormation, AWS CDK e AWS Command Line Interface (AWS CLI)
- Buscando informações de auditoria de recursos

Essa solução também ajudará a equipe de liderança a obter informações sobre os recursos e as atividades em uma conta da AWS a partir de um único painel.

> **Note**
>
> A Amazon QuickSight é um serviço pago. Antes de executá-lo para analisar dados e criar um painel, revise os QuickSight preços da Amazon.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Funções e permissões do AWS Identity and Access Management (IAM) com acesso a recursos de provisionamento
- Uma QuickSight conta da Amazon criada com acesso ao Amazon Simple Storage Service (Amazon S3) e ao Amazon Athena

- AWS CDK versão 2.55.1 ou superior instalado.
- Python versão 3.9 ou superior instalado.

Limitações

- Essa solução é implantada em uma única conta da AWS.
- A solução não rastreará os eventos que aconteceram antes de sua implantação, a menos que a AWS já CloudTrail estivesse configurada e armazenando dados em um bucket S3.

Versões do produto

- AWS CDK versão 2.55.1 ou superior
- Python, versão 3.9 ou superior.

Arquitetura

Pilha de tecnologias de destino

- Amazon Athena
- AWS CloudTrail
- AWS Glue
- AWS Lambda
- Amazon QuickSight
- Amazon S3

Arquitetura de destino

O código do AWS CDK implantará todos os recursos necessários para configurar recursos de avaliação de recursos em uma conta da AWS. O diagrama a seguir mostra o processo de envio de CloudTrail registros para o AWS Glue, Amazon Athena e. QuickSight

1. CloudTrail envia registros para um bucket do S3 para armazenamento.
2. Uma notificação de evento invoca uma função do Lambda que processa os registros e gera dados filtrados.

3. Os dados filtrados são armazenados em outro bucket do S3.
4. Um crawler do AWS Glue é configurado nos dados filtrados que estão no bucket do S3 para criar um esquema na tabela do catálogo de dados do AWS Glue.
5. Os dados filtrados estão prontos para serem consultados pelo Amazon Athena.
6. Os dados consultados são acessados por QuickSight para visualização.

Automação e escala

- Essa solução pode ser escalada de uma conta da AWS para várias contas da AWS se houver uma trilha para toda a organização no CloudTrail AWS Organizations. Ao implantar CloudTrail no nível organizacional, você também pode usar essa solução para obter detalhes de auditoria de recursos para todos os recursos necessários.
- Esse padrão usa recursos com tecnologia sem servidor da AWS para implantar a solução.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- CloudTrailA AWS ajuda você a auditar a governança, a conformidade e o risco operacional da sua conta da AWS.
- O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados. Esse padrão usa um crawler do AWS Glue e uma tabela do Catálogo de Dados do AWS Glue.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

- QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Repositório de código

O código desse padrão está disponível no GitHub infrastructure-assessment-iac-automationrepositório.

O repositório de código contém os seguintes arquivos e pastas:

- Pasta `lib`: o AWS CDK estrutura arquivos Python usados para criar recursos da AWS
- `src/lambda_code`: o código Python que é executado na função do Lambda
- `requirements.txt`: a lista de todas as dependências do Python que devem ser instaladas
- `cdk.json`: o arquivo de entrada para fornecer os valores necessários para gerar recursos

Práticas recomendadas

Configure o monitoramento e o alerta para a função do Lambda. Para obter mais informações, consulte Monitorar e solucionar problemas de funções do Lambda. Para obter as melhores práticas gerais ao trabalhar com funções do Lambda, consulte a documentação da AWS.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Clone o repositório na sua máquina local.	Para clonar o repositór io, execute o comando `git clone https://g ithub.com/aws-samp les/infrastructure -assessment-iac-au tomation.git .`	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Configurar o ambiente virtual Python e instalar as dependências necessárias.	Para ativar o ambiente virtual do Python, execute os comandos a seguir.
	`cd infrastructure-assessment-iac-automation`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Execute o comando `pip install -r requirements.txt` para configurar as dependências necessárias.
		AWS DevOps, DevOps engenheiro

Configure o ambiente do AWS CDK e sintetize o código do AWS CDK.	1. Para configurar o ambiente do AWS CDK em sua conta da AWS, execute o comando `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` . 2. Para converter o código em uma configuração de CloudFormation pilha da AWS, execute o comando`cdk synth`.	AWS DevOps, DevOps engenheiro

Configurar credenciais da AWS na sua máquina local

Tarefa	Descrição	Habilidades necessárias
Exporte variáveis para a conta e a região em que a pilha será implantada.	Para fornecer credencia is da AWS para o AWS CDK usando variáveis	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	de ambiente, execute os seguintes comandos. `export CDK_DEFAU LT_ACCOUNT=<12 Digit AWS Account Number> export CDK_DEFAU LT_REGION=<region>`	
Configurar o perfil da AWS CLI.	Para configurar o perfil da AWS CLI para a conta, siga as instruções na documentação da AWS.	AWS DevOps, DevOps engenheiro

Configurar e implantar a ferramenta de avaliação de recursos

Tarefa	Descrição	Habilidades necessárias
Implante recursos na conta.	Para implantar recursos na conta da AWS usando o AWS CDK, faça o seguinte: 1. Na raiz do repositór io clonado, no arquivo `cdk.json`, forneça entradas para os seguintes parâmetros: • `s3_context` • `ct_context` • `kms_context` • `lambda_context` • `glue_context` • `qs_context`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Esses valores definem as configurações e a nomenclatura dos recursos. Os valores padrão são definidos e podem ser alterados, se necessário. **Note** Para evitar um erro informando que o bucket do S3 já existe, certifique-se de fornecer nomes exclusivos para `s3_context` as `output` seções `ct` e. 2. Para implantar recursos, execute o comando `cdk deploy`. O `cdk deploy` comando cria um CloudTrail recurso para registrar eventos e salvar o arquivo de log no bucket do S3 de entrada. Os arquivos de log da trilha serão processados pela função do Lambda. Os resultados filtrados são armazenados no bucket S3 de saída e estão prontos para serem consumidos	

Tarefa	Descrição	Habilidades necessárias
	pelo Amazon Athena e pela Amazon. QuickSight	

Tarefa	Descrição	Habilidades necessárias
Execute o AWS Glue Crawler e crie a tabela do Data Catalog.	Um AWS Glue Crawler é usado para manter o esquema de dados dinâmico. A solução cria e atualiza partições na tabela do catálogo de dados do AWS Glue executando o rastreador periodicamente, conforme definido pelo programador do AWS Glue Crawler. Depois que os dados estiverem disponíveis no bucket S3 de saída, use as etapas a seguir para executar o crawler AWS Glue e criar o esquema da tabela do catálogo de dados para teste: 1. Faça login no Console de Gerenciamento da AWS e navegue para o console do AWS Glue. 2. No painel de navegação, em Catálogo de dados, escolha Crawlers. 3. Selecione o crawler `iac-tool-qa-resource-iac-json-crawler` . 4. Execute o crawler. 5. Depois que o crawler é executado com êxito, ele cria definições de tabela no Catálogo de Dados do AWS Glue. A AWS	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	QuickSight usará a tabela para visualizar os dados. **Note** O código do AWS CDK configura o crawler AWS Glue para ser executado em um determina do momento, mas você também pode executá-lo sob demanda.	
Implante a QuickSight construção.	1. Para implantar a QuickSigh t construção, descomente o código entre `#QuickSig ht setup - start` e `#QuickSight setup – ends` dentro`resource_ iac_tool_stack.py` . 2. Depois de remover o comentário, execute o `cdk deploy` comando para criar `QuickSight DataSource` e inserir `QuickSight DataSet` a QuickSight conta.	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Crie o QuickSight painel.	Para criar o QuickSight painel e a análise de exemplo, faça o seguinte: 1. Navegue até o QuickSight console e selecione a região da AWS onde os recursos são implantados. 2. No painel de navegação, escolha Conjuntos de dados e valide se um conjunto de dados chamado `ct-operations-iac-ds` foi criado no conjunto de dados da Amazon. QuickSight Se você não vê o conjunto de dados, reimplante a QuickSight construção. 3. Selecione o conjunto de dados `ct-operations-iac-ds` e escolha USAR NA ANÁLISE. 4. Selecione a planilha padrão. 5. Selecione as respectivas colunas na lista de campos no lado esquerdo. 6. Depois de selecionar as colunas necessárias, selecione o tipo visual apropriado para visualizar os dados.	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es, consulte Iniciando uma análise na Amazon QuickSigh t e Tipos visuais na Amazon QuickSight.	

Limpe todos os recursos da AWS na solução

Tarefa	Descrição	Habilidades necessárias
Remova os recursos da AWS.	1. Para remover os recursos da AWS implantados pela solução, execute o comando `cdk destroy`. 2. Exclua todos os objetos dos dois buckets do S3 e, em seguida, remova os buckets. Para obter mais informaçõ es, consulte Excluir um bucket.	AWS DevOps, DevOps engenheiro

Configure recursos adicionais além da automação da ferramenta de avaliação de recursos da AWS

Tarefa	Descrição	Habilidades necessárias
Monitore e limpe os recursos criados manualmente.	(Opcional) Se sua organizaç ão tem requisitos de conformid ade para criar recursos usando ferramentas de IaC, você pode alcançar a conformidade usando a automação da ferramenta	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	de avaliação de recursos da AWS para buscar recursos provisionados manualmente. Você também pode usar a ferramenta para importar os recursos para uma ferrament a IaC ou para recriá-los. Execute as seguintes tarefas de alto nível para monitorar recursos provisionados manualmente: 1. Implemente a automação da ferramenta de avaliação de recursos da AWS. 2. Configure uma função do Lambda para consultar as tabelas do Athena diariamente, encontrar os dados relevantes sobre recursos provisionados manualmente e exportá-los para um arquivo de valores separados por vírgula (CSV). 3. Depois que a função do Lambda for executada, uma notificação com os dados necessários poderá ser enviada às respectivas partes interessadas. 4. Para maior retenção, o arquivo.csv pode ser	

Tarefa	Descrição	Habilidades necessárias
	armazenado no bucket do S3. 5. Com base nas informaçõ es do arquivo.csv, exclua os recursos criados manualmente ou importe-os para uma solução IaC existente.	

Solução de problemas

Problema	Solução
O AWS CDK retorna erros.	Para obter ajuda com problemas do AWS CDK, consulte Solução de problemas comuns do AWS CDK.

Recursos relacionados

- Criar funções do Lambda com Python
- Comece a usar o AWS CDK
- Trabalhando com o AWS CDK no Python
- Criando uma trilha CloudTrail de toras
- Comece a usar a Amazon QuickSight

Mais informações

Várias contas

Para configurar a credencial da AWS CLI para várias contas, use os perfis da AWS. Para obter mais informações, consulte a seção Configurar vários perfis em Configurar a AWS CLI.

Comandos do AWS CDK

Ao trabalhar com o AWS CDK, lembre-se dos seguintes comandos úteis:

- Lista todas as pilhas no aplicativo

```
cdk ls
```

- Emite o modelo sintetizado da AWS CloudFormation

```
cdk synth
```

- Implanta a pilha na sua conta e região padrão da AWS

```
cdk deploy
```

- Compara a pilha implantada com o estado atual

```
cdk diff
```

- Abre a documentação do AWS CDK

```
cdk docs
```

Instale sistemas SAP automaticamente usando ferramentas de código aberto

Criado por Guilherme Sesterheim (AWS)

Resumo

Esse padrão mostra como automatizar a instalação de sistemas SAP usando ferramentas de código aberto para criar os seguintes recursos:

- Um banco de dados SAP S/4HANA 1909
- Uma instância do SAP ABAP Central Services (ASCS)
- Uma instância do Servidor de aplicações principal (PAS)

HashiCorp O Terraform cria a infraestrutura do sistema SAP e o Ansible configura o sistema operacional (OS) e instala os aplicativos SAP. O Jenkins executa a instalação.

Essa configuração transforma a instalação de sistemas SAP em um processo repetível, o que pode ajudar a aumentar a eficiência e a qualidade da implantação.

> **Note**
>
> O código de exemplo fornecido nesse padrão funciona tanto para sistemas de alta disponibilidade (HA) quanto para sistemas não HA.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do Amazon Simple Storage Service (Amazon S3) que contém todos os seus arquivos de mídia do SAP.
- Uma entidade principal do AWS Identity and Access Management (IAM) com uma chave de acesso e uma chave secreta e que tem as seguintes permissões:
  - Permissões somente leitura: Amazon Route 53, AWS Key Management Service (AWS KMS)
  - Permissões de leitura e gravação: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon, Amazon CloudWatch DynamoDB

- Uma zona hospedada privada do Route 53
- Uma assinatura do Red Hat Enterprise Linux for SAP com HA e Update Services 8.2 Imagem de máquina da Amazon (AMI) no Amazon Marketplace
- Uma chave gerenciada pelo cliente do AWS KMS
- Um par de chaves do Secure Shell (SSH)
- Um grupo EC2 de segurança da Amazon que permite a conexão SSH na porta 22 a partir do nome do host em que você instala o Jenkins (o nome do host provavelmente é localhost)
- Vagrant por HashiCorp instalado e configurado
- VirtualBoxinstalado e configurado pela Oracle
- Familiaridade com Git, Terraform, Ansible e Jenkins

Limitações

- Somente o SAP S/4HANA 1909 é totalmente testado para esse cenário específico. O exemplo de código Ansible nesse padrão requer modificação se você usar outra versão do SAP HANA.
- O procedimento de exemplo nesse padrão funciona para sistemas operacionais Mac OS e Linux. Alguns dos comandos podem ser executados somente em terminais baseados em UNIX. No entanto, você pode obter um resultado semelhante usando comandos diferentes e um sistema operacional Windows.

Versões do produto

- SAP S/4HANA 1909
- Red Hat Enterprise Linux (RHEL) versão 8.2 ou superior

Arquitetura

O diagrama a seguir mostra um exemplo de fluxo de trabalho que usa ferramentas de código aberto para automatizar a instalação de sistemas SAP em uma conta da AWS:

O diagrama mostra o seguinte fluxo de trabalho:

1. O Jenkins coordena a execução da instalação do sistema SAP executando o código do Terraform e do Ansible.

2. O código do Terraform cria a infraestrutura do sistema SAP.
3. O código Ansible configura o sistema operacional e instala aplicativos SAP.
4. Um banco de dados SAP S/4HANA 1909, uma instância ASCS e uma instância PAS que incluem todos os pré-requisitos definidos são instalados em uma instância da Amazon. EC2

> **Note**
>
> O exemplo de configuração nesse padrão cria automaticamente um bucket Amazon S3 em sua conta da AWS para armazenar o arquivo de estado do Terraform.

Pilha de tecnologia

- Terraform
- Ansible
- Jenkins
- Um banco de dados SAP S/4HANA 1909
- Uma instância do SAP ASCS
- Uma instância do SAP PAS
- Amazon EC2

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- HashiCorp O Terraform é um aplicativo de interface de linha de comando que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.
- O Ansible é uma ferramenta de código aberto de configuração como código (CaC) que ajuda a automatizar aplicativos, configurações e infraestrutura de TI.
- Jenkins: é um servidor de automação de código aberto que permite aos desenvolvedores construir, testar e implantar seu software.

Código

O código desse padrão está disponível no repositório GitHub aws-install-sap-with-jenkins-ansible.

Épicos

Configurar os pré-requisitos

Tarefa	Descrição	Habilidades necessárias
Adicione seus arquivos de mídia SAP a um bucket do Amazon S3.	Crie um bucket do Amazon S3 que contenha todos os arquivos de mídia do SAP. **Important** Certifique-se de seguir a hierarquia de pastas do AWS Launch Wizard para S/4HANA na documentação do Launch Wizard.	Administrador de nuvem
Instalar VirtualBox.	Instale e configure VirtualBo xpela Oracle.	DevOps engenheiro
Instale o Vagrant.	Instale e configure o Vagrant by. HashiCorp	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Configure sua conta da AWS.	1. Verifique se você tem uma entidade principal do IAM com uma chave de acesso e uma chave secreta e que tem as seguintes permissões: • Permissões somente de leitura: Amazon Route 53, AWS Key Management Service (AWS KMS) • Permissões de leitura e gravação: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon, Amazon CloudWatch DynamoDB 2. Salve a chave de acesso e a chave secreta da entidade principal do IAM para referência posterior. 3. Crie uma zona hospedada privada da Rota 53, se você ainda não tiver uma. Salve o nome da zona (por exemplo, sapteam.net) para referência posterior. 4. Assine o Red Hat Enterprise Linux for SAP com HA e Update Services 8.2 Imagem de máquina da	AWS geral

Tarefa	Descrição	Habilidades necessárias
	Amazon (AMI) no Amazon Marketplace Salve a ID da AMI (por exemplo, ami-0000000) para referência posterior. 5. Crie uma chave do AWS KMS gerenciada pelo cliente. Salve o nome do recurso da Amazon (ARN) da chave do KMS para referência posterior. **Note** Veja a seguir um exemplo de ARN de chave gerenciada pelo cliente do AWS KMS: arn:aws:kms:us-east- 1:123412341234:key/uuid 6. Crie um par de chaves SSH. Salve o nome do par de chaves e o arquivo .pem para referência posterior. 7. Crie um grupo de EC2 segurança da Amazon que permita a conexão SSH na porta 22 a partir do nome do host em que você instala o Jenkins. Salve a ID do grupo de segurança para referência posterior.	

Tarefa	Descrição	Habilidades necessárias
	Note O nome do host provavelmente é localhost.	

Compile e execute a instalação do SAP

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de código de. GitHub	Clone o repositório aws-install-sap-with-jenkins-ansible em. GitHub	DevOps engenheiro
Inicie o serviço do Jenkins.	Abra o terminal do Linux. Em seguida, navegue até a pasta local que contém a pasta do repositório de código clonado e execute o seguinte comando: `sudo vagrant up` **Note** A inicialização do Jenkins leva cerca de 20 minutos. O comando retorna uma mensagem de serviço ativo e em execução quando bem-sucedido.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Abra o Jenkins em um navegador da Web e faça login.	1. Em um navegador da Web, digite http://localhost:5555. O Jenkins irá abrir. 2. Faça login no Jenkins usando admin como nome de usuário e my_secret _pass_from_vault como senha.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Configure os parâmetros de instalação do sistema SAP.	1. No Jenkins, escolha Gerenciar Jenkins. Em seguida, escolha Gerenciar credenciais. Uma lista de variáveis de credenciais que você pode configurar é exibida. 2. Configure todas as seguintes variáveis de credencial: • Em AWS_ACCOUNT_CREDENTIALS, insira o ID da chave de acesso e o ID da chave de acesso secreta do seu diretor do IAM. • Para AMI_ID, insira o Red Hat Enterprise Linux for SAP com HA e a ID da AMI do Update Services 8.2. • Para KMS_KEY_ARN, insira o ARN da sua chave gerenciada pelo cliente do AWS KMS. • Para SSH_KEYPAIR_NAME, insira o nome do seu par de chaves SSH, sem inserir o tipo de arquivo .pem. • Para SSH_KEYPAIR_FILE, insira o nome completo do arquivo.pem do seu par	Administrador de sistemas e DevOps engenheiro da AWS

Tarefa	Descrição	Habilidades necessárias
	de chaves (por exemplo, mykeypair.pem). Certifique-se de também carregar o arquivo .pem dos pares de chaves no Jenkins. • Para S3_ROOT_FOLDER_INSTALL_FILES, insira o nome do bucket Amazon S3 — e da pasta, se aplicável — (por exemplo, s3:///S4H1909) que contém seus arquivos de mídia SAP. my-media-bucket • Para PRIVATE_DNS_ZONE_NAME, insira o nome da sua zona hospedada privada do Route 53 (por exemplo, myprivatecompanyurl.net). • Para VPC_ID, insira a ID da VPC (por exemplo, vpc-12345) da Amazon VPC na qual você está criando os recursos SAP. • Para SUBNET_IDS, insira duas sub-redes públicas IDs se você estiver trabalhando em um ambiente de teste (para futuros recursos de HA). Se você estiver trabalhando em um ambiente de produção, é uma prática recomenda	

Tarefa	Descrição	Habilidades necessárias
	da usar duas sub-redes privadas com um bastion host. • Para SECURITY_GROUP_ID, insira o ID do grupo de EC2 segurança da Amazon que permite a conexão SSH na porta 22 a partir do nome do host em que você instalou o Jenkins. **Note** Você pode configurar os outros parâmetros não obrigatórios conforme necessário, com base no seu caso de uso. Por exemplo, você pode alterar o ID do sistema SAP (SID) das instâncias, a senha padrão, os nomes e as tags do seu sistema SAP. Todas as variáveis obrigatórias têm (Obrigatório) no início de seus nomes.	

Tarefa	Descrição	Habilidades necessárias
Execute a instalação do sistema SAP.	1. No Jenkins, escolha Jenkins Home. Em seguida, escolha SAP Hana+ASCS +PAS 3 Instances. 2. Escolha Ativar e instalar. Depois, selecione Principal. 3. Escolha Criar agora. Para obter informações sobre as etapas do pipeline, consulte a seção Entendendo as etapas do pipeline de Automatização da instalação do SAP com ferramentas de código aberto no blog da AWS. **Note** Se ocorrer um erro, mova o cursor sobre a caixa de erro vermelha que aparece e escolha Registros. Os logs da etapa do pipeline que apresentou um erro são exibidos. A maioria dos erros ocorre devido a configurações de parâmetros incorretas.	DevOps engenheiro, administrador de sistemas da AWS

Recursos relacionados

- DevOps para SAP — Instalação do SAP: de 2 meses a 2 horas (Biblioteca de vídeos do DevOps Enterprise Summit)

Automatize o portfólio e a implantação de produtos do AWS Service Catalog usando o AWS CDK

Criado por Sandeep Gawande (AWS), RAJNEESH TYAGI (AWS) e Viyoma Sachdeva (AWS)

Resumo

O AWS Service Catalog ajuda você a gerenciar centralmente catálogos de serviços ou produtos de TI aprovados para uso no ambiente da AWS da sua organização. Uma coleção de produtos é chamada de portfólio, e um portfólio também contém informações de configuração. Com o AWS Service Catalog, você pode criar um portfólio personalizado para cada tipo de usuário em sua organização e, então, conceder acesso de modo seletivo ao portfólio adequado. Esses usuários podem então implantar rapidamente qualquer produto de que precisem dentro do portfólio.

Se você tiver uma infraestrutura de rede complexa, como arquiteturas multirregião de várias contas, é recomendável criar e gerenciar portfólios do Service Catalog em uma única conta central. Esse padrão descreve como usar o AWS Cloud Development Kit (AWS CDK) para automatizar a criação de portfólios do Service Catalog em uma conta central, conceder aos usuários finais acesso a eles e, opcionalmente, provisionar produtos em uma ou mais contas de destino da AWS. Essa ready-to-use solução cria os portfólios do Service Catalog na conta de origem. Opcionalmente, também provisiona produtos em contas de destino usando CloudFormation pilhas da AWS e ajuda você a configurar TagOptions os produtos:

- AWS CloudFormation StackSets — Você pode usar StackSets para lançar produtos do Service Catalog em várias regiões e contas da AWS. Nessa solução, você tem a opção de provisionar produtos automaticamente ao implantar essa solução. Para obter mais informações, consulte Como usar a AWS CloudFormation StackSets (documentação do Service Catalog) e StackSets conceitos (CloudFormation documentação).
- TagOption biblioteca — você pode gerenciar tags em produtos provisionados usando TagOption a biblioteca. A TagOptioné um par de valores-chave gerenciado no AWS Service Catalog. Não é uma tag da AWS, mas serve como um modelo para criar uma tag da AWS com base na TagOption. Para obter mais informações, consulte a TagOption biblioteca (documentação do Service Catalog).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da AWS que você deseja usar como a conta de origem para administrar os portfólios do Service Catalog.
- Se você estiver usando essa solução para provisionar produtos em uma ou mais contas de destino, a conta de destino já deverá existir e estar ativa.
- Permissões do AWS Identity and Access Management (IAM) para acessar o AWS Service Catalog, o AWS CloudFormation e o AWS IAM.

Versões do produto

- AWS CDK versão 2.27.0

Arquitetura

Pilha de tecnologias de destino

- Portfólios do Service Catalog em uma conta centralizada da AWS
- Produtos do Service Catalog implantados na conta de destino

Arquitetura de destino

1. Na conta do portfólio (ou origem), você atualiza o arquivo config.json com a conta da AWS, a região da AWS, o perfil do IAM, o portfólio e as informações do produto para seu caso de uso.
2. Você implanta o aplicativo AWS CDK.
3. O aplicativo AWS CDK assume o perfil de implantação do IAM e cria os portfólios e produtos do Service Catalog definidos no arquivo config.json.

   Se você configurou StackSets para implantar produtos em uma conta de destino, o processo continua. Se você não configurou StackSets para provisionar nenhum produto, o processo está concluído.
4. O aplicativo AWS CDK assume a função de StackSet administrador e implanta o conjunto de CloudFormation pilhas da AWS que você definiu no arquivo config.json.
5. Na conta-alvo, StackSets assume a função de StackSet execução e provisiona os produtos.

Ferramentas

Serviços da AWS

- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- O AWS CDK Toolkit é um kit de desenvolvimento em nuvem de linha de comando que ajuda você a interagir com seu aplicativo AWS CDK.
- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Service Catalog ajuda você a gerenciar de modo centralizado os catálogos de serviços de TI aprovados para a AWS. Os usuários finais podem implantar rapidamente somente os serviços de TI aprovados de que precisam, seguindo as restrições definidas pela organização.

Repositório de código

O código desse padrão está disponível em GitHub, no aws-cdk-servicecatalog-automationrepositório. O repositório de código contém os seguintes arquivos e pastas:

- cdk-sevicecatalog-app— Essa pasta contém o aplicativo AWS CDK para essa solução.
- config — Essa pasta contém o arquivo config.json e o CloudFormation modelo para implantar os produtos no portfólio do Service Catalog.
- config/config.json: esse arquivo contém todas as informações de configuração. Você atualiza esse arquivo para personalizar essa solução para seu caso de uso.
- config/templates — Essa pasta contém os CloudFormation modelos dos produtos do Service Center.
- setup.sh: esse script implanta a solução.
- uninstall.sh: esse script exclui a pilha e todos os recursos da AWS criados ao implantar essa solução.

Para usar o código de amostra, siga as instruções na seção Épicos.

Práticas recomendadas

- As funções do IAM usadas para implantar essa solução devem seguir o princípio do privilégio mínimo (documentação do IAM).
- Siga as melhores práticas para desenvolver aplicativos em nuvem com o AWS CDK (postagem no blog da AWS).
- Siga as CloudFormation melhores práticas da AWS (CloudFormation documentação).

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias

Instale o AWS CDK Toolkit.	Verifique se você tem o AWS CDK Toolkit instalado. Digite o comando a seguir para confirmar se ele está instalado e verificar a versão.
	`cdk --version`
	Se o AWS CDK Toolkit ainda não estiver instalado, insira o comando a seguir para instalá-lo.
	`npm install -g aws-cdk@2.27.0`
	Se a versão do AWS CDK Toolkit for anterior à 2.27.0, digite o comando a seguir para atualizá-la para a versão 2.27.0.
		AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`npm install -g aws-cdk@2.27.0 --force`	

Clonar o repositório.	Insira o comando da a seguir. Em Clonar o repositório na seção Informações adicionais, você pode copiar o comando completo contendo a URL do repositório. Isso clona o aws-cdk-servicecatalog-automationrepositório de. GitHub
	`git clone <repository-URL>.git`
	Isso cria uma pasta `cd aws-cdk-servicecatalog-automation` no diretório de destino. Para navegar até essa pasta, insira o comando a seguir.
	`cd aws-cdk-servicecatalog-automation`
		AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Configurar credenciais da AWS.	Insira os comandos a seguir. Eles exportam as seguintes variáveis, que definem a conta da AWS e a região em que você está implantando a pilha.
	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAU LT_REGION=<AWS Region>`
	As credenciais da AWS para o AWS CDK são fornecida s por meio de variáveis de ambiente.
		AWS DevOps, DevOps engenheiro

Configurar permissões de usuário usando perfis do IAM.	Se você for usar funções do IAM para conceder acesso ao portfólio e aos produtos nele contidos, as funções devem ter permissões para serem assumidas pela entidade principal de serviço serviceca talog.amazonaws.com. Para obter instruções sobre como conceder essas permissões, consulte Habilitar o acesso confiável com o Service Catalog (documentação do AWS Organizations).	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Configure as funções do IAM exigidas pelo StackSets.	Se você estiver usando StackSets para provisionar produtos automaticamente nas contas de destino, precisará configurar as funções do IAM que administram e executam o conjunto de pilhas. 1. Na conta de origem, confirme se `AWSCloudFormationStackSetAdministrationRole` já existe. Nas contas de destino, confirme se `AWSCloudFormationStackSetExecutionRole` já existe. Se essas funções já existirem, vá direto para o próximo épico. 2. Siga as instruções em Conceder permissões autogerenciadas (documentação do IAM) para criar a função de administração do conjunto de pilhas na conta do portfólio e criar a função de execução em cada conta de destino.	AWS DevOps, DevOps engenheiro

Personalize e implante a solução

Tarefa	Descrição	Habilidades necessárias
Crie os CloudFormation modelos.	Na `config/templates` pasta, crie CloudFormation modelos para qualquer produto que você queira incluir em seus portfólios. Para obter mais informaçõ es, consulte Como trabalhar com CloudFormation modelos da AWS (CloudFormation documentação).	Desenvolvedor de aplicativ os, AWS DevOps, DevOps engenheiro
Personalize o arquivo de configuração.	Na pasta `config`, abra o arquivo config.json e defina os parâmetros conforme apropriado para seu caso de uso. Os seguintes parâmetro s são obrigatórios, salvo indicação em contrário: Na seção `portfolios` , defina os seguintes parâmetro s para criar um ou mais portfólios do Service Catalog: • `portfolioName` : o nome do portfólio. • `providerName` : o nome da pessoa, equipe ou organização que gerencia o portfólio. • `description` : uma breve descrição do portfólio.	Desenvolvedor de aplicativ os, DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• `roles`: (opcional) nomes de todas as funções do IAM que devem ter acesso a esse portfólio. Os usuários que têm essa função podem acessar os produtos desse portfólio. • `users`: (opcional) nomes de todos os usuários do IAM que deveriam ter acesso a esse portfólio e seus produtos. • `groups`: (opcional) nomes de quaisquer grupos de usuários do IAM que deveriam ter acesso a esse portfólio e seus produtos. ⚠ Warning Os usuários do IAM têm credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissõe s necessárias para realizar a tarefa e que você os remova	

Tarefa	Descrição	Habilidades necessárias
	quando não forem mais necessários. **Important** `roles`,`users`, e `groups` são todos parâmetros opcionais , mas se você não definir um desses parâmetros, ninguém poderá visualiza r os produtos do portfólio no console do Service Catalog. Defina pelo menos um desses parâmetro s. Para obter mais informações, consulte Conceder permissõe s aos usuários finais do Service Catalog (documentação do Service Catalog). • (Opcional) Na `tagOption` seção, defina TagOptions para os produtos: • `key`— Nome da TagOption chave	

Tarefa	Descrição	Habilidades necessárias
	• `value`— Valores de string permitidos para o TagOption Para obter mais informaçõ es, consulte a TagOption biblioteca (documentação do Service Catalog). • Na seção `products`, defina os seguintes parâmetros para os produtos: • `portfolioName` : o nome do portfólio onde deseja adicionar o produto. Você pode especificar apenas um portfólio. • `productName` : o nome do produto. • `owner`: o proprietário do produto. • `productVersionName` : o nome da versão do produto no valor da string, como `v1`. • `templatePath` — O caminho do arquivo para o CloudFormation modelo do produto. • `deployWithStackSet s` — (Opcional) Especifiq ue uma ou mais contas e regiões onde você deseja	

Tarefa	Descrição	Habilidades necessárias
	usar StackSets para provisionar automatic amente produtos nos portfólios. Se você usar essa opção de implantaç ão, todos os parâmetros a seguir nesta seção serão obrigatórios: • `accounts`: as contas de destino. • `regions`: as regiões de destino. • `stackSetA dministra tionRoleName` — O nome da função do IAM usada para administrar a StackSets configura ção. Não mude esse valor. Esse perfil deve ter esse nome exato. • `stackSetE xecutionR oleName` : o nome do perfil do IAM na conta de destino que implanta as instâncias da pilha. Não mude esse valor. Esse perfil deve ter esse nome exato. Para ver um exemplo de um arquivo de configuração completo, consulte Exemplo	

Tarefa	Descrição	Habilidades necessárias
	de arquivo de configuração na seção Informações adicionais.	
Implante a solução.	Insira o comando da a seguir. Isso implanta o aplicativo AWS CDK e provisiona os portfólios e produtos do Service Catalog conforme especificado no arquivo config.json. `sh +x setup.sh`	Desenvolvedor de aplicativos, DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Verificar a implantação.	Verifique a implantação bem-sucedida fazendo o seguinte: 1. Faça login no Console de Gerenciamento da AWS com credenciais que podem acessar um ou mais dos portfólios que você definiu no arquivo de configuração. 2. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/. 3. No painel de navegação , em Provisionamento, escolha Produtos. Verifique se você vê uma lista de produtos que especificou para o portfólio. 4. Siga as instruções em Lançamento de um produto (documentação do Service Catalog) para lançar um dos produtos disponíveis. Confirme se as versões e tags disponíveis do produto correspondem aos valores fornecidos no arquivo de configuração. 5. Se você optar por provision ar produtos automatic amente em uma ou mais contas de destino usando StackSets, faça o seguinte:	AWS geral

Tarefa	Descrição	Habilidades necessárias
	a. Faça login com credenciais que lhe dão permissão para visualizar os produtos provisionados em uma das contas de destino. b. No console do Service Catalog, no painel de navegação, em Provisionamento, escolha Produtos provisionados. c. Confirme se os produtos esperados aparecem na lista.	

Tarefa	Descrição	Habilidades necessárias
(Opcional) Atualize os portfólios e os produtos.	Se você quiser usar essa solução para atualizar os portfólios ou produtos ou para provisionar novos produtos: 1. Faça as alterações necessárias no arquivo config.json. 2. Adicione ou modifique CloudFormation qualquer modelo conforme necessário na `config/template` pasta. 3. Reimplante a solução. Por exemplo, você pode adicionar mais portfólios ou provisionar mais recursos. O aplicativo AWS CDK implementa somente as alterações. Se não houver alterações nos portfólios ou produtos implantados anteriormente, a reimplantação não os afetará.	Desenvolvedor de aplicativos, DevOps engenheiro, AWS geral

Limpe a solução

Tarefa	Descrição	Habilidades necessárias
(Opcional) Remova os recursos da AWS implantados por essa solução.	Se você quiser excluir um produto provisionado, siga as instruções em Excluindo	AWS DevOps, DevOps engenheiro, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	produtos provisionados (documentação do Service Catalog). Para excluir todos os recursos criados por essa solução, insira o comando a seguir. `sh uninstall.sh`	

Recursos relacionados

- Biblioteca de estrutura do AWS Service Catalog (referência do AWS API)
- StackSets conceitos (CloudFormation documentação)
- AWS Service Catalog (marketing da AWS)
- Usando o Service Catalog com o AWS CDK (workshop da AWS)

Mais informações

Clonar o repositório

Digite o comando a seguir para clonar o repositório. GitHub

```
git clone https://github.com/aws-samples/aws-cdk-servicecatalog-automation.git
```

Arquivo de configuração de amostra

Veja a seguir um exemplo de arquivo config.json com valores de exemplo.

```
{
    "portfolios": [
        {
            "displayName": "EC2 Product Portfolio",
            "providerName": "User1",
            "description": "Test1",
            "roles": [
```

```
                "<Names of IAM roles that can access the products>"
            ],
            "users": [
                "<Names of IAM users who can access the products>"
            ],
            "groups": [
                "<Names of IAM user groups that can access the products>"
            ]
        },
        {
            "displayName": "Autoscaling Product Portfolio",
            "providerName": "User2",
            "description": "Test2",
            "roles": [
                "<Name of IAM role>"
            ]
        }
    ],
    "tagOption": [
        {
            "key": "Group",
            "value": [
                "finance",
                "engineering",
                "marketing",
                "research"
            ]
        },
        {
            "key": "CostCenter",
            "value": [
                "01",
                "02",
                "03",
                "04"
            ]
        },
        {
            "key": "Environment",
            "value": [
                "dev",
                "prod",
                "stage"
            ]
```

```
        }
    ],
    "products": [
        {
            "portfolioName": "EC2 Product Profile",
            "productName": "Ec2",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template1.json"
        },
        {
            "portfolioName": "Autoscaling Product Profile",
            "productName": "autoscaling",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template2.json",
            "deployWithStackSets": {
                "accounts": [
                    "012345678901",
                ],
                "regions": [
                    "us-west-2"
                ],
                "stackSetAdministrationRoleName":
 "AWSCloudFormationStackSetAdministrationRole",
                "stackSetExecutionRoleName": "AWSCloudFormationStackSetExecutionRole"
            }
        }
    ]
}
```

Automatize backups orientados por eventos para o Amazon CodeCommit S3 usando e Eventos CodeBuild CloudWatch

Criado por Kirankumar Chandrashekar (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), você pode usar a AWS CodeCommit para hospedar repositórios seguros baseados em Git. CodeCommit é um serviço de controle de origem totalmente gerenciado. No entanto, se um CodeCommit repositório for excluído acidentalmente, seu conteúdo também será excluído e não poderá ser restaurado.

Esse padrão descreve como fazer backup automático de um CodeCommit repositório em um bucket do Amazon Simple Storage Service (Amazon S3) após uma alteração ser feita no repositório. Se o CodeCommit repositório for excluído posteriormente, essa estratégia de backup fornecerá uma opção de point-in-time recuperação.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um CodeCommit repositório existente, com acesso do usuário configurado de acordo com seus requisitos. Para obter mais informações, consulte Configuração para a AWS CodeCommit na CodeCommit documentação.
- Um bucket S3 para fazer o upload dos CodeCommit backups.

Limitações

- Esse padrão faz backup automático de todos os seus CodeCommit repositórios. Se você quiser fazer backup de CodeCommit repositórios individuais, você deve modificar a regra do Amazon CloudWatch Events.

Arquitetura

O diagrama a seguir ilustra o fluxo de trabalho deste padrão.

O fluxo de trabalho consiste nas seguintes etapas:

1. O código é enviado para um CodeCommit repositório.
2. O CodeCommit repositório notifica CloudWatch os eventos de uma alteração no repositório (por exemplo, um `git push` comando).
3. CloudWatch Events invoca a AWS CodeBuild e envia a ela as informações do CodeCommit repositório.
4. CodeBuild clona o CodeCommit repositório inteiro e o empacota em um arquivo.zip.
5. CodeBuild carrega o arquivo.zip em um bucket do S3.

Pilha de tecnologia

- CloudWatch Eventos
- CodeBuild
- CodeCommit
- Amazon S3

Ferramentas

- Amazon CloudWatch Events — CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- AWS CodeBuild — CodeBuild é um serviço de integração contínua totalmente gerenciado que compila o código-fonte, executa testes e produz pacotes de software prontos para implantação.
- AWS CodeCommit — CodeCommit é um serviço de controle de origem totalmente gerenciado que hospeda repositórios seguros baseados em Git.
- AWS Identity and Access Management (IAM): o IAM é um serviço da web que ajuda você a controlar o acesso aos recursos da AWS com segurança.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet.

Épicos

Crie um CodeBuild projeto

Tarefa	Descrição	Habilidades necessárias
Crie uma função CodeBuild de serviço.	Faça login no Console de Gerenciamento da AWS e abra o console do IAM. Selecione Perfis e, depois, Criar perfil. Crie uma função de serviço CodeBuild para clonar o CodeCommit repositório, fazer upload de arquivos para o bucket do S3 e enviar registros para a Amazon. CloudWatch Para obter mais informações, consulte Criar uma função de CodeBuild serviço na CodeBuild documentação.	Administrador de nuvem
Crie um CodeBuild projeto.	No CodeBuild console, escolha Criar CodeBuild projeto. Crie um CodeBuild projeto usando o `buildspec .yml` modelo da seção Informações adicionais. Para obter ajuda com essa história, consulte Criar um projeto de construção na CodeBuild documentação.	Administrador de nuvem

Crie e configure a regra de CloudWatch eventos

Tarefa	Descrição	Habilidades necessárias
Crie uma função do IAM para CloudWatch eventos.	No console do IAM, escolha Roles e crie um papel do IAM para CloudWatch Events. Para obter mais informações sobre isso, consulte a função CloudWatch Events IAM na documentação do IAM. **Important** Você deve adicionar `codebuild:StartBuild` permissões à função do IAM para CloudWatch Eventos.	Administrador de nuvem
Crie uma regra de CloudWatch eventos.	1. No CloudWatch console, escolha Eventos e, em seguida, escolha Regras. Escolha Criar regra e use a regra CloudWatch Eventos na seção Informações adicionais. Isso cria uma regra que escuta alterações de eventos (por exemplo, `git push` ou `git commit` comandos) em seus CodeCommit repositórios. Para obter mais informações, consulte Criar uma regra de CloudWatch eventos para uma	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	CodeCommit fonte na CodePipeline documentação da AWS. 2. Escolha Destinos, escolha Tópico e, em seguida, escolha Configurar entrada. Escolha Transformador de entrada e use o caminho e o modelo de entrada na seção Informações adicionais. Isso garante que os detalhes CodeCommit do seu repositório sejam analisados e enviados como variáveis de ambiente para o CodeBuild projeto. Para obter mais informações, consulte o tutorial do transformador de entrada na CloudWatch documentação. 3. Escolha Configurar detalhes, e insira um nome e uma descrição para a regra. Escolha Criar regra. **Important** Essa regra de CloudWatch eventos descreve as alterações em todos os seus CodeCommit repositórios. Você deve	

Tarefa	Descrição	Habilidades necessárias
	modificar a regra de CloudWatch Eventos se quiser fazer backup de CodeCommit repositórios individuais ou usar buckets S3 separados para backups de repositórios diferentes.	

Recursos relacionados

Criando um CodeBuild projeto

- Criar uma função CodeBuild de serviço
- Crie um CodeBuild projeto
- Permissões necessárias para comandos do cliente Git

Criando e configurando uma regra de CloudWatch eventos

- Criar uma regra de CloudWatch eventos para uma CodeCommit fonte
- Usar o transformador de entrada para personalizar o que é passado para o evento de destino
- Crie uma regra de CloudWatch eventos que inicie em um evento
- Crie uma função do CloudWatch Events IAM

Mais informações

CodeBuild modelo buildspec.yml

```
version: 0.2
phases:
  install:
    commands:
      - pip install git-remote-codecommit
```

```
  build:
    commands:
       - env
       - git clone -b $REFERENCE_NAME codecommit::$REPO_REGION://$REPOSITORY_NAME
       - dt=$(date '+%d-%m-%Y-%H:%M:%S');
       - echo "$dt"
       - zip -yr $dt-$REPOSITORY_NAME-backup.zip ./
       - aws s3 cp $dt-$REPOSITORY_NAME-backup.zip s3:// #substitute a valid S3 Bucket
 Name here
```

CloudWatch Regra de eventos

```
{
  "source": [
    "aws.codecommit"
  ],
  "detail-type": [
    "CodeCommit Repository State Change"
  ],
  "detail": {
    "event": [
      "referenceCreated",
      "referenceUpdated"
    ]
  }
}
```

Transformador de entrada de amostra para o alvo da regra de CloudWatch eventos

Caminho de entrada:

```
{"referenceType":"$.detail.referenceType","region":"$.region","repositoryName":"$.detail.reposi
```

Modelo de entrada (preencha os valores conforme apropriado):

```
{
    "environmentVariablesOverride": [
        {
            "name": "REFERENCE_NAME",
            "value": ""
        },
        {
```

```
            "name": "REFERENCE_TYPE",
            "value": ""
        },
        {
            "name": "REPOSITORY_NAME",
            "value": ""
        },
        {
            "name": "REPO_REGION",
            "value": ""
        },
        {
            "name": "ACCOUNT_ID",
            "value": ""
        }
    ]
}
```

Automatize a exclusão de AWS CloudFormation pilhas e recursos associados

Criado por SANDEEP SINGH (AWS) e James Jacob (AWS)

Resumo

AWS CloudFormationé um serviço amplamente usado para gerenciar a infraestrutura de nuvem como código (IaC). Ao usar CloudFormation, você gerencia os recursos relacionados como uma única unidade chamada pilha. Você pode criar, atualizar e excluir um conjunto de recursos criando, atualizando e excluindo pilhas.

Às vezes, você não precisa mais dos recursos em uma CloudFormation pilha. Dependendo dos recursos e de suas configurações, pode ser complicado excluir uma pilha e seus recursos associados. Em sistemas de produção do mundo real, as exclusões às vezes falham ou demoram muito devido a condições ou restrições conflitantes que não podem ser substituídas. CloudFormation Isso pode exigir planejamento e execução cuidadosos para garantir que todos os recursos sejam excluídos adequadamente de maneira eficiente e consistente. Esse padrão descreve como configurar uma estrutura que ajuda você a gerenciar a exclusão de CloudFormation pilhas que envolvem as seguintes complexidades:

- Recursos com proteção contra exclusão — Alguns recursos podem ter a proteção contra exclusão ativada. Exemplos comuns são tabelas do Amazon DynamoDB e buckets do Amazon Simple Storage Service (Amazon S3). A proteção contra exclusão impede a exclusão automática, como a exclusão por meio de. CloudFormation Se você quiser excluir esses recursos, deverá substituir ou desativar temporariamente a proteção de exclusão manual ou programaticamente. Você deve considerar cuidadosamente a implicação de excluir esses recursos antes de continuar.
- Recursos com políticas de retenção — Certos recursos, como chaves AWS Key Management Service (AWS KMS) e buckets do Amazon S3, podem ter políticas de retenção que especificam por quanto tempo eles devem ser retidos após a solicitação da exclusão. Você deve considerar essas políticas na estratégia de limpeza para manter a conformidade com as políticas organizacionais e os requisitos regulatórios.
- Exclusão retardada de funções Lambda que estão anexadas a uma VPC — A exclusão de AWS Lambdauma função conectada a uma nuvem privada virtual (VPC) pode levar de 5 a 40 minutos, dependendo das várias dependências interconectadas envolvidas no processo. Se você separar a função da VPC antes de excluir a pilha, poderá reduzir esse atraso para menos de 1 minuto.

- Recursos não criados diretamente por CloudFormation — Em determinados designs de aplicativos, os recursos podem ser criados fora da CloudFormation pilha original, seja pelo próprio aplicativo ou por recursos provisionados por meio da pilha. Veja os dois exemplos a seguir:
  - CloudFormation pode provisionar uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que executa um script de dados do usuário. Em seguida, esse script pode criar um AWS Systems Managerparâmetro para armazenar dados relacionados ao aplicativo. Esse parâmetro não é gerenciado por meio de CloudFormation.
  - CloudFormation pode provisionar uma função Lambda que gera automaticamente um grupo Amazon CloudWatch Logs para armazenar registros. Esse grupo de registros não é gerenciado por meio de CloudFormation.

  Embora esses recursos não sejam gerenciados diretamente pelo CloudFormation, eles geralmente precisam ser limpos quando a pilha é excluída. Se não forem gerenciados, eles podem ficar órfãos e levar ao consumo desnecessário de recursos.

Embora essas grades de proteção possam causar complexidade, elas são intencionais e críticas. CloudFormation Permitir ignorar todas as restrições e excluir recursos indiscriminadamente pode levar a consequências prejudiciais e imprevistas em muitos cenários. No entanto, como DevOps engenheiro de nuvem responsável pelo gerenciamento do ambiente, às vezes pode ser necessário ignorar essas restrições, principalmente em ambientes de desenvolvimento, teste ou preparação.

Resultados de negócios desejados

Ao implementar essa estrutura, você pode obter os seguintes benefícios:

- Gerenciamento de custos — a limpeza regular e eficiente de ambientes temporários, como end-to-end ambientes de teste de aceitação de usuários, ajuda a evitar que os recursos funcionem por mais tempo do que o necessário. Isso pode reduzir significativamente os custos.
- Segurança — A limpeza automatizada de recursos desatualizados ou não utilizados reduz a superfície de ataque e ajuda a manter um ambiente seguro AWS .
- Eficiência operacional — A limpeza regular e automatizada pode fornecer os seguintes benefícios operacionais:
  - Scripts automatizados que removem grupos de logs antigos ou buckets vazios do Amazon S3 podem melhorar a eficiência operacional mantendo o ambiente limpo e gerenciável.
  - A exclusão e recriação rápida de pilhas oferece suporte à iteração rápida para design e implementação, o que pode levar a uma arquitetura mais robusta e resiliente.

- Excluir e reconstruir ambientes regularmente pode ajudá-lo a identificar e corrigir possíveis problemas. Isso pode ajudar você a garantir que a infraestrutura resista a cenários do mundo real.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Python versão 3.6 ou posterior, instalado
- AWS Command Line Interface (AWS CLI), instalado e configurado

Limitações

- Uma convenção de nomenclatura é usada para identificar os recursos que devem ser excluídos. O código de amostra nesse padrão usa um prefixo para o nome do recurso, mas você pode definir sua própria convenção de nomenclatura. Os recursos que não usarem essa convenção de nomenclatura não serão identificados ou posteriormente excluídos.

Arquitetura

O diagrama a seguir mostra como essa estrutura identifica a CloudFormation pilha de destino e os recursos adicionais associados a ela.

O diagrama mostra o seguinte fluxo de trabalho:

1. Reúna recursos — A estrutura de automação usa uma convenção de nomenclatura para retornar todas as CloudFormation pilhas relevantes, repositórios do Amazon Elastic Container Registry (Amazon ECR), tabelas do DynamoDB e buckets do Amazon S3.

> **Note**
>
> As funções desse estágio usam paginadores, um recurso do Boto3 que abstrai o processo de iteração em um conjunto de resultados de API truncado. Isso garante que todos os recursos sejam processados. Para otimizar ainda mais o desempenho, considere aplicar

a filtragem do lado do servidor ou considere usá-la JMESPath para realizar a filtragem do lado do cliente.

2. Pré-processamento — A estrutura de automação identifica e aborda as restrições de serviço que devem ser substituídas para permitir a exclusão dos recursos. CloudFormation Por exemplo, ele altera a `DeletionProtectionEnabled` configuração das tabelas do DynamoDB para. `False` Na interface de linha de comando, para cada recurso, você recebe um prompt perguntando se deseja substituir a restrição.
3. Excluir pilha — A estrutura de automação exclui a CloudFormation pilha. Na interface de linha de comando, você recebe um prompt perguntando se deseja excluir a pilha.
4. Pós-processamento — a estrutura de automação exclui todos os recursos relacionados que não foram provisionados diretamente CloudFormation como parte da pilha. Exemplos desses tipos de recursos incluem parâmetros e grupos de CloudWatch registros do Systems Manager. Funções separadas reúnem esses recursos, os pré-processam e, em seguida, os excluem. Na interface de linha de comando, para cada recurso, você recebe um prompt perguntando se deseja excluir o recurso.

> **Note**
>
> As funções desse estágio usam paginadores, um recurso do Boto3 que abstrai o processo de iteração em um conjunto de resultados de API truncado. Isso garante que todos os recursos sejam processados. Para otimizar ainda mais o desempenho, considere aplicar a filtragem do lado do servidor ou considere usá-la JMESPath para realizar a filtragem do lado do cliente.

Automação e escala

Se sua CloudFormation pilha incluir outros recursos que não estão incluídos no código de amostra ou se a pilha tiver uma restrição que não tenha sido tratada nesse padrão, você poderá adaptar a estrutura de automação para seu caso de uso. Siga a mesma metodologia de coleta de recursos, pré-processamento, exclusão da pilha e, em seguida, pós-processamento.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- CloudFormation A Interface de Linha de Comando (CFN-CLI) é uma ferramenta de código aberto que ajuda você a desenvolver e testar extensões de terceiros AWS e, em seguida, registrá-las para uso em. CloudFormation
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS

Outras ferramentas

- Click é uma ferramenta Python que ajuda você a criar interfaces de linha de comando.
- Poetry é uma ferramenta para gerenciamento e empacotamento de dependências em Python.
- O Pyenv é uma ferramenta que ajuda você a gerenciar e alternar entre as versões do Python.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no GitHub cloudformation-stack-cleanuprepositório.

Práticas recomendadas

- Marque recursos para facilitar a identificação — implemente uma estratégia de marcação para identificar recursos criados para diferentes ambientes e propósitos. As tags podem simplificar o processo de limpeza ajudando você a filtrar recursos com base em suas tags.
- Configurar ciclos de vida dos recursos — Defina os ciclos de vida dos recursos para excluir automaticamente os recursos após um determinado período. Essa prática ajuda a garantir que ambientes temporários não se tornem passivos de custo permanentes.

Épicos

Instalar as ferramentas

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	1. Crie uma pasta em seu ambiente virtual. Nomeie com o nome do seu projeto. 2. Abra um terminal em sua máquina local e navegue até essa pasta. 3. Digite o comando a seguir para clonar o cloudformation-stack-cleanup repositório no diretório do seu projeto: `git clone https://github.com/aws-samples/cloudformation-stack-cleanup.git`	DevOps engenheiro
Instale o Poetry.	Siga as instruções (documentação do Poetry) para instalar o Poetry no ambiente virtual de destino.	DevOps engenheiro

Instale as dependências.	1. Digite o comando a seguir para navegar até o diretório do projeto:
	`cd cloudformation-stack-cleanup`
	2. Digite o comando:
	`poetry install`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Isso instala todas as dependências necessárias, como Boto3, click e o código-fonte da CLI. CloudFormation	
(Opcional) Instale o Pyenv.	Siga as instruções (GitHub) para instalar o Pyenv.	DevOps engenheiro

(Opcional) Personalize a estrutura

Tarefa	Descrição	Habilidades necessárias
Crie funções que coletem, pré-processem e excluam os recursos de destino.	1. No repositório clonado, digite o seguinte comando para navegar até o `cli` diretório: `cd cfncli/cli` 2. Abra o arquivo cleanup_environment.py. 3. Crie uma nova função Python que reúna o tipo de recurso que você deseja modificar. Para ver um exemplo, consulte a `gather_ddb_tables` função nesse arquivo. 4. Crie uma nova função Python que substitua as restrições de serviço do recurso de destino. Para ver um exemplo, consulte a	DevOps engenheiro, Python

Tarefa	Descrição	Habilidades necessárias
	`remove_ddb_deletion_protection` função nesse arquivo. 5. Crie uma nova função Python que colete recursos de destino não gerenciados. Para ver um exemplo, consulte a `gather_log_groups` função nesse arquivo. 6. Crie uma nova função Python que exclua recursos de destino não gerenciados. Para ver um exemplo, consulte a `delete_log_group` função nesse arquivo. 7. Salve e feche o arquivo cleanup_enviornment.py.	

Crie exemplos de recursos

Tarefa	Descrição	Habilidades necessárias
Crie uma CloudFormation pilha.	1. Navegue até o diretório de projeto do . 2. Insira o comando a seguir para criar uma CloudFormation pilha que provisiona uma tabela do DynamoDB e um grupo de segurança. Atualize o valor para`<VPCID>`:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`aws cloudformation create-stack \ --stack-name sampleforcleanup-Stack \ --template-body file://samples/sample-cfn-stack.yaml \ --parameters ParameterKey=VpcId,ParameterValue=<VPCID> \ --region us-east-1`	
Crie um parâmetro do Systems Manager.	Insira o comando a seguir para criar um parâmetro do Systems Manager que não seja provisionado por meio de: CloudFormation `aws ssm put-parameter \ --name "/samplefor cleanup/database/password" \ --value "your_db_password" \ --type "SecureString" \ --description "Database password for my app" \ --tier "Standard" \ --region "us-east-1"`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Crie um bucket do Amazon S3.	Insira o seguinte comando para criar um bucket do Amazon S3 que não seja provisionado por meio de: CloudFormation `aws s3api create-bucket \ --bucket samplesor cleanup-unmanagedb ucket-<UniqueIdent ifier> \ --region us-east-1 \ --create-bucket-co nfiguration LocationC onstraint=us-east-1`	AWS DevOps

Exclua os recursos de amostra

Tarefa	Descrição	Habilidades necessárias
Exclua a CloudFormation pilha.	1. Insira o seguinte comando para excluir a CloudForm ation pilha de amostras, o parâmetro Systems Manager e o bucket do Amazon S3 que você criou: `cfncli --region us- east-1 \ dev cleanup-env \ --prefix-list sampleforcleanup` 2. Quando solicitado, insira Y para continuar.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Valide a exclusão de recursos.	Na saída, confirme se todos os recursos de amostra foram excluídos. Para obter um exemplo de saída, consulte a seção Recursos adicionais desse padrão.	AWS DevOps

Recursos relacionados

- Excluir uma pilha (CloudFormation documentação)
- Solução de problemas CloudFormation (CloudFormation documentação)
- Conceder às funções do Lambda acesso aos recursos em uma Amazon VPC (documentação do Lambda)
- Como excluo uma AWS CloudFormation pilha que está presa no status DELETE_FAILED? (Centro de AWS conhecimento)

Mais informações

Veja a seguir um exemplo de saída do `cfncli` comando:

```
cfncli --region aus-east-1  dev cleanup-env --prefix-list sampleforcleanup


https://sts.us-east-1.amazonaws.com
Cleaning up: ['sampleforcleanup'] in xxxxxxxxxx:us-east-1
Do you want to proceed? [Y/n]: Y
No S3 buckets
No ECR repositories
No Lambda functions in VPC
The following DynamoDB tables will have their deletion protection removed:
sampleforcleanup-MyDynamoDBTable
Do you want to proceed with removing deletion protection from these tables? [Y/n]: Y
Deletion protection disabled for DynamoDB table 'sampleforcleanup-MyDynamoDBTable'.
The following CloudFormation stacks will be deleted:
sampleforcleanup-Stack
Do you want to proceed with deleting these CloudFormation stacks? [Y/n]: Y
```

```
Initiated deletion of CloudFormation stack: `sampleforcleanup-Stack`
Waiting for stack `sampleforcleanup-Stack` to be deleted...
CloudFormation stack `sampleforcleanup-Stack` deleted successfully.
The following ssm_params will be deleted:
/sampleforcleanup/database/password
Do you want to proceed with deleting these ssm_params? [Y/n]: Y
Deleted SSM Parameter: /sampleforcleanup/database/password
Cleaned up: ['sampleforcleanup']
```

Automatize o gerenciamento dinâmico de pipelines para implantar soluções de hotfix em ambientes Gitflow usando e AWS Service CatalogAWS CodePipeline

Criado por Balaji Vedagiri (AWS), Faisal Shahdad (AWS), Shanmugam Shanker (AWS) e Vivek Thangamuthu (AWS)

Resumo

> **Note**
>
> AWS CodeCommit não está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão aborda um cenário de gerenciamento de um pipeline dinâmico de hotfix dedicado exclusivamente à implantação segura de soluções de hotfix em um ambiente de produção. A solução é implementada e gerenciada usando um AWS Service Catalog portfólio e um produto. Uma EventBridge regra da Amazon é usada para automação de eventos. As restrições são aplicadas usando as restrições de portfólio e as funções AWS Identity and Access Management (IAM) do Service Catalog para desenvolvedores. Somente uma AWS Lambda função tem permissão para iniciar o produto Service Catalog, acionada pela EventBridge regra. Esse padrão foi projetado para ambientes com uma configuração específica do Gitflow, descrita em Informações adicionais.

Normalmente, um hotfix é implantado para resolver problemas críticos ou de segurança relatados em um ambiente ativo, como produção. Os hotfixes devem ser implantados diretamente somente nos ambientes de preparação e produção. Os pipelines de preparação e produção são usados extensivamente para solicitações regulares de desenvolvimento. Esses pipelines não podem ser usados para implantar hotfixes porque há recursos contínuos de garantia de qualidade que não podem ser promovidos à produção. Para lançar hotfixes, esse padrão descreve um pipeline dinâmico e de curta duração com os seguintes recursos de segurança:

- Criação automática — Um pipeline de hotfix é criado automaticamente sempre que uma ramificação de hotfix é criada em um AWS CodeCommit repositório.
- Restrições de acesso — Os desenvolvedores não têm acesso para criar esse pipeline fora do processo de hotfix.

- Estágio controlado — O pipeline tem um estágio controlado com um token de acesso especial, garantindo que uma pull request (PR) só possa ser criada uma vez.
- Estágios de aprovação — Os estágios de aprovação são incluídos no pipeline para obter as aprovações necessárias das partes interessadas relevantes.
- Exclusão automática — O pipeline de hotfix é excluído automaticamente sempre que uma `hotfix` ramificação é excluída no CodeCommit repositório após ser mesclada com um PR.

Pré-requisitos e limitações

Pré-requisitos

- Contas da AWS São necessários três ativos da seguinte forma:
  - Conta de ferramentas - Para configuração de integração contínua e entrega contínua (CI/CD).
  - Conta Stage - Para testes de aceitação do usuário.
  - Conta de produção - Para um usuário final comercial.
  - (Opcional) Adicione uma Conta da AWS para atuar como uma conta de controle de qualidade. Essa conta é necessária se você quiser uma configuração de pipeline principal, incluindo controle de qualidade, e uma solução de pipeline de hotfix para testes.
- Uma AWS CloudFormation pilha com uma condição opcional para ser implantada na conta de controle de qualidade usando o pipeline principal, se necessário. O padrão ainda pode ser testado sem a configuração do pipeline principal, criando e excluindo uma `hotfix` ramificação.
- Um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar CloudFormation os modelos usados para criar produtos do Service Catalog.
- Crie regras de aprovação de relações públicas para o CodeCommit repositório de acordo com os requisitos de conformidade (depois de criar o repositório).
- Restrinja as permissões do IAM de desenvolvedores e líderes de equipe para negar a execução da função Lambda prcreation-lambda, pois ela deve ser invocada somente a partir do pipeline.

Limitações

- O CloudFormation provedor é usado no estágio de implantação e o aplicativo é implantado usando um conjunto de CloudFormation alterações. Se você quiser usar uma opção de implantação diferente, modifique a CodePipeline pilha conforme necessário.

- Esse padrão usa outros arquivos AWS CodeBuild de configuração para implantar um microsserviço de amostra. Se você tiver um tipo de carga de trabalho diferente (por exemplo, cargas de trabalho sem servidor), deverá atualizar todas as configurações relevantes.
- Esse padrão implanta o aplicativo em um único lado Região da AWS (por exemplo, Leste dos EUA (Norte da Virgínia) us-east-1). Contas da AWS Para implantar em várias regiões, altere a referência da região em comandos e pilhas.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte os serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

Os diagramas nesta seção fornecem fluxos de trabalho para um evento de criação de ciclo de vida e para um evento de exclusão do ciclo de vida.

O diagrama anterior para criar um evento de ciclo de vida mostra o seguinte:

1. O desenvolvedor cria uma `hotfix-*` ramificação no CodeCommit repositório para desenvolver uma solução relacionada ao hotfix.
2. O evento de criação da `hotfix-*` ramificação é capturado por meio da EventBridge regra. Os detalhes do evento incluem o nome do repositório e o nome da ramificação.
3. A EventBridge regra invoca a AWS Lambda função. `hotfix-lambda-function` A EventBridge regra passa as informações do evento para a função Lambda como entrada.
4. A função Lambda processa a entrada para recuperar o nome do repositório e o nome da ramificação. Ele lança o produto Service Catalog com valores recuperados da entrada processada.
5. O produto Service Catalog inclui uma configuração de pipeline que implantará a solução nos ambientes de palco e produção. O bloco do pipeline inclui estágios de origem, construção e implantação. Além disso, há um estágio de aprovação manual para promover a implantação no ambiente de produção.
6. O estágio de origem recupera o código do repositório e da `hotfix-*` ramificação que foram criados na primeira etapa. O código é passado para o estágio de construção por meio de um bucket do Amazon S3 para artefatos. No estágio de construção, é criada uma imagem de contêiner que inclui o hotfix desenvolvido na `hotfix-*` filial e enviado para o Amazon Elastic Container Registry (Amazon ECR).

7. A fase de implantação no ambiente de estágio atualiza o Amazon Elastic Container Service (Amazon ECS) com a imagem de contêiner mais recente que inclui o hotfix. O hotfix é implantado criando e executando um CloudFormation conjunto de alterações.
8. A função `prcreation-lambda` Lambda é invocada após a implantação bem-sucedida no ambiente Stage. Essa função Lambda cria um PR da `hotfix-*` ramificação para as `main` ramificações `develop` e do repositório. A função Lambda garante que a correção desenvolvida na `hotfix-*` ramificação seja mesclada novamente e incluída nas implantações subsequentes.
9. Um estágio de aprovação manual ajuda a garantir que as partes interessadas necessárias revisem a correção e aprovem a implantação na produção.
10. O estágio de implantação no ambiente de produção atualiza o Amazon ECS com a imagem de contêiner mais recente que inclui o hotfix. O hotfix é implantado criando e executando um CloudFormation conjunto de alterações.

O diagrama anterior para excluir um evento de ciclo de vida mostra o seguinte:

1. O desenvolvedor exclui a `hotfix-*` ramificação após a implantação bem-sucedida do hotfix no ambiente de produção.
2. O evento de exclusão da `hotfix-*` ramificação é capturado por meio de uma EventBridge regra. Os detalhes do evento incluem o nome do repositório e o nome da ramificação.
3. A EventBridge regra invoca a função Lambda. A EventBridge regra passa as informações do evento para a função Lambda como entrada.
4. A função Lambda processa a entrada para recuperar o nome do repositório e o nome da ramificação. A função Lambda determina o respectivo produto do Service Catalog a partir da entrada passada e, em seguida, encerra o produto.
5. O encerramento do produto provisionado pelo Service Catalog exclui o pipeline e os recursos relevantes que foram criados anteriormente nesse produto.

Automação e escala

- O padrão inclui uma EventBridge regra e uma função Lambda, que podem lidar com várias solicitações de criação de ramificações de hotfix em paralelo. A função Lambda provisiona o produto Service Catalog para a regra de evento correspondente.

- A configuração do pipeline é feita usando o produto Service Catalog, que fornece recursos de controle de versão. A solução também se expande automaticamente para lidar com vários desenvolvimentos de hotfix para o mesmo aplicativo em paralelo.
- A função prcreation-lambda garante que essas alterações de hotfix também sejam mescladas novamente nas ramificações `main` e nas `develop` ramificações por meio de uma criação automática de pull request. Essa abordagem é essencial para manter as ramificações `main` e as `develop` ramificações atualizadas com todas as correções e evitar possíveis regressões de código. Esse processo ajuda a manter a consistência entre as ramificações e evitar regressões de código, garantindo que todas as ramificações de longa duração tenham as correções mais recentes.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeCommité um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem. AWS CodeCommit não está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Para obter mais informações, consulte Como migrar seu AWS CodeCommit repositório para outro provedor Git.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.

- AWS Service Catalogajuda você a gerenciar centralmente catálogos de serviços de TI aprovados. AWS Os usuários finais podem implantar rapidamente somente os serviços de TI aprovados de que precisam, seguindo as restrições definidas pela organização.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- AWS CloudFormation Linter (cfn-lint) é um linter que verifica os modelos CloudFormation YAML ou JSON em relação à especificação do recurso. CloudFormation Ele também executa outras verificações, como a verificação de valores válidos para as propriedades dos recursos e a adesão às melhores práticas.
- cfn-nag é uma ferramenta de código aberto que identifica possíveis problemas de segurança em CloudFormation modelos pesquisando padrões.
- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres. Esse padrão usa o Docker para compilar e testar imagens de contêiner localmente.
- O Git é um sistema de controle de versão distribuído e de código aberto.

Repositório de código

O código desse padrão está disponível no repositório GitHub dynamic_hotfix_codepipeline.

Práticas recomendadas

Revise e ajuste as funções do IAM e as políticas de controle de serviços (SCP) em seu ambiente para garantir que elas restrinjam o acesso de forma adequada. Isso é crucial para evitar quaisquer ações que possam anular as medidas de segurança incluídas nesse padrão. Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Configurar o ambiente de trabalho

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositório de amostra em um novo diretório em seu local de trabalho, execute o seguinte comando: `git clone git@github.com:aws-samples/dynamic_hotfix_codepipeline.git`	AWS DevOps
Exporte variáveis de ambiente para implantação CloudFormation de pilha.	Defina as seguintes variáveis de ambiente que serão usadas como entrada para as CloudFormation pilhas posteriormente nesse padrão. • `ApplicationName` — Essa variável é usada para nomear recursos criados para um aplicativo, facilitando o rastreamento deles. Use o comando a seguir, `Applicationname` substituindo-o pelo nome real do aplicativo: `export ApplicationName=<Applicationname>` • `BucketStartName` — Essa variável serve para nomear um bucket do	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Amazon S3. Os nomes dos buckets do S3 devem ser globalmente exclusivos em todos Contas da AWS. Use o comando a seguir, `BucketName` substituindo-o por um nome exclusivo para seu bucket do S3: `export BucketStartName=<BucketName>` • Números de conta e regiões — Essas variáveis armazenam Conta da AWS números de diferentes ambientes e da região de implantação. Use os comandos a seguir, substituindo os espaços reservados (como `prodaccountnumber eregion`) pelos Conta da AWS números reais e pelos Região da AWS que você está usando. **Note** `QAAccount` é opcional. Se você quiser usar`QAAccount`, configure-o usando os parâmetros da	

Tarefa	Descrição	Habilidades necessárias

	pilha principal do pipeline.
	
	`export ProdAccou nt=<prodaccountnum ber>`
	`export StageAcco unt=<stage/preprod accountnumber>`
	`export QAAccount =<qaccountnumber>`
	`export ToolsAcco unt=<toolsaccountn umber>`
	`export DepRegion =<region>`	

Configure os pré-requisitos necessários em Contas da AWS

Tarefa	Descrição	Habilidades necessárias

Crie os recursos necessários para CI/CD na conta de ferramentas.	Para implantar a CloudFormation pilha na conta de ferramentas, use os comandos a seguir. (Remova o `QAAccount` parâmetro se você não estiver usando a conta de controle de qualidade para configuração.)
	
	`#InToolsAccount`
	`aws cloudformation deploy \`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	``
	    --template-file
	 pre-requisites/pre-
	reqs.yaml \
	    --stack-name
	 prereqs \
	    --parameter-overri
	des BucketStartName=${
	BucketStartName} \
	    ApplicationName=
	${ApplicationName}
	 ProdAccount=${Prod
	Account} \
	    StageAccount=${Sta
	geAccount} ToolsAcco
	unt=${ToolsAccount} \
	    QAAccount=${QAAcco
	unt} \
	    --capabilities
	 CAPABILITY_IAM
	 CAPABILITY_NAMED_IAM
	 --region ${DepRegion}
	``
	
	Anote os recursos que o CodeCommit repositório e o Amazon ECR criaram a partir da pilha anterior. Esses parâmetros são necessários para configurar a `main` ramificação do pipeline nas próximas etapas.	

Tarefa	Descrição	Habilidades necessárias

Crie os recursos necessários para CI/CD nas contas de carga de trabalho.	1. Para empacotar o CloudFormation modelo em cada conta de carga de trabalho (estágio, produção e controle de qualidade opcional), use os comandos a seguir. No comando a seguir, `S3bucketpackage` substitua pelo nome do bucket do Amazon S3 que você deseja usar para empacotamento.
	
	`#InStageAccount`
	`aws cloudformation package \`
	`--template-file pre-requisites/infrastack.yaml \`
	`--s3-bucket <S3bucketpackage> \`
	`--s3-prefix infraStack \`
	`--region ${DepRegion} \`
	`--output-template-file pre-requisites/infrastructure_stage.template`
	
	`#InProdAccount`
	`aws cloudformation package \`
	`--template-file pre-requisites/infrastack.yaml \`
	`--s3-bucket <S3bucketpackage> \`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`--s3-prefix infraStack \ --region ${DepRegion} \ --output-template-file pre-requisites/infrastructure_prod.template`
	
	2. Para implantar o CloudFormation modelo em cada conta de carga de trabalho, use os seguintes comandos:
	
	`#InStageAccount aws cloudformation deploy --stack-name inframainstack \ --parameter-overrides Applicationame=${Applicationame} ToolsAccount=${ToolsAccount} DepRegion=${DepRegion} \ --template-file pre-requisites/infrastructure_stage.template --region ${DepRegion} --capabilities CAPABILITY_NAMED_IAM`
	
	`#InProdAccount aws cloudformation deploy --stack-name inframainstack \`	

Tarefa	Descrição	Habilidades necessárias
	`--parameter-overrides ApplicationName=${ApplicationName} ToolsAccount=${ToolsAccount} DepRegion=${DepRegion} \` `--template-file pre-requisites/infrastructure_prod.template --region ${DepRegion} --capabilities CAPABILITY_NAMED_IAM`	

Tarefa	Descrição	Habilidades necessárias

Atualize a política do bucket de artefatos do S3 para permitir o acesso às contas de carga de trabalho.	Para atualizar os pré-requisitos da CloudFormation pilha na conta de ferramentas, use os comandos a seguir para adicionar todas as permissões necessárias para as contas de carga de trabalho de estágio e produção. (Remova o `QAAccount` parâmetro se você não o estiver usando para configuração.)
	`#InToolsAccount`
	`aws cloudformation deploy \`
	`--template-file pre-requisites/pre-reqs.yaml \`
	`--stack-name prereqs \`
	`--parameter-overrides BucketStartName=${BucketStartName} \`
	`ApplicationName=${ApplicationName} ProdAccount=${ProdAccount} \`
	`StageAccount=${StageAccount} ToolsAccount=${ToolsAccount} \`
	`QAAccount=${QAAccount} PutPolicy=true \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`
		AWS DevOps

Configure a função Lambda e os recursos do Service Catalog na conta de ferramentas

Tarefa	Descrição	Habilidades necessárias

Configure o portfólio e os produtos do Service Catalog.	Para configurar o portfólio e os produtos do Service Catalog, faça o seguinte:
	
	1. Faça o upload dos modelos pipeline-main.yaml e pipeline-hotfix.yaml do repositório no diretório CodePipeline para um bucket existente do Amazon S3 () na região em que você deseja implantar (). `Bucketname` `DepRegion`
	
	`#InToolsAccount`
	`aws s3 cp ./codepip`
	`eline/pipeline-mai`
	`n.yaml s3://<Buc`
	`ketname>/pipeline-`
	`main.yaml`
	`aws s3 cp ./codepip`
	`eline/pipeline-hot`
	`fix.yaml s3://<Buc`
	`ketname>/pipeline-`
	`hotfix.yaml`
	
	2. Configure o portfólio e o produto do Service Catalog que gerenciarão o pipeline das `main` `hotfix` filiais. Anote os detalhes da `Outputs` seção para `MainProductId` e `MainProductArtifac`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`tId` da pilha a seguir. As informações são necessárias em etapas posteriores durante a configuração da tubulação da `main` filial.
	
	`#InToolsAccount`
	`aws cloudformation deploy \`
	`--template-file pre-requisites/servicecatalogsetup.yaml \`
	`--stack-name servicecatalogsetup \`
	`--parameter-overrides TemplateBucket=<Bucketname> \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`
	
	3. Forneça acesso a uma função do IAM que implantará recursos na conta de ferramentas no portfólio principal do pipeline do portfólio Service Catalog. Use esse portfólio para implantar o aplicativo usando a `main` ramificação. Para obter mais informações sobre como fornecer acesso, consulte Concedendo acesso aos	

Tarefa	Descrição	Habilidades necessárias
	usuários na documentação do Service Catalog.	

Tarefa	Descrição	Habilidades necessárias
Configure as funções do Lambda.	Essa solução usa as seguintes funções do Lambda para gerenciar fluxos de trabalho de hotfix: • `hotfix-lambda-function` manipula o provisionamento de produtos do Service Catalog quando uma `hotfix` ramificação é criada. • `hotfix-cleanup-lambda-function` gerencia o encerramento do produto quando uma `hotfix` filial é excluída. • `prcreation-lambda` cria pull requests da `hotfix` ramificação para a `develop` `main` ramificação e. Para permitir que as funções do Lambda provisionem e encerrem produtos do Service Catalog quando `hotfix` ramificações são criadas ou excluídas por meio da EventBridge regra associada, use as seguintes etapas: 1. Para criar as funções e permissões do IAM para as funções do Lambda, use o comando a seguir para	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	implantar uma CloudFormation pilha: `#InToolsAccount aws cloudformation deploy \ --template-file pre-requisites/lambdasetup.yaml \ --stack-name prsclambdasetup \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}` 2. Após a implantação da pilha, conceda o `hotfix-lambda-execution-role` acesso ao portfólio do pipeline de hotfix do portfólio Service Catalog usando o. AWS Management Console Esse acesso permite que a função Lambda inicie ou encerre o produto Service Catalog para filiais de hotfix.	

Crie um pipeline para a filial principal e implante o aplicativo em contas de carga de trabalho

Tarefa	Descrição	Habilidades necessárias
Configure o pipeline para a `main` filial.	Para configurar o pipeline para a ramificação principal, execute o comando a seguir	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	na conta de ferramentas. Substitua os parâmetros por `MainProductId` e `MainProductArtifactId` por valores das saídas da `servicecatalogsetup` pilha.
	
	`#InToolsAccount`
	`aws servicecatalog provision-product \`
	`--product-id <MainProductId> \`
	`--provisioning-artifact-id <MainProductArtifactId> \`
	`--provisioned-product-name "${ApplicationName}-main-pipeline" \`
	`--provisioning-parameters Key=CodeCommitRepoName,Value="${ApplicationName}-repository" Key=ECRRepository,Value="${ApplicationName}-app" \`
	`--region=${DepRegion}`	

Tarefa	Descrição	Habilidades necessárias
Implante o aplicativo usando a `main` ramificação.	1. Para clonar o CodeCommit repositório que foi criado nos pré-requisitos, use o comando. `git clone` Para obter mais informações, consulte Conectar-se ao CodeCommit repositório clonando o repositório conforme descrito na documentação. CodeCommit 2. Copie todos os arquivos do aplicativo do `repotemplates` diretório disponível no repositório para o clone () do seu repositório local. `${ApplicationName}-repository` Modifique os arquivos a seguir para atualizar o `ToolsAccount` ID. Em cada arquivo, localize o `RegistryAccountid` parâmetro e defina seu valor como seu `ToolsAccount` ID. Confirme as alterações no CodeCommit repositório e envie os arquivos para as `develop` ramificações `main` e para as ramificações. • ecs-configuration-prod.yaml • ecs-configuration-qa.yaml	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• ecs-configuration-stage.yaml 3. Para verificar a implantação do aplicativo, monitore a CodePipeline execução usando AWS Management Console o. Após a conclusão da implantação, acesse o aplicativo usando o FQDN do Application Load Balancer no ambiente de estágio. Confirme se o aplicativo funciona conforme o esperado. 4. Para aprovar a implantação para produção, use o CodePipeline console para localizar o pipeline do seu aplicativo. Encontre o `ApprovalToStart` palco. Analise as alterações e, se satisfatórias, forneça aprovação manual para continuar com a implantação da produção.	

Crie o pipeline para uma ramificação hotfix-* e implante o hotfix

Tarefa	Descrição	Habilidades necessárias
Crie uma `hotfix-*` ramificação e confirme as alterações.	Para criar um pipeline para a `hotfix-*` filial e implantar o hotfix nas contas de carga de trabalho, faça o seguinte:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	1. Crie uma ramificação usando um nome que comece com a palavra-chave`hotfix`. Por exemplo, esse padrão usa a `hotfix-check1` ramificação no repositório do CodeCommit aplicativo (`${ApplicationName}-repository`). Para obter etapas mais detalhadas, consulte Conectar a um AWS CodeCommit repositório e os comandos básicos do Git na CodeCommit documentação. 2. Verifique se o produto `Hotfix CICD Pipeline` Service Catalog foi provisionado dinamicamente com sucesso para a filial. `hotfix-check1` O nome do produto provisionado tem o nome dessa ramificação do hotfix e o nome do repositório do CodeCommit aplicativo. 3. Confirme algumas pequenas alterações no arquivo index.html e envie-as para o CodeCommit repositório.	

Tarefa	Descrição	Habilidades necessárias
	4. Verifique se a CodePipeline execução foi bem-sucedida no ambiente de palco. Para implantar no ambiente de produção, forneça aprovação manual em CodePipeline. 5. Confirme se as alterações estão visíveis na página inicial do aplicativo usando o nome de domínio totalmente qualificado (FQDN) do Application Load Balancer. O FQDN está disponível na `Outputs` seção de. `inframainstack-ALBStack-*`	
Exclua a `hotfix-check1` ramificação.	Para excluir a `hotfix-check1` ramificação criada anteriormente, faça o seguinte: 1. Exclua a `hotfix-check1` ramificação que está no repositório do CodeCommit aplicativo. 2. Verifique se o produto Service Catalog que foi provisionado para a `hotfix-check1` filial foi encerrado com êxito.	AWS DevOps

Limpar recursos

Tarefa	Descrição	Habilidades necessárias

Limpe os recursos implantados.	Para limpar os recursos que foram implantados anteriormente, faça o seguinte:
	1. Para reduzir o serviço Amazon ECS para zero réplicas nas contas de carga de trabalho, use o seguinte comando:
	`aws ecs update-service --cluster ${ApplicationName}-Cluster --service ${ApplicationName}-Service-stage --desired-count 0 --region ${DepRegion}`
	`aws ecs update-service --cluster ${ApplicationName}-Cluster --service ${ApplicationName}-Service-prod --desired-count 0 --region ${DepRegion}`
	2. Encerre o produto Service Catalog que foi provisionado para a filial. `main`
	3. Limpe objetos criados nos buckets do Amazon S3 na conta de ferramentas. Exclua todas as imagens do Docker no Amazon ECR
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	antes de excluir o registro em si.
	4. Remova as funções do IAM na seção de acesso concedido dos portfólios do Service Catalog antes de excluir o portfólio do Service Catalog.
	5. Exclua as CloudForm ation pilhas implantadas na conta de ferramentas e nas contas de carga de trabalho.
	
	`##In Tools Account##`
	`aws cloudformation delete-stack --stack-name servicecatalogsetup --region ${DepRegion}`
	`aws cloudformation delete-stack --stack-name prlambdasetup --region ${DepRegion}`
	`aws cloudformation delete-stack --stack-name prereqs --region ${DepRegion}`
	
	`##In Workload Accounts##`
	`aws cloudformation delete-stack --stack-name inframainstack --region ${DepRegion}`	

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte Excluindo produtos provisionados na documenta ção do Service Catalog.	

Solução de problemas

Problema	Solução
As alterações que você confirmou no CodeCommit repositório não estão sendo implantadas.	Verifique se há erros nos CodeBuild registros na ação de compilação do Docker. Para obter mais informações, consulte a documentação do CodeBuild .
O produto Service Catalog não está sendo provisionado.	Analise as CloudFormation pilhas relacionadas em busca de eventos com falha. Para obter mais informações, consulte a documentação do CloudFormation .

Recursos relacionados

- Comandos básicos do Git
- Configurar uma política do IAM para limitar os envios e mesclagens a uma ramificação
- Conecte-se a um AWS CodeCommit repositório
- Concedendo acesso aos usuários
- Enviando uma imagem do Docker para um repositório privado do Amazon ECR
- Solução de problemas AWS CodeBuild
- O que é AWS CodePipeline?

Mais informações

Esse padrão foi projetado para ambientes com uma configuração do Gitflow que é adotada para o fluxo de trabalho de desenvolvimento. A CI/CD process. The pipelines follow the deployment

cycle that starts from development and moves through quality assurance (QA), stage, and production environments. The CI/CD configuração inclui duas ramificações do git com implantações promocionais em ambientes da seguinte forma:

- A `develop` filial é implantada no ambiente de desenvolvimento.
- A `main` filial é implantada nos ambientes de controle de qualidade, estágio e produção.

Nessa configuração, é um desafio aplicar um hotfix ou um patch de segurança mais rápido do que o ciclo normal de implantação enquanto o desenvolvimento ativo de novos recursos está em andamento. É necessário um processo dedicado para atender às solicitações de hotfix ou segurança, garantindo que os ambientes ativos permaneçam funcionando adequadamente e seguros.

No entanto, você pode usar outras opções disponíveis sem precisar de um processo de implantação dedicado se:

- O CI/CD process is well-equipped with automated testing, such as functional and end-to-end tests, which eliminate the need for manual testing and prevent delays in deployments to production. However, if automated testing isn't well integrated into the CI/CD processo, a introdução de uma pequena correção no ambiente de produção, pode se tornar complexo e complicado para os desenvolvedores. Isso ocorre porque pode haver novos recursos aguardando aprovação e aprovação no ambiente de controle de qualidade. Um hotfix ou correção de segurança não pode ser colocado em produção de forma direta e simultânea.
- As equipes de desenvolvimento implantam continuamente novos recursos no ambiente de produção, integrando hotfixes ou patches de segurança na implantação programada de cada novo recurso. Em outras palavras, a próxima atualização de recursos para o ambiente de produção compreende dois componentes: a adição de um novo recurso e a inclusão do hotfix ou patch de segurança. No entanto, se o ciclo de implantação não for contínuo, pode haver vários novos recursos já aguardando aprovação no ambiente de controle de qualidade. Gerenciar versões diferentes e garantir que as alterações corretas sejam reaplicadas pode então se tornar complexo e propenso a erros.

> **Note**
>
> Se você estiver usando a versão 2 do AWS CodePipeline com os acionadores adequados configurados na `hotfix` ramificação, ainda precisará de um processo dedicado para atender às solicitações não programadas. Na versão 2, você pode configurar gatilhos para

solicitações push ou pull. A execução será colocada em fila ou executada imediatamente, dependendo do estado anterior do pipeline. No entanto, com um pipeline dedicado, as correções são aplicadas imediatamente ao ambiente de produção, garantindo que problemas urgentes sejam resolvidos sem demora.

Automatize a ingestão e a visualização de métricas personalizadas do Amazon MWAA no Amazon Managed Grafana usando o Terraform

Criado por Faisal Abdullah (AWS) e Satya Vajrapu (AWS)

Resumo

Esse padrão discute como usar o Amazon Managed Grafana para criar e monitorar métricas personalizadas que são ingeridas pelo Amazon Managed Workflows for Apache Airflow (Amazon MWAA). O Amazon MWAA serve como orquestrador de fluxos de trabalho, empregando Directed Acyclic Graphs () que são programados em Python. DAGs Esse padrão se concentra no monitoramento de métricas personalizadas, incluindo o número total de DAGs execuções na última hora, a contagem de aprovados e reprovados a DAGs cada hora e a duração média desses processos. Essa análise mostra como o Amazon Managed Grafana se integra ao Amazon MWAA para permitir monitoramento e insights abrangentes sobre a orquestração de fluxos de trabalho nesse ambiente.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS com as permissões de usuário necessárias para criar e gerenciar o seguinte Serviços da AWS:
  - AWS Identity and Access Management Funções e políticas (IAM)
  - AWS Lambda
  - Amazon Managed Grafana
  - Amazon Managed Workflows for Apache Airflow (Amazon MWAA)
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Timestream
- Acesso a um ambiente de shell que pode ser um terminal em sua máquina local ou AWS CloudShell.
- Um ambiente de shell com o Git instalado e a versão mais recente do AWS Command Line Interface (AWS CLI) instalada e configurada. Para obter mais informações, consulte Instalação ou atualização para a versão mais recente do AWS CLI na AWS CLI documentação.
- A seguinte versão do Terraform instalada: `required_version = ">= 1.6.1, < 2.0.0"` Você pode usar o tfswitch para alternar entre diferentes versões do Terraform.

- Fonte de identidade configurada AWS IAM Identity Center para o seu Conta da AWS. Para obter mais informações, consulte Confirme suas fontes de identidade no IAM Identity Center na documentação do IAM Identity Center. Você pode escolher entre o Active Directory padrão Diretório do Centro de Identidade do IAM ou um provedor de identidade externo (IdP), como o Okta. Para obter mais informações, consulte Recursos relacionados.

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- Terraforma `required_version = ">= 1.6.1, < 2.0.0"`
- Amazon Managed Grafana versão 9.4 ou posterior. Esse padrão foi testado na versão 9.4.

Arquitetura

O diagrama de arquitetura a seguir destaca o Serviços da AWS usado na solução.

O diagrama anterior percorre o seguinte fluxo de trabalho:

1. As métricas personalizadas no Amazon MWAA se originam das DAGs que estão sendo executadas no ambiente. As métricas são carregadas no bucket do Amazon S3 em formato de arquivo CSV. O seguinte DAGs usa os recursos de consulta de banco de dados do Amazon MWAA:
   - `run-example-dag`— Esse DAG contém um exemplo de código Python que define uma ou mais tarefas. Ele é executado a cada 7 minutos e imprime a data. Depois de imprimir a data, o DAG inclui uma tarefa para suspender ou pausar a execução por um período específico.
   - `other-sample-dag`— Este DAG é executado a cada 10 minutos e imprime a data. Depois de imprimir a data, o DAG inclui uma tarefa para suspender ou pausar a execução por um período específico.

- `data-extract`— Esse DAG é executado a cada hora e consulta o banco de dados Amazon MWAA e coleta métricas. Depois que as métricas são coletadas, esse DAG as grava em um bucket do Amazon S3 para processamento e análise adicionais.

2. Para agilizar o processamento de dados, as funções do Lambda são executadas quando são acionadas por eventos do Amazon S3, o que facilita o carregamento de métricas no Timestream.
3. O Timestream é integrado como uma fonte de dados no Amazon Managed Grafana, onde todas as métricas personalizadas do Amazon MWAA são armazenadas.
4. Os usuários podem consultar os dados e criar painéis personalizados para visualizar os principais indicadores de desempenho e obter informações sobre a orquestração dos fluxos de trabalho no Amazon MWAA.

Ferramentas

Serviços da AWS

- AWS IAM Identity Centerajuda você a gerenciar centralmente o acesso de login único (SSO) a todos os seus Contas da AWS aplicativos e à nuvem.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado. Nesse padrão, AWS Lambda executa o código Python em resposta aos eventos do Amazon S3 e gerencia os recursos computacionais automaticamente.
- O Amazon Managed Grafana é um serviço de visualização de dados totalmente gerenciado que você pode usar para consultar, correlacionar, visualizar e alertar sobre suas métricas, registros e rastreamentos. Esse padrão usa o Amazon Managed Grafana para criar um painel para visualização de métricas e alertas.
- O Amazon Managed Workflows for Apache Airflow (Amazon MWAA) é um serviço gerenciado de orquestração para o Apache Airflow que você pode usar para configurar e operar pipelines de dados na nuvem em grande escala. O Apache Airflow é uma ferramenta de código aberto usada para criar, agendar e monitorar programaticamente sequências de processos e tarefas chamadas de fluxos de trabalho. Nesse padrão, a amostra DAGs e um extrator de métricas DAG são implantados no Amazon MWAA.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade

de dados. Nesse padrão, o Amazon S3 é usado para armazenar DAGs scripts e métricas personalizadas no formato CSV.

- O Amazon Timestream LiveAnalytics for is é um banco de dados de séries temporais rápido, escalável, totalmente gerenciado e criado especificamente para facilitar o armazenamento e a análise de trilhões de pontos de dados de séries temporais por dia. O Timestream for LiveAnalytics também se integra aos serviços comumente usados para coleta de dados, visualização e aprendizado de máquina. Nesse padrão, ele é usado para ingerir as métricas personalizadas geradas pelo Amazon MWAA.

Outras ferramentas

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem. Esse padrão usa um módulo Terraform para automatizar o provisionamento da infraestrutura em. AWS

Repositório de código

O código desse padrão está disponível GitHub no repositório visualize-amazon-mwaa-custom-metrics-grafana. A `stacks/Infra` pasta contém o seguinte:

- Arquivos de configuração do Terraform para todos os recursos AWS
- Arquivo.json do painel Grafana na pasta `grafana`
- Amazon Managed Workflows para Apache Airflow DAGs na pasta `mwaa/dags`
- Código Lambda para analisar o arquivo.csv e armazenar métricas no banco de dados Timestream na pasta `src`
- Arquivos.json da política do IAM na pasta `templates`

Práticas recomendadas

O Terraform deve armazenar o estado sobre sua infraestrutura e configuração gerenciadas para que possa mapear recursos do mundo real para sua configuração. Por padrão, o Terraform armazena o estado localmente em um arquivo chamado`terraform.tfstate`. É crucial garantir a segurança e a integridade do seu arquivo de estado do Terraform, pois ele mantém o estado atual da sua infraestrutura. Para obter mais informações, consulte Remote State na documentação do Terraform.

Épicos

Implemente a infraestrutura usando o Terraform

Tarefa	Descrição	Habilidades necessárias

Implantar a infraestrutura.	Para implantar a infraestrutura da solução, faça o seguinte:
	1. Abra um terminal ou prompt de comando em seu computador local ou usando AWS CloudShell.
	2. Navegue até o diretório em que você deseja clonar o repositório.
	3. Para clonar o repositór io, execute o seguinte comando:
	`git clone https://g ithub.com/aws-samp les/visualize-amaz on-mwaa-custom-met rics-grafana`
	4. Depois que o processo de clonagem for concluído , execute o comando a seguir para navegar até o diretório do repositório clonado:
	`cd visualize-amazon-m waa-custom-metrics- grafana/stacks/infra`
	5. Para baixar e inicializar os provedores necessári
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	os, execute o seguinte comando:
	`terraform init`
	6. Para obter uma visão abrangente de todos os recursos que o Terraform criará, execute o seguinte comando:
	`terraform plan`
	O Terraform fornece os seguintes recursos:
	• Amazon Virtual Private Cloud (Amazon VPC) e componentes de rede associados
	• Recursos do Amazon S3
	• AWS Lambda funções
	• Recursos do Amazon Managed Grafana (espaço de trabalho, painéis, fonte de dados)
	• Suporte aos recursos do IAM (funções e políticas)
	7. Para criar os AWS recursos a partir da saída do plano, execute o seguinte comando:
	`terraform apply -auto-approve`	

Tarefa	Descrição	Habilidades necessárias
	O provisionamento da infraestrutura é concluído em aproximadamente 20 minutos. 8. Para criar os AWS recursos especificados de acordo com a configuração definida nos seus arquivos do Terraform, execute o seguinte comando: `terraform apply`	

Valide os recursos de infraestrutura implantados

Tarefa	Descrição	Habilidades necessárias
Valide o ambiente Amazon MWAA.	Para validar o ambiente Amazon MWAA, faça o seguinte: 1. Faça login no AWS Management Console, navegue até o console do painel do Amazon MWAA e selecione Open Airflow UI. 2. Você deve ver os três seguintes DAGs no status Ativo: • extração de dados • run-example-dag • other-sample-dag	AWS DevOps, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	3. Se um DAG não estiver ativo, você poderá ativá-lo ativando a chave seletora ao lado do nome do DAG.	
Verifique as programações do DAG.	Para ver cada programaç ão do DAG, acesse a guia Programação na interface do Airflow. Cada um dos itens a seguir DAGs tem uma programaç ão pré-configurada, que é executada no ambiente Amazon MWAA e gera métricas personalizadas: • run-example-dag- Funciona a cada 7 minutos • other-sample-dag- Funciona a cada 10 minutos • extração de dados - É executado a cada hora Você também pode ver as execuções bem-sucedidas de cada DAG na coluna Execuções.	Engenheiro de dados, AWS DevOps

Configurar o ambiente Amazon Managed Grafana

Tarefa	Descrição	Habilidades necessárias
Configure o acesso ao espaço de trabalho Amazon Managed Grafana.	Os scripts do Terraform criaram o espaço de trabalho, os painéis e a página de métricas necessários do Amazon Managed Grafana. Para configurar o acesso para que você possa visualizá-los, faça o seguinte: 1. Abra o console do Amazon Managed Grafana. 2. Em Espaços de trabalho, selecione o espaço de trabalho e `grafana-ws-dev` navegue até a guia Autenticação no painel inferior. 3. Escolha o botão Atribuir novo usuário ou grupo. 4. Adicione seu grupo na guia Grupos ou um usuário na guia Usuários e escolha o botão Atribuir usuários e grupos. 5. Depois que o usuário (ou grupo) for adicionado, transforme esse usuário (ou grupo) em administr ador. Selecione o usuário em Usuários ou grupos atribuídos na guia Grupo de usuários atribuídos e	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	escolha Tornar administrador no menu suspenso. Para obter mais informações, consulte Use AWS IAM Identity Center com seu espaço de trabalho Amazon Managed Grafana na documentação do Amazon Managed Grafana. 6. Navegue até Espaços de trabalho e escolha a URL do espaço de trabalho Grafana. Para entrar no Amazon Managed Grafana como administrador, escolha Entrar com. AWS IAM Identity Center	

Tarefa	Descrição	Habilidades necessárias
Instale o plug-in Amazon Timestream.	As métricas personalizadas do Amazon MWAA são carregadas no banco de dados Timestream. Você usa o plug-in Timestream para visualizar as métricas com os painéis Amazon Managed Grafana. Para instalar o plug-in Timestream, faça o seguinte: 1. No console Amazon Managed Grafana, expanda o menu no painel de navegação esquerdo e acesse Administração, Plugins. 2. Pesquise e instale a versão mais recente do plug-in Amazon Timestream. 3. Depois que o plug-in for instalado, acesse Administração, Fontes de dados para ver a fonte de dados Timestream. Se a fonte de dados não estiver listada, atualize a página. Para obter mais informações, consulte Estender seu espaço de trabalho com plug-ins na documentação do Amazon Managed Grafana.	AWS DevOps, DevOps engenheiro

Visualize as métricas personalizadas no painel Amazon Managed Grafana

Tarefa	Descrição	Habilidades necessárias
Veja o painel Amazon Managed Grafana.	Para visualizar as métricas que foram ingeridas no espaço de trabalho Amazon Managed Grafana, faça o seguinte: 1. No console Amazon Managed Grafana, escolha Painéis no painel de navegação esquerdo. 2. Para visualizar as métricas, escolha painéis de eventos do MWAA e selecione mwaa_metrics. A página de métricas do painel mostra as seguintes informações: • O DAG total é executado na última hora • Total de execuções do DAG bem-sucedidas, malsucedidas e em execução na última hora • Duração média de todas as execuções bem-sucedidas e malsucedidas do DAG	AWS DevOps
Personalize o painel Amazon Managed Grafana.	Para personalizar os painéis para futuros aprimoramentos, faça o seguinte:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	1. Na `mwaa_metrics` página do painel Amazon Managed Grafana, escolha o ícone de configurações do painel. 2. Para visualizar a estrutura de dados que define o painel, escolha o modelo JSON. Você pode personalizar o painel fazendo edições nesse modelo JSON diretamente no console. Como alternativa, o código-fonte desse painel está disponível no `dashboard.json` arquivo na `stacks/infra/grafana` pasta no GitHub repositório.	

Limpe AWS os recursos

Tarefa	Descrição	Habilidades necessárias
Pausa a execução do Amazon MWAA DAG.	Para pausar a execução do DAG, faça o seguinte: 1. No console do Amazon MWAA, navegue até os ambientes do Airflow e escolha Open Airflow UI.	AWS DevOps, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	2. Para pausar o DAG, use a chave seletora ao lado de cada DAG. 3. Atualize a página da interface do Airflow, que deve listar três DAGs na seção Pausado.	
Exclua os objetos nos buckets do Amazon S3.	Para excluir os buckets mwaa-events-bucket-* e mwaa-metrics-bucket-* do Amazon S3, siga as instruções para usar o console do Amazon S3 em Excluindo um bucket na documentação do Amazon S3.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Destrua os recursos criados pelo Terraform.	Para destruir os recursos criados pelo Terraform e o arquivo de estado local associado do Terraform, faça o seguinte: 1. (Opcional) Antes de excluir os recursos, você pode visualizar as alterações que o Terraform fará. Para gerar um plano, execute o seguinte comando: `terraform plan -destroy` A saída do comando mostra que o `destroy` comando excluirá todos os AWS recursos que foram criados anteriormente. 2. `terraform destroy -auto-approve` Esse comando leva aproximadamente 20 minutos para destruir a infraestrutura. **Note** Para destruir todos os recursos gerenciados pelo Terraform, execute	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	o comando a seguir. : a `-auto-approve` tag não espera a confirmação do usuário para começar a destruir os recursos.
	3. Para excluir o arquivo de estado local do Terraform , execute os seguintes comandos:
	`rm .terraform.lock.hcl`
	`rm -rf .terraform`
	`rm terraform.tfstate*`	

Solução de problemas

Problema	Solução
`null_resource.plugin_mgmt (local-exec): aws: error: argument operation: Invalid choice, valid choices are:`	Atualize seu AWS CLI para a versão mais recente.
Erro ao carregar fontes de dados - `Fetch error: 404 Not Found Instantiating…`	O erro é intermitente. Aguarde alguns minutos e, em seguida, atualize suas fontes de dados para visualizar a fonte de dados Timestream listada.

Recursos relacionados

AWS documentação

- Amazon Managed Grafana para criação de painéis e visualização
- Configurar o Amazon Managed Grafana para usar o Okta
- Use AWS IAM Identity Center com seu espaço de trabalho Amazon Managed Grafana
- Trabalhando com o DAGs Amazon MWAA

AWS vídeos

- Configure o IAM Identity Center com o Amazon Managed Grafana para autenticação, conforme mostrado no vídeo a seguir.

https://www.youtube-nocookie.com/embed/XX2Xcz-PS9U? controles = 0

- Se o IAM Identity Center não estiver disponível, você também pode integrar a autenticação Amazon Managed Grafana usando um provedor de identidade externo (IdP), como o Okta, conforme mostrado no vídeo a seguir.

https://www.youtube-nocookie.com/embed/A4 OuJHxl2xp? controles = 0

Mais informações

Você pode criar uma solução abrangente de monitoramento e alerta para seu ambiente Amazon MWAA, permitindo gerenciamento proativo e resposta rápida a possíveis problemas ou anomalias. O Amazon Managed Grafana inclui os seguintes recursos:

Alertas — Você pode configurar alertas no Amazon Managed Grafana com base em limites ou condições predefinidos. Configure notificações por e-mail para alertar as partes interessadas relevantes quando determinadas métricas excederem ou ficarem abaixo dos limites especificados. Para obter mais informações, consulte o alerta do Grafana na documentação do Amazon Managed Grafana.

Integração — Você pode integrar o Amazon Managed Grafana com várias ferramentas de terceiros OpsGenie, como, PagerDuty, ou o Slack para melhorar os recursos de notificação. Por exemplo, você pode configurar webhooks ou integrá-los APIs para acionar incidentes e notificações nessas plataformas com base nos alertas gerados no Amazon Managed Grafana. Além disso, esse padrão

fornece um GitHub repositório para criar AWS recursos. Você pode integrar ainda mais esse código aos seus fluxos de trabalho de implantação de infraestrutura.

Simplifique o desenvolvimento e a implantação de bots do Amazon Lex usando um fluxo de trabalho automatizado

Criado por Balaji Panneerselvam (AWS), Anand Jumnani (AWS), Attila Dancso (AWS), James O'Hara (AWS) e Pavan Dusanapudi (AWS)

Resumo

Desenvolver e implantar bots conversacionais do Amazon Lex pode ser um desafio quando você está tentando gerenciar vários recursos, desenvolvedores e ambientes. Um fluxo de trabalho automatizado usando princípios de infraestrutura como código (IaC) pode ajudar a agilizar o processo. Esse padrão pode ajudar a melhorar a produtividade dos desenvolvedores do Amazon Lex e permitir o gerenciamento eficiente do ciclo de vida dos bots das seguintes formas:

- Permita o desenvolvimento simultâneo de vários recursos - Com um fluxo de trabalho automatizado, os desenvolvedores podem trabalhar em diferentes recursos paralelamente em ramificações separadas. As alterações podem então ser mescladas e implantadas sem bloquear outros trabalhos.
- Use a interface de usuário do console Amazon Lex — Os desenvolvedores podem usar o console fácil de usar do Amazon Lex para criar e testar bots. Os bots são então descritos no código de infraestrutura para implantação.
- Promova bots em todos os ambientes - O fluxo de trabalho automatiza a promoção de versões de bots de ambientes inferiores, como desenvolvimento e teste até a produção. Essa abordagem reduz o risco e a sobrecarga das promoções manuais.
- Mantenha o controle de versão - O gerenciamento das definições de bots no Git, em vez de apenas por meio do serviço Amazon Lex, fornece controle de versão e uma trilha de auditoria. As alterações são rastreadas para desenvolvedores individuais, ao contrário de quando usamos apenas os bots armazenados AWS Management Console ou APIs modificados AWS.

Ao automatizar o processo de lançamento de bots do Amazon Lex, as equipes podem fornecer recursos mais rapidamente com menos risco e esforço. Os bots permanecem sob controle de versão em vez de isolados no console do Amazon Lex.

Pré-requisitos e limitações

Pré-requisitos

- O fluxo de trabalho envolve vários Contas da AWS ambientes diferentes (desenvolvimento, produção e DevOps), o que requer gerenciamento de contas e configurações de acesso entre contas.
- Python 3.9 disponível em seu ambiente de implantação ou pipeline.
- Git instalado e configurado em uma estação de trabalho local para controle de origem.
- AWS Command Line Interface (AWS CLI) instalado e configurado para autenticação usando a linha de comando ou o Python.

Limitações

- Acesso ao repositório — O fluxo de trabalho pressupõe que o pipeline de integração contínua e entrega contínua (CI/CD) tenha as permissões necessárias para confirmar as alterações no repositório do código-fonte.
- Versão inicial do bot — As ferramentas exigem que uma versão inicial do bot seja implantada usando AWS CloudFormation modelos. Você deve criar a primeira iteração do bot e confirmá-la no repositório antes que o fluxo de trabalho automatizado possa assumir o controle.
- Conflitos de mesclagem — Embora o fluxo de trabalho tenha como objetivo permitir o desenvolvimento simultâneo, ainda existe a possibilidade de conflitos de mesclagem ao integrar alterações de diferentes ramificações. A resolução de conflitos nas configurações de bots pode exigir intervenção manual.

Versões do produto

- Python 3.9 ou superior
- AWS CDK v2 2.124.0 ou superior
- AWS SDK para Python (Boto3)1,28 ou superior

Arquitetura

O diagrama a seguir mostra a arquitetura de alto nível e os principais componentes da solução.

Os principais componentes incluem o seguinte:

- Lex bot repo — Um repositório Git que armazena as definições de IaC para os bots Amazon Lex.

- DevOps— Um Conta da AWS dedicado a abrigar os dutos de CI/CD e os recursos relacionados para o processo de desenvolvimento e implantação.
- Pipelines — As AWS CodePipeline instâncias que automatizam vários estágios do ciclo de vida de desenvolvimento e implantação de bots, como criar um novo bot, exportar a definição de um bot, importar uma definição de bot e excluir um bot.
- Bots de tickets e bot principal — Os recursos de bots do Amazon Lex, em que os bots de tickets são bots de recursos específicos desenvolvidos por equipes ou desenvolvedores individuais e o bot principal é o bot básico que integra todos os recursos.

O diagrama da arquitetura ilustra o seguinte fluxo de trabalho:

1. Bot principal de linha de base — O ponto de partida do fluxo de trabalho é definir a linha de base do bot principal no ambiente de desenvolvimento (Dev). O bot principal serve como base para futuros desenvolvimentos e adições de recursos.
2. Criar bot de ticket — Quando um novo recurso ou alteração é necessário, um bot de ticket é criado. O bot de tickets é essencialmente uma cópia ou ramificação do bot principal em que os desenvolvedores podem trabalhar sem afetar a versão principal.
3. Bot de exportação de tíquetes - Depois que o trabalho no bot de tíquetes estiver concluído, ele será exportado do serviço Amazon Lex. Em seguida, a ramificação que contém o bot do ticket é realocada a partir da ramificação principal. Essa etapa garante que todas as alterações feitas no bot principal enquanto o bot do ticket estava em desenvolvimento sejam incorporadas, reduzindo possíveis conflitos.
4. Importar bot de ticket rebaseado e validar — O bot de ticket rebaseado é importado de volta para o ambiente de desenvolvimento e validado para garantir que funcione corretamente com as alterações mais recentes da ramificação principal. Se a validação for bem-sucedida, uma pull request (PR) será criada para mesclar as alterações do bot do ticket na ramificação principal.
5. Excluir bot de ticket — Depois que as alterações forem mescladas com sucesso na ramificação principal, o bot de ticket não será mais necessário. O bot do ticket pode ser excluído para manter o ambiente limpo e gerenciável.
6. Implante o bot principal no ambiente de desenvolvimento e teste — O bot principal atualizado, agora incluindo os novos recursos ou alterações, é implantado no ambiente de desenvolvimento. Aqui, ele passa por testes completos para garantir que todas as funcionalidades funcionem conforme o esperado.
7. Implantar o bot principal no ambiente de produção — Depois que os testes no ambiente de desenvolvimento forem concluídos e bem-sucedidos, o bot principal será implantado no ambiente

de produção. Essa etapa é a etapa final do fluxo de trabalho, na qual os novos recursos ficam disponíveis para os usuários finais.

Automação e escala

O fluxo de trabalho automatizado permite que os desenvolvedores trabalhem paralelamente em diferentes recursos, cada um em ramificações separadas. Isso facilita o desenvolvimento simultâneo, permitindo que as equipes colaborem de forma eficaz e forneçam recursos com mais rapidez. Com filiais isoladas umas das outras, as mudanças podem ser mescladas e implantadas sem bloquear ou interferir em outros trabalhos em andamento.

O fluxo de trabalho automatiza a implantação e a promoção de versões de bots em diferentes ambientes, como desenvolvimento, teste e produção.

Armazenar definições de bots em um sistema de controle de versão como o Git fornece uma trilha de auditoria abrangente e permite uma colaboração eficiente. As mudanças são rastreadas para desenvolvedores individuais, garantindo transparência e responsabilidade em todo o ciclo de vida do desenvolvimento. Essa abordagem também facilita as revisões de código, permitindo que as equipes identifiquem e resolvam problemas antes da implantação na produção.

Usando AWS CodePipeline e outros Serviços da AWS, o fluxo de trabalho automatizado pode ser escalado para acomodar o aumento das cargas de trabalho e do tamanho das equipes.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software de código aberto para definir Nuvem AWS infraestrutura em código usando linguagens de programação familiares e provisionando-a por meio dela. AWS CloudFormation O exemplo de implementação nesse padrão usa Python.
- AWS CDK Interface de linha de comando (AWS CDK CLI) - O AWS CDK kit de ferramentas é a principal ferramenta para interagir com seu aplicativo. AWS CDK Ele executa seu aplicativo, interroga o modelo de aplicativo que você definiu e produz e implanta os AWS CloudFormation modelos gerados pelo CDK.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS Esse padrão é usado CloudFormation para implantar as configurações de bots do Amazon Lex e os recursos relacionados usando a infraestrutura como código.

- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação. Esse padrão é usado CodeBuild para criar e empacotar os artefatos de implantação.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente. Esse padrão é usado CodePipeline para orquestrar o pipeline de entrega contínua.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Lex V2 serve AWS service (Serviço da AWS) para criar interfaces conversacionais (bots) para aplicativos usando voz e texto.
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS

Outras ferramentas

- O Git é um sistema de controle de versão distribuído de código aberto.

Repositório de código

O código desse padrão está disponível no repositório GitHub management-framework-sample-for-amazon-lex. O repositório de códigos contém as seguintes pastas e arquivos:

- `prerequisite`pasta — Contém definições de CloudFormation pilha (usando o AWS CDK) para configurar os recursos e ambientes necessários.
- `prerequisite/lexmgmtworkflow`folder — Diretório principal do projeto Lex Management Workflow, incluindo definições de pilha e código Python.
- `prerequisite/tests`— Contém testes unitários.
- `src`pasta — Diretório de código-fonte, incluindo o wrapper e utilitários de gerenciamento de bots do Amazon Lex.

- `src/dialogue_lambda`— Diretório de código-fonte da função Lambda do gancho de diálogo que intercepta e processa as entradas do usuário durante uma conversa com um bot do Amazon Lex.

Práticas recomendadas

- Separação de preocupações
  - Mantenha uma separação clara de responsabilidades entre DevOps os ambientes de desenvolvimento e produção.
  - Use separadamente Contas da AWS para cada ambiente para impor limites adequados de isolamento e segurança.
  - Use funções entre contas e princípios de acesso com privilégios mínimos para garantir o acesso controlado entre ambientes.
- Infraestrutura como código
  - Revise e atualize regularmente o código da infraestrutura para se alinhar às melhores práticas e aos requisitos em evolução.
  - Estabeleça uma estratégia clara de ramificação e mesclagem para o repositório de código-fonte
- Teste e validação
  - Implemente testes automatizados em vários estágios do pipeline para detectar problemas no início do ciclo de desenvolvimento.
  - Use o console Amazon Lex ou estruturas de teste automatizadas para validar as configurações e a funcionalidade do bot antes de promovê-lo para ambientes superiores.
  - Considere a implementação de portas de aprovação manual para implantações em ambientes críticos ou de produção.
- Monitoramento e registro
  - Configure mecanismos de monitoramento e registro para os pipelines, implantações e interações de bots.
  - Monitore eventos de pipeline, status de implantação e métricas de desempenho de bots para identificar e resolver problemas imediatamente.
  - Use serviços da AWS, como Amazon CloudWatch, AWS CloudTrail, e AWS X-Ray para registro e monitoramento centralizados.
  - Revise e analise regularmente o desempenho, a eficiência e a eficácia do fluxo de trabalho automatizado.
- Segurança e conformidade

- Implemente práticas seguras de codificação e siga as melhores práticas AWS de segurança para o desenvolvimento e a implantação de bots do Amazon Lex.
- Analise e atualize regularmente as funções, políticas e permissões do IAM para se alinhar ao princípio do menor privilégio.
- Considere integrar a verificação de segurança e as verificações de conformidade aos pipelines.

Épicos

Configure o IaC para o gerenciamento de bots do Amazon Lex

Tarefa	Descrição	Habilidades necessárias

Configure o ambiente CDK local.	1. Para clonar o repositório desse padrão e navegar até o `prerequisite` diretório, execute o seguinte comando:
	`git clone https://github.com/aws-samples/management-framework-sample-for-amazon-lex.git`
	`cd management-framework-sample-for-amazon-lex`
	2. Para instalar e ativar o ambiente virtual Python, execute o seguinte comando que instala as dependências do CDK localmente na pasta do projeto, em vez de globalmente:
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`pip install virtualenv`
	`python<version> -m venv .venv`
	`source .venv/bin/activate`
	`python -m pip install -r requirements.txt`	

Crie uma função entre contas no `devops` ambiente.	A `devops` conta é responsável por hospedar e gerenciar os CI/CD pipelines. To enable the CI/CD pipelines para interagir com os `dev` `prod` ambientes. Execute os comandos a seguir para criar uma função entre contas na `devops` conta.
	`cdk bootstrap --profile=devops`
	
	`cdk deploy LexMgmtDevopsRoleStack -c dev-account-id=222222222222 -c prod-account-id=333333333333 --profile=devops`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Crie uma função entre contas no `dev` ambiente.	Crie uma função do IAM na `dev` conta com as permissões necessárias para permitir que a `devops` conta assuma essa função. O pipeline de CI/CD usa essa função para realizar ações na `dev` conta, como implantar e gerenciar recursos de bots do Amazon Lex.
	
	Para criar a função do IAM, execute os seguintes comandos:
	
	`cdk bootstrap --profile =dev`
	
	`cdk deploy LexMgmtCr ossaccountRoleStac k -c devops-account- id=1111111111111 -- profile=dev`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Crie uma função entre contas no `prod` ambiente.	Crie uma função do IAM na `prod` conta com as permissões necessárias para permitir que a `devops` conta assuma essa função. O pipeline de CI/CD usa essa função para realizar ações na `prod` conta, como implantar e gerenciar recursos de bots do Amazon Lex.
	`cdk bootstrap --profile =prod`
	
	`cdk deploy LexMgmtCr ossaccountRoleStac k -c devops-account- id=1111111111111 -- profile=prod`
		AWS DevOps

Crie pipelines no `devops` ambiente.	Para gerenciar o fluxo de trabalho de desenvolvimento dos bots do Amazon Lex, execute o comando a seguir para configurar pipelines no `devops` ambiente. `cdk deploy LexMgmtWo rkflowStack -c devops- account-id=111111111 1111 -c dev-account- id=2222222222222 -c prod-account-id=33 3333333333 --profile =devops`	AWS DevOps

Estabeleça a linha de base para o bot principal

Tarefa	Descrição	Habilidades necessárias
Defina a versão inicial do bot principal.	Para definir a versão inicial do bot principal, acione o `BaselineBotPipeline` pipeline. O pipeline implanta a definição básica de bot definida no CloudFormation modelo, exporta a definição principal do bot como arquivos.json e armazena o código principal do bot em um sistema de controle de versão.	AWS DevOps

Implemente o fluxo de trabalho de desenvolvimento de recursos

Tarefa	Descrição	Habilidades necessárias
Crie o bot de tickets para desenvolver e testar um recurso.	`TicketBot` é uma nova instância de bot importada da definição de bot principal existente na ramificação de recursos. Essa abordagem garante que o novo bot tenha todas as funcionalidades e configurações atuais do bot principal. Para definir a versão inicial do bot de tickets, acione o `CreateTicketBotPipeline` pipeline.	Desenvolvedor Lex Bot

Tarefa	Descrição	Habilidades necessárias
	O pipeline cria uma nova ramificação de recursos no sistema de controle de versão e cria uma nova instância de bot de tickets com base no bot principal.	
Desenvolva e teste o recurso de bot de tickets.	Para desenvolver e testar o recurso, faça login AWS Management Console e abra o console do Amazon Lex em https://console.aws.amazon.com/lex/. Para obter mais informações, consulte Testando um bot usando o console na documentação do Amazon Lex. Com a `TicketBot` instância, agora você pode adicionar, modificar ou estender a funcionalidade do bot para implementar o novo recurso. Por exemplo, você pode criar ou modificar intenções, enunciados, slots e fluxos de diálogo. Para obter mais informações, consulte Adicionar intenções na documentação do Amazon Lex.	Desenvolvedor Lex Bot

Tarefa	Descrição	Habilidades necessárias
Exporte a definição do bot de tickets.	A definição de bot exportada é essencialmente uma represent ação da configuração e funcionalidade do bot em formato JSON. Para exportar a definição do bot de tickets, acione o `ExportTicketBotPip eline` pipeline. O pipeline exporta a definição do bot de ticket como arquivos.json e armazena o código do bot de ticket em uma ramificação de recursos no sistema de controle de versão.	Desenvolvedor Lex Bot

Tarefa	Descrição	Habilidades necessárias
Rebaseie a ramificação de recursos a partir da ramificação principal mais recente.	Durante o desenvolvimento de um novo recurso, a ramificação principal pode ter recebido outras alterações de diferentes desenvolvedores ou equipes. Para incorporar essas alterações na ramificação de recursos, execute uma operação Git`rebase`. Essa operação basicamente reproduz as confirmações da ramificação de recursos em cima das confirmações mais recentes da ramificação principal, garantindo que a ramificação de recursos inclua todas as alterações mais recentes.	Desenvolvedor Lex Bot

Tarefa	Descrição	Habilidades necessárias
Importe e valide o bot de tíquetes rebaseado.	Depois de realocar a ramificação do recurso, você deve importá-la para a instância do ticket bot. Essa importação atualiza o bot de tickets existente com as alterações mais recentes da ramificação reformulada. Para importar o bot de tickets reformulado, acione o `ImportTicketBotPipeline` pipeline. O pipeline importa os arquivos.json de definição do bot de ticket na ramificação de recursos do sistema de controle de versão para a `TicketBot` instância.	Desenvolvedor Lex Bot

Tarefa	Descrição	Habilidades necessárias
Valide a definição de bot reformulada.	Depois de importar a definição de bot reformulada, é fundamental validar sua funcionalidade. Você quer garantir que o novo recurso funcione conforme o esperado e não entre em conflito com a funcionalidade existente. Essa validação normalmente envolve testar o bot com vários cenários de entrada, verificar as respostas e verificar se o bot se comporta conforme o esperado. Você pode realizar a validação de uma das seguintes formas: • Teste o bot manualmente usando o console do Amazon Lex. • Use uma abordagem automatizada usando estruturas e ferramentas de teste que possam simular as interações do usuário e afirmar as respostas esperadas.	Desenvolvedor Lex Bot

Tarefa	Descrição	Habilidades necessárias
Mescle a ramificação de recursos na ramificação principal.	Depois de desenvolver e testar o novo recurso na `TicketBot` instância isolada, faça o seguinte: 1. Confirme as alterações na ramificação de recursos correspondente no sistema de controle de versão. 2. Para mesclar a ramificação do recurso na ramificação principal, crie uma pull request (PR). Esse PR serve como uma solicitação para revisar e incorporar as alterações na base de código principal.	Desenvolvedor do Lex Bot, administrador do repositório

Tarefa	Descrição	Habilidades necessárias
Exclua a ramificação de recursos e o bot do ticket.	Depois que uma ramificação de recursos for mesclada com sucesso na ramificação principal, exclua a ramificação de recursos e o bot do ticket do repositório de código-fonte. Para excluir a ramificação do recurso e o bot do ticket, acione o `DeleteTicketBotPipeline` pipeline. O pipeline remove os recursos temporários do bot que foram criados durante o processo de desenvolvimento (por exemplo, o bot do ticket). Essa ação ajuda a manter um repositório limpo e evitar confusões ou conflitos com futuras ramificações de recursos.	Desenvolvedor Lex Bot

Mantenha o bot principal

Tarefa	Descrição	Habilidades necessárias
Importe a definição mais recente do bot principal para o `dev` ambiente.	Para importar a definição mais recente do bot principal na ramificação principal para o `dev` ambiente, acione o `DeployBotDevPipeline` pipeline.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	O pipeline também cria uma tag git na aprovação.	
Importe a definição mais recente do bot principal para o `prod` ambiente.	Para importar a definição de bot mais recente na ramificação principal para o `prod` ambiente, forneça a referência da tag da tarefa anterior como parâmetro e acione o `DeployBotProdPipeline` pipeline. O pipeline importa a definição de bot mais recente de uma tag específica para o `prod` ambiente.	AWS DevOps

Solução de problemas

Problema	Solução
Quando você implanta bots do Amazon Lex em diferentes Contas da AWS, os serviços de ferramentas devem ter as permissões necessárias para acessar recursos nessas contas.	Para conceder acesso entre contas, use funções e políticas do IAM. Crie funções do IAM nas contas de destino e anexe políticas às funções que concedem as permissões necessárias. Em seguida, assuma essas funções na conta em que o bot Amazon Lex está implantado. Para obter mais informações, consulte Permissões do IAM necessárias para importar e permissões do IAM necessárias para exportar bots no Lex V2 na documentação do Amazon Lex.

Recursos relacionados

- Importação de bots no Amazon Lex V2
- Inicie um pipeline em CodePipeline
- Trabalhando com bots Amazon Lex V2

Automatize a implantação de conjuntos de pilhas usando a AWS e a AWS CodePipeline CodeBuild

Criado por Thiyagarajan Mani (AWS), Mihir Borkar (AWS) e Raghu Gowda (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Em sua integração e entrega contínuas (CI/CD) processes, you might want to deploy applications automatically into all your existing AWS accounts and into new accounts that you add to your organization in AWS Organizations. When you architect a CI/CDsolução para esse requisito), a capacidade de administrador delegado do conjunto de pilhas da AWS CloudFormation é útil porque permite uma camada de segurança ao restringir o acesso à conta de gerenciamento. No entanto, a AWS CodePipeline usa o modelo de permissões gerenciadas por serviços para implantar aplicativos em várias contas e regiões. Você deve usar a conta de gerenciamento do AWS Organizations para implantar com conjuntos de pilhas, porque a AWS CodePipeline não oferece suporte ao recurso de administrador delegado de conjuntos de pilhas.

Este padrão descreve como você pode contornar essa limitação. O padrão usa a AWS CodeBuild e um script personalizado para automatizar a implantação de conjuntos de pilhas com a AWS. CodePipeline Ele automatiza essas atividades de implantação de aplicativos:

- Implemente um aplicativo como conjuntos de pilhas em unidades organizacionais existentes () OUs
- Estenda a implantação de um aplicativo em regiões adicionais OUs
- Remover um aplicativo implantado de todas ou de regiões específicas OUs

Pré-requisitos e limitações

Pré-requisitos

Antes de seguir as etapas deste padrão:

- Criar organizações na sua conta de gerenciamento do AWS Organizations. Para obter instruções, consulte a documentação do AWS Organizations.

- Habilite o acesso confiável entre AWS Organizations e CloudFormation use permissões gerenciadas por serviços. Para obter instruções, consulte Habilitar acesso confiável com AWS Organizations na CloudFormation documentação.

Limitações

O código fornecido com esse padrão tem as seguintes limitações:

- Você pode implantar somente um único CloudFormation modelo para um aplicativo; atualmente, a implantação de vários modelos não é suportada.
- A personalização da implementação atual exige DevOps experiência.
- Esse padrão não usa chaves do AWS Key Management System (AWS KMS). No entanto, você pode ativar essa funcionalidade reconfigurando o CloudFormation modelo incluído nesse padrão.

Arquitetura

Essa arquitetura para o pipeline de implantação de CI/CD trata do seguinte:

- Restringe o acesso direto à conta de gerenciamento delegando a responsabilidade de implantação do conjunto de pilhas a uma conta de CI/CD dedicada como administradora do conjunto de pilhas para implantações de aplicativos.
- Usa o modelo de permissão gerenciado por serviços para implantar o aplicativo automaticamente sempre que uma nova conta é criada e mapeada em uma UO.
- Garante a consistência da versão do aplicativo em todas as contas no nível do ambiente.
- Usa vários estágios de aprovação nos níveis do repositório e do pipeline para fornecer camadas adicionais de segurança e governança para o aplicativo implantado.
- Supera a limitação atual de usar um script CodePipeline de implantação personalizado para implantar ou CodeBuild remover automaticamente conjuntos de pilhas e instâncias de pilha. Para ver uma ilustração do controle de fluxo e da hierarquia das chamadas de API implementadas pelo script personalizado, consulte a seção Informações adicionais.
- Cria conjuntos de pilhas individuais para ambientes de desenvolvimento, teste e produção. Além disso, você pode criar conjuntos de pilhas que OUs combinam várias regiões em cada estágio. Por exemplo, você pode combinar sandbox e desenvolvimento OUs em um estágio de implantação de desenvolvimento.

- Oferece suporte à implantação ou exclusão de aplicativos em um subconjunto de contas ou lista de. OUs

Automação e escala

Você pode usar o código fornecido com esse padrão para criar um CodeCommit repositório da AWS e um pipeline de código para seu aplicativo. Em seguida, você pode implantá-los como conjuntos de pilhas em várias contas no nível da UO. O código também automatiza componentes como tópicos do Amazon Simple Notification Service (Amazon SNS) para notificar aprovadores, os perfis necessários do AWS Identity and Access Management (IAM) e a política de controle de serviços (SCP) a ser aplicada na conta de gerenciamento.

Ferramentas

Serviços da AWS

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- A AWS CodeDeploy automatiza implantações no Amazon Elastic Compute Cloud (Amazon EC2) ou em instâncias locais, funções do AWS Lambda ou serviços Amazon Elastic Container Service (Amazon ECS).
- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias contas AWS em uma organização que você cria e gerencia de maneira centralizada.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.

Repositório de código

O código desse padrão está disponível no repositório GitHub automated-code-pipeline-stackset-deployment. Para ver a estrutura de pastas e outros detalhes, consulte o arquivo readme do repositório.

Práticas recomendadas

Este padrão restringe o acesso direto à conta de gerenciamento durante a implantação do aplicativo no nível da UO. Adicionar vários estágios de aprovação ao processo de pipeline e repositório ajuda a fornecer segurança e governança adicionais para os aplicativos e componentes que você implanta usando essa abordagem.

Épicos

Configure contas no AWS Organizations

Tarefa	Descrição	Habilidades necessárias
Habilite o recurso de gerenciamento entre contas.	Ative todos os atributos na conta de gerenciamento da sua organização seguindo as instruções na documentação do AWS Organizations.	Administrador da AWS, administrador da plataforma
Crie uma conta de CI/CD.	No AWS Organizations, em sua organização, crie uma conta de CI/CD dedicada e designe uma equipe para possuir e controlar o acesso à conta.	Administrador da AWS
Adicionar um administrador delegado.	Na conta de gerenciamento, registre a conta CI/CD que você criou na etapa anterior como administrador delegado do conjunto de pilhas. Para obter instruções, consulte a CloudFormation documentação da AWS.	Administrador da AWS, administrador da plataforma

Crie um repositório de aplicativos e um pipeline de CI/CD

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de códigos.	1. Clone o repositório de código fornecido com esse padrão em seu computador: `git clone https://github.com/aws-samples/automated-code-pipeline-stackset-deployment.git` 2. Analise o arquivo readme para entender a estrutura de diretórios e outros detalhes.	AWS DevOps
Crie tópicos do SNS.	Você pode usar o `sns-template.yaml` modelo fornecido no GitHub repositório para criar tópicos do SNS e configurar assinaturas para solicitações de aprovação. 1. No console da AWS, faça login na conta CI/CD. 2. Abra o CloudFormation console em https://console.aws.amazon.com/cloudformation. 3. Criar uma nova pilha com novos recursos (opção padrão). 4. Em Especificar modelo, escolha Carregar um arquivo de modelo,	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Escolher arquivo e selecione o `sns-template.yaml` arquivo na `templates` pasta do GitHub repositório clonado. Escolha Próximo. 5. Forneça um nome significativo para a pilha de aplicativos. 6. Especifique um prefixo para os recursos. 7. Escolha Próximo, Próximo e Enviar. 8. Quando a pilha for criada com sucesso, escolha a guia Saídas e anote os Amazon Resource Names (ARNs) dos tópicos do SNS para pull requests, o ambiente de teste e o ambiente de produção. Você usará essas informações em etapas subsequentes.	

Tarefa	Descrição	Habilidades necessárias
Crie perfis do IAM para componentes de CI/CD.	Você pode usar o `cicd-role-template.yaml` modelo fornecido no GitHub repositório para criar funções e políticas do IAM exigidas pelos componentes de CI/CD. 1. No console da AWS, faça login na conta CI/CD. 2. Abra o CloudFormation console em https://console.aws.amazon.com/cloudformation. 3. Criar uma nova pilha com novos recursos (opção padrão). 4. Em Especificar modelo, escolha Carregar um arquivo de modelo, Escolher arquivo e selecione o `cicd-role-template.yaml` arquivo na `templates` pasta do GitHub repositório clonado. Escolha Próximo. 5. Forneça um nome significativo para a pilha de aplicativos. 6. Use os valores para os seguintes parâmetros. • O ARN para a política para o limite de permissões. Você pode obter esse ARN na seção	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Detalhes da política da sua política de limite de permissões no console do IAM. • O ARN do tópico de aprovação de produção do SNS que você anotou anteriormente. • O ARN do tópico de aprovação de teste do SNS que você anotou anteriormente. • Um prefixo para recursos criados pelo modelo. 7. Escolha Próximo, Próximo e Enviar. 8. Quando a pilha for criada com sucesso, escolha a guia Saídas e anote as funções ARNs do IAM que foram criadas. Você usará essas informações em etapas subsequentes.	

Tarefa	Descrição	Habilidades necessárias
Crie um CodeCommit repositório e um pipeline de código para seu aplicativo.	Você pode usar o `cicd-pipeline-template.yaml` modelo fornecido no GitHub repositório para criar um CodeCommit repositório e um pipeline de código para seu aplicativo. 1. No console da AWS, faça login na conta CI/CD. 2. Abra o CloudFormation console em https://console.aws.amazon.com/cloudformation. 3. Criar uma nova pilha com novos recursos (opção padrão). 4. Em Especificar modelo, escolha Carregar um arquivo de modelo, Escolher arquivo e selecione o `cicd-pipeline-template.yaml` arquivo na `templates` pasta do GitHub repositório clonado. Escolha Próximo. 5. Forneça um nome significativo para a pilha de aplicativos. 6. Use os valores para os seguintes parâmetros. • AppRepositoryName— O nome do CodeCommi	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	t repositório que será criado para o aplicativo. • AppRepositoryDescr iption— Uma breve descrição do CodeCommi t repositório que será criado para o aplicativo. • ApplicationName— O nome do seu aplicativo. Essa string é usada como nome do CodeCommit repositório e como prefixo do pipeline de CI/CD. • CloudWatchEventRol eARN — O ARN da função do CloudWatch evento da tarefa anterior. • CodeBuildProjectRo leARN — O ARN da função do CodeBuild projeto da tarefa anterior. • CodePipelineRoleARN — O ARN da CodePipeline função da tarefa anterior. • DeploymentConfigBu cket— O nome do bucket do Amazon Simple Storage Service (Amazon S3) no qual os arquivos de configura ção de implantação e o arquivo.zip do script serão armazenados.	

Tarefa	Descrição	Habilidades necessárias
	• DeploymentConfigKey— O caminho e o nome do arquivo.zip (chave Amazon S3). • PRApprovalSNSARN — O ARN do tópico SNS para notificações de pull request. • ProdApprovalSNSARN — O ARN do tópico SNS para aprovações de produção. • TESTApprovalSNSARN — O ARN do tópico SNS para aprovações de testes. • TemplateBucket— O nome do bucket do S3 no modelo de criação do CI/CD account where the CI/CD pipeline será armazenado. 7. Escolha Próximo, Próximo e Enviar. 8. Quando a pilha é concluída com êxito, ela cria um CodeCommit repositório com o nome especificado e uma estrutura de diretórios padrão, arquivos de configuração de implantação, scripts e um pipeline de código para o repositório.	

Implantar um conjunto de pilhas

Tarefa	Descrição	Habilidades necessárias

Clone o repositório do aplicativo.	O modelo de pipeline de CI/CD que você usou anteriormente cria um exemplo de repositório de aplicativos e pipeline de código. Para clonar e verificar o repositório:
	1. Faça login na conta de CI/CD.
	2. Localize o repositório do aplicativo e o pipeline de CI/CD que você criou no épico anterior.
	3. Copie a URL do repositório e use o comando git clone para clonar o repositório na sua máquina local.
	4. Verifique se a estrutura do diretório e os arquivos correspondem ao seguinte:
	`root`
	`|- deploy_configs`
	`|  |- deployment_config.json`
	`|- parameters`
	`|  |- template-parameter-dev.json`
	`|  |- template-parameter-test.json`
	`|  |- template-parameter-prod.json`
	`|- templates`
	`|  |- template.yml`
		Desenvolvedor de aplicativos, Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	<pre>|- buildspec.yml</pre> onde a `deploy_configs` pasta contém o arquivo de configuração de implantação e as `parameters` pastas `templates` e incluem arquivos padrão que você substituirá por seus próprios arquivos CloudFormation de modelo e parâmetros. **Important** Não personalize a estrutura de pastas. 5. Crie uma ramificação de atributos.	

Tarefa	Descrição	Habilidades necessárias
Adicione artefatos do aplicativo.	Atualize o repositório do aplicativo usando um CloudFormation modelo. **Note** Essa solução oferece suporte à implantação de apenas um único CloudFormation modelo. 1. Crie seu CloudFormation modelo para implantar as alterações no código do aplicativo e dê um nome a ele`<application-name>.yaml` . 2. Substitua o `template.yml` arquivo na `templates` pasta do repositório do aplicativo pelo CloudFormation modelo que você criou na etapa 1. 3. Prepare arquivos de parâmetros para cada ambiente (desenvolvimento, teste e produção). 4. Nomeie os arquivos de parâmetros usando o formato `<cloudformation-template-na`	Desenvolvedor de aplicativos, Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	me>-parameter-<environment-name>.json . 5. Substitua os arquivos de parâmetros padrão na pasta `parameters` pelos arquivos da etapa 4.	

Tarefa	Descrição	Habilidades necessárias
Atualize o arquivo de configuração de implantação.	Atualize o arquivo `deployment_config.json` : 1. No repositório do aplicativo, navegue até a pasta `deploy_configs` . 2. Abra o arquivo `deployment_config.json` : `{ "deployment_action": "<deploy/delete>", "stack_set_name": "<stack set name>", "stack_set_desciption": "<stack set description>", "deployment_targets": { "dev": { "org_units": ["list of OUs"], "regions": ["list of regions"], "filter_accounts": ["list of accounts"], "filter_type":`	Desenvolvedor de aplicativos, Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias

	"<DIFFERENCE/INTERSECTION/UNION>"
	},
	"test": {
	"org_units": ["list of OUs"],
	"regions": ["list of regions"],
	"filter_accounts": ["list of accounts"],
	"filter_type": "<DIFFERENCE/INTERSECTION/UNION>"
	},
	"prod": {
	"org_units": ["list of OUs"],
	"regions": ["list of regions"],
	"filter_accounts": ["list of accounts"],	

Tarefa	Descrição	Habilidades necessárias

```
    "filter_type":
 "<DIFFERENCE/INTER
SECTION/UNION>"

             }


    },
    "cft_capa
bilities": ["CAPABIL
ITY_IAM", "CAPABILI
TY_NAMED_IAM"],
    "auto_dep
loyement": "<True/Fa
lse>",
    "retain_s
tacks_on_account_r
emoval": "<True/Fa
lse>",
    "region_d
eployment_concurre
ncy": "<SEQUENTIAL/
PARALLEL>"
}
```

3. Atualize os valores da ação de implantação, nome do conjunto de pilhas, descrição do conjunto de pilhas e destinos de implantação.

   Por exemplo, você pode configurar `deploymen t_action` para `delete` para excluir todo o conjunto de pilhas e nas instâncias de pilha associadas. Use

Tarefa	Descrição	Habilidades necessárias
	`deploy` para criar um novo conjunto de pilhas, atualizar um conjunto de pilhas existente ou adicionar ou remover instâncias de pilha para outras OUs regiões ou regiões. Para obter MAIS exemplos, consulte a seção Informações adicionais. Esse padrão cria conjuntos de pilhas individuais para cada ambiente adicionando o nome do ambiente ao nome do conjunto de pilhas que você fornece no arquivo de configuração de implantação.	

Tarefa	Descrição	Habilidades necessárias
Confirme as alterações e implante o conjunto de pilhas.	Confirme as alterações que você especificou em seu modelo de aplicativo e mescle e implante o conjunto de pilhas em vários ambientes, etapa por etapa: 1. Salve todos os seus arquivos e confirme as alterações na ramificação de atributos do seu repositório de aplicativos local. 2. Envie a ramificação do atributo para o repositório remoto. 3. Crie uma solicitação pull para mesclar as alterações na ramificação principal. Quando a solicitação pull for aprovada e as alterações forem mescladas na ramificação principal, o pipeline de CI/CD será inicializado. 4. Quando o estágio de desenvolvimento e implantação for concluído com êxito, verifique o CloudFormation console StackSets, guia Service-Managed.	Desenvolvedor de aplicativos, Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	Você verá um novo conjunto de pilhas com o sufixo `dev`. 5. Verifique se há algum problema nos CodeBuild registros do estágio de desenvolvimento e implantação. 6. Implante o conjunto de pilhas nos ambientes de teste e de produção solicitando que seus aprovadores aprovem as implantações nesses estágios e repetindo as etapas 5 e 6. Os conjuntos de pilhas para os ambientes de teste e produção têm os sufixos `test` e `prod`.	

Solução de problemas

Problema	Solução
A implantação falha com a exceção: Altere o nome do arquivo de parâmetros do modelo como -parameter- .json com, nomes padrão não são permitidos <application name><evn>	Os arquivos CloudFormation de parâmetro s do modelo devem seguir a convenção de nomenclatura especificada. Atualize os nomes dos arquivos de parâmetros e tente novamente .
A implantação falha com a exceção:	O nome do CloudFormation modelo deve seguir a convenção de nomenclatura especific

Problema	Solução
Altere o nome do CloudFormation modelo como .yml; o padrão template.yml ou template.yaml não são permitidos <application name>	ada. Atualize o nome do arquivo e tente novamente.
A implantação falha com a exceção: Nenhum CloudFormation modelo válido e seu arquivo de parâmetros foram encontrados para o ambiente {nome do ambiente}	Verifique as convenções de nomenclatura do arquivo para o CloudFormation modelo e seu arquivo de parâmetros para o ambiente especificado.
A implantação falha com a exceção: Ação de implantação inválida fornecida no arquivo de configuração de implantação. As opções válidas são 'implantar' e 'excluir'.	Você especificou um valor inválido para o parâmetro `deployment_action` no arquivo de configuração de implantação. O parâmetro tem dois valores válidos: `deploy` e `delete`. Use `deploy` para criar e atualizar os conjuntos de pilhas e as instâncias da pilha associada s deles. Use `delete` somente quando quiser remover todo o conjunto de pilhas e instâncias de pilha associadas.

Recursos relacionados

- GitHub automated-code-pipeline-stackset-repositório de implantação
- Habilitar todos os atributos na organização (documentação do AWS Organizations)
- Registre um administrador delegado (CloudFormation documentação da AWS)
- Metas em nível de conta para conjuntos de pilhas gerenciados por serviços (documentação da AWS) CloudFormation

Mais informações

Fluxograma

O fluxograma a seguir mostra o controle de fluxo e a hierarquia das chamadas de API implementadas pelo script personalizado para automatizar a implantação do conjunto de pilhas.

Exemplos de arquivos de configuração de implantação

Criação de um novo conjunto de pilhas

O arquivo de configuração de implantação a seguir cria um novo conjunto de pilhas chamado `sample-stack-set` na região da AWS `us-east-1` em três OUs.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                             "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Implantação de um conjunto de pilhas existente em outra UO

Se você implantar a configuração mostrada no exemplo anterior e quiser implantar o conjunto de pilhas em uma UO adicional chamada `dev-org-unit-2` no ambiente de desenvolvimento, o arquivo de configuração de implantação poderá ter a seguinte aparência.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Implantação de um conjunto de pilhas existente em outra região da AWS

Se você implantar a configuração mostrada no exemplo anterior e quiser implantar o conjunto de pilhas em uma região adicional da AWS (`us-east-2`) no ambiente de desenvolvimento para dois OUs (`dev-org-unit-1edev-org-unit-2`), o arquivo de configuração de implantação pode ter a seguinte aparência.

> **Note**
>
> Os recursos no CloudFormation modelo devem ser válidos e específicos da região.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                             "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Remover uma instância de pilha de uma UO ou região da AWS

Digamos que a configuração de implantação mostrada no exemplo anterior tenha sido implantada. O arquivo de configuração a seguir remove as instâncias da pilha das duas regiões da UO `dev-org-unit-2`.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                             "dev": {
```

```
                                    "org_units": ["dev-org-unit-1"],
                                    "regions": ["us-east-1", "us-east-2"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                },
                            "test": {
                                    "org_units": ["test-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                },
                            "prod": {
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                        },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

O arquivo de configuração a seguir remove a instância de pilha da região da AWS `us-east-1` para ambas OUs no ambiente de desenvolvimento.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                    "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                    "regions": ["us-east-2"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                },
                            "test": {
                                    "org_units": ["test-org-unit-1"],
                                    "regions": ["us-east-1"],
```

```
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                                "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                            },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
 }
```

Apagamento de todo o conjunto de pilhas

O arquivo de configuração de implantação a seguir apaga todo o conjunto de pilhas e todas as instâncias de pilha associadas.

```
{
     "deployment_action": “delete”,
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                                "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                                "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                                "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
```

```
                                    "filter_type": ""
                                }
                            },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Exclusão de uma conta da implantação

O arquivo de configuração de implantação a seguir exclui a conta `111122223333`, que faz parte da UO `dev-org-unit-1`, da implantação.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                    "org_units": ["dev-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": ["111122223333"],
                                    "filter_type": "DIFFERENCE"
                                },
                            "test": {
                                    "org_units": ["test-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                },
                            "prod": {
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                            },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Implantando o aplicativo em um subconjunto de contas em uma UO

O arquivo de configuração de implantação a seguir implanta o aplicativo em apenas três contas (111122223333, 444455556666 e777788889999) na UO `dev-org-unit-1`.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": ["111122223333",
"444455556666", "777788889999"],
                                        "filter_type": "INTERSECTION"
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Anexe automaticamente uma política gerenciada da AWS para Systems Manager aos perfis de EC2 instância usando o Cloud Custodian e o AWS CDK

Criado por Ali Asfour (AWS) e Aaron Lennon (AWS)

Resumo

Você pode integrar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o AWS Systems Manager para automatizar tarefas operacionais e fornecer mais visibilidade e controle. Para se integrarem ao Systems Manager, EC2 as instâncias devem ter um AWS Systems Manager Agent (SSM Agent) instalado e uma política do `AmazonSSMManagedInstanceCore` AWS Identity and Access Management (IAM) anexada aos seus perfis de instância.

No entanto, se você quiser garantir que todos os perfis de EC2 instância tenham a `AmazonSSMManagedInstanceCore` política anexada, você pode enfrentar desafios para atualizar novas EC2 instâncias que não tenham perfis de instância ou EC2 instâncias que tenham um perfil de instância, mas não tenham a `AmazonSSMManagedInstanceCore` política. Também pode ser difícil adicionar essa política em várias contas da Amazon Web Services (AWS) e regiões da AWS.

Esse padrão ajuda a resolver esses desafios implantando três políticas de Cloud Custodian em suas contas da AWS:

- A primeira política do Cloud Custodian verifica as EC2 instâncias existentes que têm um perfil de instância, mas não têm a `AmazonSSMManagedInstanceCore` política. A política `AmazonSSMManagedInstanceCore` é então anexada.
- A segunda política do Cloud Custodian verifica as EC2 instâncias existentes sem um perfil de instância e adiciona um perfil de instância padrão que tem a `AmazonSSMManagedInstanceCore` política anexada.
- A terceira política do Cloud Custodian cria funções do AWS Lambda em suas contas para monitorar a criação de instâncias e perfis EC2 de instância. Isso garante que a `AmazonSSMManagedInstanceCore` política seja anexada automaticamente quando uma EC2 instância é criada.

Esse padrão usa as DevOps ferramentas da AWS para obter uma implantação contínua e em grande escala das políticas do Cloud Custodian em um ambiente de várias contas, sem provisionar um ambiente computacional separado.

Pré-requisitos e limitações

Pré-requisitos

- Duas ou mais contas ativas da AWS. Uma conta é a conta de segurança e as outras são contas de membros.
- Permissões para provisionar recursos na conta de segurança. Esse padrão usa permissões de administrador, mas você deve conceder permissões de acordo com os requisitos e as políticas da sua organização.
- Capacidade de assumir um perfil do IAM da conta de segurança até as contas dos membros e criar os perfis do IAM necessários. Para obter mais informações, consulte Delegar acesso entre contas da AWS usando perfis do IAM na documentação do IAM.
-

> **Important**
>
> AWS Command Line Interface (AWS CLI), instalada e configurada. Para fins de teste, você pode configurar a AWS CLI usando o comando `aws configure` ou definindo variáveis de ambiente. : isso não é recomendado para ambientes de produção e recomendamos que essa conta tenha acesso com privilégios mínimos. Para obter mais informações, consulte Conceder privilégio mínimo na documentação do IAM.

- O arquivo `devops-cdk-cloudcustodian.zip` (anexado), transferido por download para o computador local.
- Familiaridade com o Python.
- As ferramentas necessárias (Node.js, AWS Cloud Development Kit (AWS CDK) e Git), instaladas e configuradas. Você pode usar o arquivo `install-prerequisites.sh` no arquivo `devops-cdk-cloudcustodian.zip` para instalar essas ferramentas. Certifique-se de executar esse arquivo com privilégios de raiz.

Limitações

- Embora esse padrão possa ser usado em um ambiente de produção, certifique-se de que todas as políticas e perfis do IAM atendam aos requisitos e políticas da sua organização.

Versões do pacote

- Cloud Custodian versão 0.9 ou mais recente

- TypeScript versão 3.9.7 ou posterior
- Node.js versão 14.15.4 ou superior
- `npm` versão 7.6.1 ou mais recente
- AWS CDK versão 1.96.0 ou superior

Arquitetura

O diagrama mostra o seguinte fluxo de trabalho:

1. As políticas do Cloud Custodian são enviadas para um CodeCommit repositório da AWS na conta de segurança. Uma regra da Amazon CloudWatch Events inicia automaticamente o CodePipeline pipeline da AWS.
2. O pipeline busca o código mais recente CodeCommit e o envia para a parte de integração contínua do pipeline de integração contínua e entrega contínua (CI/CD) gerenciado pela AWS. CodeBuild
3. CodeBuild executa as DevSecOps ações completas, incluindo a validação da sintaxe da política nas políticas do Cloud Custodian, e executa essas políticas no `--dryrun` modo de verificar quais recursos foram identificados.
4. Se não houver erros, a próxima tarefa alertará o administrador para revisar as alterações e aprovar a implantação nas contas dos membros.

Pilha de tecnologia

- AWS CDK
- CodeBuild
- CodeCommit
- CodePipeline
- IAM
- Cloud Custodian

Automação e escala

O módulo de pipelines do AWS CDK provisiona um pipeline de CI/CD que é usado CodePipeline para orquestrar a criação e o teste do código-fonte CodeBuild, além da implantação de recursos da AWS com pilhas da AWS. CloudFormation É possível usar esse padrão para todas as contas-membro e regiões da organização. Você também pode estender a pilha `Roles creation` para implantar outros perfis do IAM em suas contas de membros.

Ferramentas

- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software para definir a infraestrutura de nuvem em código e provisioná-la por meio da AWS. CloudFormation
- O AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- CodeBuildA AWS é um serviço de construção totalmente gerenciado na nuvem.
- CodeCommitA AWS é um serviço de controle de versão que você pode usar para armazenar e gerenciar ativos de forma privada.
- CodePipelineA AWS é um serviço de entrega contínua que você pode usar para modelar, visualizar e automatizar as etapas necessárias para lançar seu software.
- O AWS Identity and Access Management é um serviço da web que ajuda você a controlar o acesso aos recursos da AWS com segurança.
- O Cloud Custodian é uma ferramenta que unifica dezenas de ferramentas e os scripts que muitas organizações usam para gerenciar suas contas de nuvem pública em uma ferramenta de código aberto.
- O Node.js é um JavaScript tempo de execução criado no JavaScript motor V8 do Google Chrome.

Código

Para obter uma lista detalhada dos módulos, perfis da conta, arquivos e comandos de implantação usados nesse padrão, consulte o arquivo `README` no arquivo `devops-cdk-cloudcustodian.zip` (em anexo).

Épicos

Configure o pipeline com o AWS CDK

Tarefa	Descrição	Habilidades necessárias
Configure o CodeCommit repositório.	1. Descompacte o arquivo `devops-cdk-cloudcustodian.zip` (anexado) no diretório de trabalho do computador local. 2. Faça login no AWS Management Console para obter sua conta de segurança, abra o CodeCommit console e crie um novo `devops-cdk-cloudcustodian` repositório. 3. Vá para o diretório do projeto e configure o CodeCommit repositório como origem, confirme as alterações e, em seguida, envie-as para a ramificação de origem executando os seguintes comandos: • `cd devops-cdk-cloudcustodian` • `git init --initial-branch=main` • `git add . git commit -m 'initial commit'`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	• `git remote add origin https://git-codecommit.us-east-1.amazonaws.com/v1/devops-cdk-cloudcustodian` • `git push origin main` Para obter mais informações sobre isso, consulte Criação de um CodeCommit repositório na CodeCommit documentação da AWS.	
Instale as ferramentas necessárias	Use o arquivo `install-prerequisites.sh` para instalar todas as ferramentas necessárias no Amazon Linux. Não inclui a AWS CLI porque ela vem pré-instalada. Para obter mais informações, consulte Pré-requisitos na seção de Conceitos básicos do AWS CDK na documentação do AWS CDK.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Instale os pacotes AWS CDK obrigatórios.	1. Configure seu ambiente virtual executando o seguinte comando na AWS CLI: `$ python3 -m venv .env` 2. No ambiente virtual, a executar o comando a seguir: `$ source .env/bin/activate` 3. Depois que o ambiente virtual for ativado, instale as dependências, execute o seguinte comando: `$ pip install -r requirements.txt` 4. Para adicionar dependências adicionais (por exemplo, outras bibliotecas do AWS CDK), adicione-as ao arquivo `requirements.txt` e execute o seguinte comando: `pip install -r requirements.txt` Os pacotes a seguir são exigidos pelo AWS CDK e estão incluídos no arquivo `requirements.txt` : • `aws-cdk.aws-cloudwatch`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	• `aws-cdk.aws-codebuild` • `aws-cdk.aws-codecommit` • `aws-cdk.aws-codedeploy` • `aws-cdk.aws-codepipeline` • `aws-cdk.aws-codepipeline-actions` • `aws-cdk.aws-events` • `aws-cdk.aws-events-targets` • `aws-cdk.aws-iam` • `aws-cdk.aws-logs` • `aws-cdk.aws-s3` • `aws-cdk.aws-sns` • `aws-cdk.aws-sns-subscriptions` • `aws-cdk.aws-sqs` • `aws-cdk.core`	

Configure o ambiente

Tarefa	Descrição	Habilidades necessárias
Atualize as variáveis necessárias.	Abra o `vars.py` arquivo na pasta raiz do seu CodeCommit repositório e atualize as seguintes variáveis:	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	• Atualize `var_deploy_region = 'us-east-1'` com a região da AWS na qual você deseja que o pipeline seja implantado. • Atualize `var_codecommit_repo_name = "cdk-cloudcustodian"` com o nome do seu CodeCommit repositório. • Atualize `var_codecommit_branch_name = "main"` com o nome da CodeCommit filial. • Atualize `var_adminEmail=notifyadmin@email.com'` com o endereço de e-mail do administrador que aprova as alterações. • Atualize `var_slackWebHookUrl = https://hooks.slack.com/services/T000000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX` com o webhook do Slack usado para enviar notificações do Cloud Custodian quando alterações são feitas. • Atualize `var_orgId = 'o-yyyyyyyyyy'` com o ID da sua organização.	

Tarefa	Descrição	Habilidades necessárias
	• Atualize `security_account = '123456789011'` com o ID da conta da AWS para a conta em que o pipeline está implantado. • Atualize `member_accounts = ['111111111111','111111111112','111111111113']` com as contas membros nas quais você deseja inicializar a pilha do AWS CDK e implantar os perfis do IAM necessários. • Defina `cdk_bootstrap_member_accounts = True` para `True` se você quiser que o pipeline inicialize automaticamente o AWS CDK em suas contas membros. Se definido para `True`, também será necessário o nome de um perfil do IAM existente nas contas dos membros que pode ser assumido a partir da conta de segurança. Esse perfil do IAM também deve ter as permissões necessárias para inicializar o AWS CDK.	

Tarefa	Descrição	Habilidades necessárias
	• **Note** Atualize `cdk_bootstrap_role = 'AWSControlTowerExecution'` com o nome de um perfil do IAM existente nas contas dos membros que pode ser assumido a partir da conta de segurança. Esse perfil também deve ter permissão para inicializar o AWS CDK. : Isso só se aplica se `cdk_bootstrap_member_accounts` estiver definido como`True`.	

Tarefa	Descrição	Habilidades necessárias

Atualize o arquivo account.yml com as informações da conta do membro.	Para executar a ferramenta c7n-org Cloud Custodian em várias contas, você deve colocar o arquivo de configuração `accounts.yml` na raiz do repositório. Veja a seguir um exemplo de arquivo de configuração do Cloud Custodian para AWS:
	`accounts:`
	`- account_id: '123123123123'`
	`  name: account-1`
	`  regions:`
	`  - us-east-1`
	`  - us-west-2`
	`  role: arn:aws:iam::123123123123:role/CloudCustodian`
	`  vars:`
	`  charge_code: xyz`
	`  tags:`
	`  - type:prod`
	`  - division:some division`
	`  - partition:us`
	`  - scope:pci`
		Desenvolvedor

Inicialize as contas da AWS

Tarefa	Descrição	Habilidades necessárias
Inicialize a conta de segurança.	Inicialize `deploy_account` com o aplicativo `cloudcust`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`odian_stack` executando o seguinte comando: `cdk bootstrap -a 'python3 cloudcustodian/cloudcustodian_stack.py`	
Opção 1: inicialize automaticamente as contas dos membros.	Se a variável `cdk_bootstrap_member_accounts` for definida como para `True` no arquivo `vars.py`, as contas especificadas na variável `member_accounts` serão automaticamente inicializadas pelo pipeline. Se necessário, é possível atualizar `*cdk_bootstrap_role*` com um perfil do IAM que você pode assumir a partir da conta de segurança e que tem as permissões necessárias para inicializar o AWS CDK. Novas contas adicionadas à variável `member_accounts` são inicializadas automaticamente pelo pipeline para que os perfis necessários possam ser implantados.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Opção 2: inicialize manualmente as contas dos membros.	Embora não seja recomendável usar essa abordagem, você pode definir o valor de `cdk_bootstrap_member_accounts` para `False` e executar essa etapa manualmente executando o seguinte comando: `$ cdk bootstrap -a 'python3 cloudcustodian/member_account_roles_stack.py' \ --trust {security_account_id} \ --context assume-role-credentials:writeIamRoleName={role_name} \ --context assume-role-credentials:readIamRoleName={role_name} \ --mode=ForWriting \ --context bootstrap=true \ --cloudformation-execution-policies arn:aws:iam::aws:policy/AdministratorAccess`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Important Certifique-se de atualizar `{role_name}` os valores `{security_account_id}` e com o nome de uma função do IAM que você possa assumir na conta de segurança e que tenha as permissões necessárias para inicializar o AWS CDK. Você também pode usar outras abordagens para inicializar as contas dos membros, por exemplo, com a AWS CloudFormation. Para obter mais informações, consulte Inicialização na documentação do AWS CDK.	

Implante as pilhas de AWS CDK

Tarefa	Descrição	Habilidades necessárias
Crie os perfis do IAM nas contas dos membros.	Execute o seguinte comando para implantar a pilha `member_account_rol`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`es_stack` e criar os perfis do IAM nas contas-membro: `cdk deploy --all -a 'python3 cloudcustodian/member_account_roles_stack.py' --require-approval never`	
Implante a pilha de pipeline do Cloud Custodian.	Execute o seguinte comando para criar o pipeline `cloudcustodian_stack.py` do Cloud Custodian que é implantado na conta de segurança: `cdk deploy -a 'python3 cloudcustodian/cloudcustodian_stack.py'`	Desenvolvedor

Recursos relacionados

- Conceitos básicos do AWS CDK

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Compile automaticamente pipelines de CI/CD e clusters do Amazon ECS para microsserviços usando o AWS CDK

Criado por Varsha Raju (AWS)

Resumo

Esse padrão descreve como criar automaticamente a integração contínua e a entrega contínua (CI/CD) pipelines and underlying infrastructure for building and deploying microservices on Amazon Elastic Container Service (Amazon ECS). You can use this approach if you want to set up proof-of-concept CI/CD pipelines to show your organization the benefits of CI/CD, microservices, and DevOps. You can also use this approach to create initial CI/CDpipelines) que você pode personalizar ou alterar de acordo com os requisitos da sua organização.

A abordagem do padrão cria um ambiente de produção e um ambiente de não produção, cada um com uma nuvem privada virtual (VPC) e um cluster do Amazon ECS configurado para ser executado em duas zonas de disponibilidade. Esses ambientes são compartilhados por todos os seus microsserviços e, em seguida, você cria um CI/CD pipeline for each microservice. These CI/CD pipeline, extrai as alterações de um repositório de origem na AWS CodeCommit, cria automaticamente as alterações e as implanta em seus ambientes de produção e não produção. Quando um pipeline conclui com êxito todas as suas etapas, você pode usá-lo URLs para acessar o microsserviço nos ambientes de produção e não produção.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS).
- Um bucket do Amazon Simple Storage Service (Amazon S3) existente que contém o arquivo `starter-code.zip` (anexado)
- AWS Cloud Development Kit (AWS CDK), instalado e configurado. Para obter mais informações, consulte Conceitos básicos do AWS CDK na documentação do AWS CDK.
- Python 3 e `pip` instalado e configurado Para obter mais informações, consulte a documentação do Pyton.
- Familiaridade com o AWS CDK, AWS CodeBuild, CodePipeline AWS, CodeCommit Amazon Elastic Container Registry (Amazon ECR), Amazon ECS e AWS Fargate.
- Familiaridade com o Docker.

- Uma compreensão do CI/CD e. DevOps

Limitações

- Os limites gerais da conta da AWS se aplicam. Para obter mais informações, consulte Service Quotas da AWS, na documentação de Referência geral da AWS.

Versões do produto

- Esse código foi testado usando o Nose.js versão 16.13.0 e o AWS CDK versão 1.132.0.

Arquitetura

O diagrama mostra o seguinte fluxo de trabalho:

1. Um desenvolvedor de aplicativos confirma o código em um CodeCommit repositório.
2. Um pipeline é inicializado.
3. CodeBuild cria e envia a imagem do Docker para um repositório Amazon ECR
4. CodePipeline implanta uma nova imagem em um serviço Fargate existente em um cluster Amazon ECS não produtivo.
5. O Amazon ECS extrai a imagem do repositório Amazon ECR para um serviço Fargate que não é de produção.
6. O teste é realizado usando um URL que não é de produção.
7. O gerente de lançamento aprova a implantação de produção.
8. CodePipeline implanta a nova imagem em um serviço Fargate existente em um cluster de produção do Amazon ECS
9. O Amazon ECS extrai a imagem do repositório Amazon ECR para um serviço Fargate de produção.
10. Os usuários de produção acessam seu atributo usando uma URL de produção.

Pilha de tecnologia

- AWS CDK
- CodeBuild

- CodeCommit
- CodePipeline
- Amazon ECR
- Amazon ECS
- Amazon VPC

Automação e escala

Você pode usar a abordagem desse padrão para criar pipelines para microsserviços implantados em uma pilha compartilhada da AWS. CloudFormation A automação pode criar mais de um cluster do Amazon ECS em cada VPC e também criar pipelines para microsserviços implantados em um cluster compartilhado do Amazon ECS. No entanto, isso exige que você forneça novas informações de recursos como entradas para a pilha do pipeline.

Ferramentas

- AWS CDK — O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software para definir a infraestrutura de nuvem em código e provisioná-la por meio da AWS. CloudFormation
- AWS CodeBuild — CodeBuild A AWS é um serviço de construção totalmente gerenciado na nuvem. CodeBuild compila seu código-fonte, executa testes de unidade e produz artefatos prontos para serem implantados.
- AWS CodeCommit — CodeCommit A AWS é um serviço de controle de versão que permite que você armazene e gerencie de forma privada repositórios Git na nuvem da AWS. CodeCommit elimina a necessidade de você gerenciar seu próprio sistema de controle de origem ou se preocupar com a escalabilidade de sua infraestrutura.
- AWS CodePipeline — CodePipeline A AWS é um serviço de entrega contínua que você pode usar para modelar, visualizar e automatizar as etapas necessárias para lançar seu software. Você pode modelar e configurar rapidamente os diferentes estágios de um processo de lançamento de software. CodePipeline automatiza as etapas necessárias para liberar suas alterações de software continuamente.
- Amazon ECS: o Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido que é usado na execução, interrupção e gerenciamento de contêineres em um cluster. Você pode executar tarefas e serviços em uma infraestrutura com tecnologia sem servidor gerenciada pelo AWS Fargate. Como alternativa, para

ter mais controle sobre sua infraestrutura, você pode executar suas tarefas e serviços em um cluster de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que você gerencia.

- Docker: o Docker ajuda os desenvolvedores a empacotar, enviar e executar facilmente qualquer aplicativo como um contêiner leve, portátil e autossuficiente.

Código

O código desse padrão está disponível nos arquivos `cicdstarter.zip` e `starter-code.zip` (anexado).

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Configure o diretório de trabalho para o AWS CDK.	1. Crie um diretório chamado `cicdproject` na sua máquina local. 2. Baixe o arquivo `cicdstarter.zip` (anexado) no diretório `cicdproject` e descompacte-o. Ele cria uma pasta chamada `cicdstarter`. 3. Execute o comando `cd <user-home>/cicdproject/cicdstarter`. 4. Configure o ambiente virtual Python executando o comando `python3 -m venv .venv`. 5. Execute o comando `source ./.venv/bin/activate`.	AWS DevOps, infraestrutura de nuvem

Tarefa	Descrição	Habilidades necessárias
	6. Configure seu ambiente da AWS executando o comando `aws configure` ou usando as seguintes variáveis de ambiente: • `AWS_ACCESS_KEY_ID` • `AWS_SECRET_ACCESS_KEY` • `AWS_DEFAULT_REGION`	

Crie a infraestrutura compartilhada

Tarefa	Descrição	Habilidades necessárias
Crie a infraestrutura compartilhada.	1. No diretório de trabalho, execute o comando `cd cicdvpcecs .` 2. Execute o comando `pip3 install -r requirements.txt` para instalar todas as dependências necessárias do Python 3. Execute o `cdk bootstrap command` para definir o ambiente da AWS para o AWS CDK. 4. Execute o comando `cdk synth --context aws_account=<aws_account_ID> --context aws_region=<aws-region> .`	AWS DevOps, infraestrutura de nuvem

Tarefa	Descrição	Habilidades necessárias
	5. Execute o comando `cdk deploy --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` . 6. A CloudFormation pilha da AWS cria a seguinte infraestrutura: • Uma VPC que não é de produção chamada `cicd-vpc-ecs/cicd-vpc-nonprod` • Uma VPC de produção chamada `cicd-vpc-ecs/cicd-vpc-prod` • Um cluster Amazon ECS não de produção chamado `cicd-ecs-nonprod` • Um cluster Amazon ECS de produção chamado `cicd-ecs-prod`	

Tarefa	Descrição	Habilidades necessárias
Monitore a CloudFormation pilha da AWS.	1. Faça login no Console de Gerenciamento da AWS, abra o CloudFormation console da AWS e escolha a `cicd-vpc-ecs` pilha na lista. 2. No painel de detalhes da pilha, clique na guia Eventos e monitore o progresso da criação da pilha.	AWS DevOps, infraestrutura de nuvem

Tarefa	Descrição	Habilidades necessárias
Teste a CloudFormation pilha da AWS.	1. Depois que a CloudFormation pilha `cicd-vpc-ecs` da AWS for criada, certifique-se de que os `cicd-vpc-ecs/cicd-vpc-nonprod` e `cicd-vpc-ecs/cicd-vpc-prod` VPCs sejam criados. 2. Certifique-se de que os clusters `cicd-ecs-nonprod` e `cicd-ecs-prod` do Amazon ECS sejam criados. **Important** Certifique-se de registrar o IDs para os dois VPCs e o grupo de segurança IDs para os grupos de segurança padrão em ambos VPCs.	AWS DevOps, infraestrutura de nuvem

Crie um pipeline de CI/CD para um microsserviço

Tarefa	Descrição	Habilidades necessárias
Crie a infraestrutura para o microsserviço.	1. Nomeie o microsserviço. Por exemplo, esse padrão usa `myservice1` como o nome do microsserviço.	AWS DevOps, infraestrutura de nuvem

Tarefa	Descrição	Habilidades necessárias
	2. No diretório de trabalho, execute o comando `cd <working-directory>/cdkpipeline` . 3. Execute o comando `pip3 install -r requirements.txt` . 4. Execute o comando `cdk synth` completo que está disponível na seção Informações adicionais deste padrão. 5. Execute o comando `cdk deploy` completo que está disponível na seção Informações adicionais deste padrão. **Note** Você também pode fornecer os valores para ambos os comandos usando o `cdk.json` arquivo no diretório.	
Monitore a CloudFormation pilha da AWS.	Abra o CloudFormation console da AWS e monitore o progresso da `myservice1-cicd-stack` pilha. Eventualmente, o status muda para `CREATE_COMPLETE` .	AWS DevOps, infraestrutura de nuvem

Tarefa	Descrição	Habilidades necessárias
Teste a CloudFormation pilha da AWS.	1. No CodeCommit console da AWS, verifique se um repositório chamado `myservice1` existe e contém o código inicial. 2. No CodeBuild console da AWS, verifique se `myservice1` existe um projeto de construção chamado. 3. No console do Amazon ECR, verifique se um repositório Amazon ECR chamado `myservice1` existe. 4. No console do Amazon ECS, verifique se um serviço Fargate chamado `myservice1` existe em um cluster Amazon ECS não produtivo e de produção. 5. No console do Amazon Elastic Compute Cloud (Amazon EC2), verifique se os Application Load Balancers não produtivos e de produção foram criados. Registre os nomes DNS do ALBs. 6. No CodePipeline console da AWS, verifique se `myservice1` existe um	

Tarefa	Descrição	Habilidades necessárias
	pipeline chamado. Deve ter os estágios `Source`, `Build`, `Deploy-NonProd` e `Deploy-Prod`. O pipeline também deve ter um status `in progress`. 7. Monitore o pipeline até que todas as etapas estejam concluídas. 8. Aprove-o manualmente para produção. 9. Em uma janela do navegador, insira os nomes DNS do ALBs. 10. O aplicativo deve ser exibido `Hello World` na não produção e na produção URLs.	

Tarefa	Descrição	Habilidades necessárias
Use o pipeline.	1. Abra o CodeCommit repositório que você criou anteriormente e abra o `index.js` arquivo. 2. Substitua `Hello World` por `Hello CI/CD`. 3. Salve e confirme as alterações na ramificação principal. 4. Verifique se o pipeline é inicializado e se a alteração passa pelos estágios `Build`, `Deploy-NonProd` e `Deploy-Prod`. 5. Aprove a produção manualmente. 6. Tanto a produção quanto a não produção URLs devem agora ser exibidas *`Hello CICD`*.	AWS DevOps, infraestrutura de nuvem
Repita esse épico para cada microsserviço.	Repita as tarefas desse épico para criar um pipeline de CI/CD para cada um dos seus microsserviços.	AWS DevOps, infraestrutura de nuvem

Recursos relacionados

- Usando Python com o AWS CDK
- Referência do AWS CDK em Python
- Criação de um serviço AWS Fargate usando o AWS CDK

Mais informações

Comando da **`cdk synth`**

```
cdk synth --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production
 VPC> --context vpc_prod_id=<id_of_production_VPC> --context
 ecssg_nonprod_id=< default_security_group_id_of_non-production_VPC>
 --context ecssg_prod_id=<default_security_group_id_of_production_VPC>
 --context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

`cdk deploy` command

```
cdk deploy --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production_VPC>
 --context vpc_prod_id=<id_of_production_VPC> --context ecssg_nonprod_id=<
 default_security_group_id_of_non-production_VPC> --context
 ecssg_prod_id=<default_security_group_id_of_production_VPC> --
context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie uma arquitetura pouco acoplada com microsserviços usando DevOps práticas e o AWS Cloud9

Criado por Alexandre Nardi (AWS)

Resumo

Aviso: não AWS Cloud9 está mais disponível para novos clientes. Os clientes existentes do AWS Cloud9 podem continuar usando o serviço normalmente. Saiba mais

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão demonstra como desenvolver um aplicativo web típico em uma arquitetura sem servidor, para desenvolvedores e líderes de desenvolvimento que estão começando a testar DevOps práticas na Amazon Web Services (AWS). Ele cria um aplicativo de amostra que cria uma vitrine e um backend para navegar e comprar livros e fornece um microsserviço que pode ser desenvolvido de forma independente. O padrão usa o AWS Cloud9 como ambiente de desenvolvimento, um banco de dados do Amazon DynamoDB como armazenamento de dados e serviços da AWS, como AWS e AWS, para integração contínua CodePipeline e funcionalidade de implantação contínua (CodeBuild CI/CD).

O padrão orienta você nas seguintes atividades de desenvolvimento:

- Criar um ambiente de desenvolvimento do AWS Cloud9
- Usando CloudFormation modelos da AWS para criar um aplicativo web e um microsserviço para livros
- Usando o AWS Cloud9 para modificar o frontend, confirmar alterações e testar alterações
- Criando e testando um pipeline de CI/CD para o microsserviço
- Automatizando testes unitários

O código desse padrão é fornecido em GitHub, no repositório AWS DevOps End-to-End Workshop.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa

- Arquivos do AWS DevOps End-to-End Workshop baixados para o seu computador

> **Important**
>
> A criação desse aplicativo de demonstração em sua conta da AWS cria e consome recursos da AWS. Você é responsável pelo custo dos serviços e recursos da AWS usados para criar e executar o aplicativo. Depois de concluir seu trabalho, lembre-se de remover todos os recursos para evitar cobranças contínuas. Para obter instruções de limpeza, consulte a seção Épicos.

Limitações

Este passo a passo é destinado apenas para fins de demonstração e desenvolvimento. Para usá-lo em um ambiente de produção, consulte as melhores práticas de segurança na documentação do AWS Identity and Access Management (IAM) e faça as alterações necessárias nos perfis do IAM, no Amazon DynamoDB e em outros serviços usados. O aplicativo web é derivado do aplicativo de demonstração do AWS Bookstore; para considerações adicionais, consulte a seção Limitações conhecidas do arquivo README.

Arquitetura

A arquitetura do aplicativo da livraria é ilustrada na seção Arquitetura do arquivo README do aplicativo de demonstração do AWS Bookstore.

Do ponto de vista da implantação, o aplicativo Bookstore Demo usa um único CloudFormation modelo para implantar todos os serviços e objetos em uma única pilha. Esse padrão faz algumas alterações para demonstrar como um determinado desenvolvedor ou equipe poderia trabalhar em um produto específico (livros) e atualizá-lo independentemente do resto do aplicativo. Por esse motivo, o código desse padrão separa as funções do AWS Lambda e os objetos relacionados do microsserviço Books em um CloudFormation segundo modelo, que cria uma pilha de livros. Isso possibilita ver o microsserviço sendo atualizado usando práticas de CI/CD. No diagrama a seguir, a borda tracejada identifica o microsserviço Books.

Ferramentas

Ferramentas

- Estrutura Jest para testes JavaScript
- Python 3.9

Código

O código-fonte e os modelos desse padrão estão disponíveis no GitHub repositório AWS DevOps End-to-End Workshop. Antes de seguir as etapas na seção Épicos, baixe todos os arquivos do repositório para o seu computador.

> **Note**
>
> A seção Epics fornece as etapas de alto nível para este passo a passo, para fornecer informações gerais sobre o processo. Para concluir cada etapa, consulte o arquivo README no repositório do AWS DevOps End-to-End Workshop para obter instruções detalhadas.

O repositório do AWS DevOps End-to-End Workshop estende o repositório do aplicativo de demonstração do AWS Bookstore e usa uma versão modificada do código AWS Cloud9 Bootstrapping para criar o AWS Cloud9 IDE.

Práticas recomendadas

Usar o aplicativo Bookstore é simples. Aqui estão algumas das melhores práticas recomendadas:

- Ao instalar o aplicativo, você pode usar um nome de projeto de sua escolha ou usar o nome padrão (`demobookstore`) por conveniência.
- Depois de instalar e executar o aplicativo, é uma boa prática desligar o banco de dados Amazon Neptune se você quiser continuar testando por mais um dia, pois a instância do banco de dados pode resultar em cobranças adicionais. No entanto, esteja ciente de que o banco de dados será iniciado automaticamente após sete dias.
- Para obter detalhes do código, consulte a documentação do repositório do aplicativo de demonstração do AWS Bookstore. Ela descreve cada microsserviço e tabela.
- Para obter melhores práticas adicionais, consulte Alguns desafios se você tiver tempo... seção do arquivo README no repositório do AWS DevOps End-to-End Workshop. Recomendamos que você analise as informações para se aprofundar nos recursos adicionais de segurança e praticar serviços de dissociação.

Épicos

Fazer download do código-fonte

Tarefa	Descrição	Habilidades necessárias
Baixe o código-fonte em GitHub.	O código-fonte e os modelos desse padrão estão disponíveis em GitHub, no repositório do AWS DevOps End-to-End Workshop. Antes de seguir as próximas etapas na seção Épicos, baixe todos os arquivos do repositório para o seu computador. **Note** A seção Epics fornece as etapas de alto nível para este passo a passo, para fornecer informações gerais sobre o processo. Para concluir cada etapa, consulte o arquivo README no repositório do AWS DevOps End-to-End Workshop para obter instruções detalhadas. O repositório do AWS DevOps End-to-End Workshop estende o repositório do aplicativo de demonstração do AWS	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Bookstore e usa uma versão modificada do código AWS Cloud9 Bootstrapping para criar o AWS Cloud9 IDE.	

Crie o aplicativo web do Bookstore e o microsserviço Books

Tarefa	Descrição	Habilidades necessárias
Crie as funções do Lambda e de frontend para o aplicativo Bookstore.	1. Faça login no CloudFormation console e implante o `DemoBookstoreMainTemplate.yml` modelo para criar a DemoBookStoreStack pilha. Isso cria as funções de frontend e Lambda que estão fora do microsserviço Books. 2. Na guia Saídas da pilha, anote o URL do site abaixo do WebApplicationrótulo.	Desenvolvedor
Crie o microsserviço Books.	No CloudFormation console, implante o `DemoBooksToreBooksServiceTemplate.yml` modelo para criar a DemoBooksServiceStack pilha.	Desenvolvedor
Teste seu aplicativo.	Use o URL do site da DemoBookStoreStack pilha para acessar o aplicativo Bookstore.	Desenvolvedor

Use o ambiente do Cloud9 para manter seu aplicativo

Tarefa	Descrição	Habilidades necessárias
Crie um AWS Cloud9 IDE.	No CloudFormation console, implante o `C9EnvironmentTemplate.yml` modelo para criar um ambiente AWS Cloud9.	Desenvolvedor, líder de desenvolvimento
Crie CodeCommit repositórios.	1. Faça login no CodeCommit console da AWS e verifique se você tem um `demobookstore-WebAssets` repositório que contém o código do aplicativo front-end. 2. Crie um repositório para o microsserviço Books chamado `demobookstore-BooksService` . 3. Clone os dois repositórios no AWS Cloud9 (`demobookstore-WebAssets` e `demobookstore-BooksService`) usando o comando `git clone`.	Desenvolvedor
Altere o código no frontend e verifique o pipeline.	1. Use o AWS Cloud9 para fazer algumas alterações no código em uma página da web. Isso atualizará o repositório `demobookstore-WebAssets` . 2. No CodePipeline console da AWS, verifique se o	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	DemoBookstore-Assets-Pipeline está em execução. 3. Teste seu aplicativo web atualizando-o no navegador (Ctrl+F5 no Firefox).	

Implemente um pipeline de CI/CD para o microsserviço Books

Tarefa	Descrição	Habilidades necessárias
Adicione os arquivos YAML para a compilação e a atualização do serviço.	1. No AWS Cloud9, faça o upload dos arquivos `buildspec.yml` e `DemoBookstoreBooksServiceUpdateTemplate.yml`. • `buildspec.yml` tem instruções de construção e também inclui instruções de teste para testes automatizados. Eles são comentados neste momento e serão usados posteriormente. • `DemoBookstoreBooksServiceUpdateTemplate.yml` é uma versão atualizada do `DemoBookstoreBooksServiceTemplate.yml`, para ser usada no estágio de implantação do pipeline.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	2. Faça commit e envie os arquivos.	
Crie um bucket do S3 para o pipeline de compilação.	Para criar um bucket do S3, siga as instruções na documentação do Amazon S3. • O nome do bucket deve ser exclusivo globalmente, por exemplo, `demobookstore-books-service-pipeline-bucket-<YYYYMMDDHHMM>`. • Desmarque a caixa de seleção Bloquear todo o acesso público e marque a caixa de seleção Eu reconheço...	Desenvolvedor
Use o IAM para criar uma função para CloudFormation implantação.	Crie uma função `demobookstore-CloudFormation-role` a anexe-a à política `AdministratorAccess`. No próximo épico, você pode reconfigurar essa função para obter permissões mínimas.	Desenvolvedor
Crie um novo pipeline para automatizar a criação e a implantação do microsserviço Books.	Crie um funil (por exemplo, demobookstore- BooksService -Pipeline) com os estágios Commit, Build e Deploy, conforme descrito no arquivo README.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Teste seu microsserviço no AWS Cloud9.	Faça uma alteração na ListBooksfunção e veja o pipeline funcionando.	Desenvolvedor
Automatize o teste unitário para a função ListBooks Lambda.	No AWS Cloud9 IDE, habilite a compilação para executar testes unitários e verificar os resultados do teste. Para obter instruções, consulte o arquivo README.	Desenvolvedor

(Opcional) Implementar funcionalidade adicional

Tarefa	Descrição	Habilidades necessárias
Torne sua solução segura.	Configure `demobookstore-CloudFormation-role` para ter permissões mínimas e verifique também outras funções usadas.	Desenvolvedor
Elimine dependências nos CloudFormation modelos.	O método para trocar informações entre o modelo `DemoBooks toreMainTemplate.y ml` e o modelo `DemoBooks toreBooksServiceTe mplate.yml` é baseado em saídas e importações. A passagem de valores entre esses dois modelos adiciona dependências. Para eliminar as dependências, considere	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	usar o AWS Systems Manager Parameter Store.	
Crie um microsserviço Cart.	Use o microsserviço Books como exemplo para retirar as funções relacionadas ao carrinho de compras do modelo `DemoBookStoreMainTemplate.yml` e criar um microsserviço de carrinho de compras.	Desenvolvedor

Limpeza

Tarefa	Descrição	Habilidades necessárias
Exclua os buckets do S3.	No console do Amazon S3, exclua os seguintes buckets associados ao aplicativo web de amostra: • Dois buckets criados para o aplicativo de demonstração da AWS Bookstore. Os nomes dos buckets começam com o nome da pilha que você forneceu para a AWS CloudFormation quando criou o front-end; por exemplo,. DemoBookStoreStack • <YYYYMMDDHHMM>Um bucket para o pipeline de construção; por exemplo,	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	demobookstore-books-service-pipeline-bucket-.	
Exclua as pilhas.	No CloudFormation console, exclua as pilhas associadas ao aplicativo web de amostra: • DemoBooksServiceStack • DemoBookStoreStack A remoção pode levar mais de 90 minutos. Se a remoção falhar, exclua-os novamente e também exclua todos os recursos manuais (por exemplo, a VPC ou as interfaces de rede) com base nas notificações.	Desenvolvedor
Excluas os perfis do IAM.	No console do IAM, exclua as seguintes funções: • `demobookstore-Cloudformation-role` • `demobookstore-BooksService-BuildProject-service-role` Para step-by-step obter instruções, consulte a documentação do IAM.	Desenvolvedor

Recursos relacionados

- Aplicativo de demonstração do AWS Bookstore
- Exemplo de AWS Cloud9 Bootstrapping
- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- Criação de um bucket (documentação do Amazon S3)

Mais informações

Para obter step-by-step instruções detalhadas, consulte o arquivo README no GitHub repositório do AWS DevOps End-to-End Workshop.

Sobre a atualização de maio de 2023: esse padrão foi atualizado para usar versões mais recentes do Node e do Python. Atualizamos muitos dos pacotes no código-fonte e removemos o Glyphicon porque ele não é mais gratuito. Também removemos todas as dependências do repositório do aplicativo de demonstração do AWS Bookstore, para que os dois repositórios agora possam evoluir de forma independente.

Crie e envie imagens do Docker para o Amazon ECR usando GitHub Actions e Terraform

Criado por Ruchika Modi (AWS)

Resumo

Esse padrão explica como você pode criar GitHub fluxos de trabalho reutilizáveis para criar seu Dockerfile e enviar a imagem resultante para o Amazon Elastic Container Registry (Amazon ECR). O padrão automatiza o processo de criação de seus Dockerfiles usando o Terraform e o Actions. GitHub Isso minimiza a possibilidade de erro humano e reduz substancialmente o tempo de implantação.

Uma ação GitHub push para a ramificação principal do seu GitHub repositório inicia a implantação dos recursos. O fluxo de trabalho cria um repositório Amazon ECR exclusivo com base na combinação da GitHub organização e do nome do repositório. Em seguida, ele envia a imagem do Dockerfile para o repositório Amazon ECR.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma GitHub conta ativa.
- Um GitHub repositório.
- Terraform versão 1 ou posterior instalado e configurado.
- Um bucket do Amazon Simple Storage Service (Amazon S3) para o back-end do Terraform.
- Uma tabela do Amazon DynamoDB para bloqueio e consistência do estado do Terraform. A tabela deve ter uma chave de partição nomeada `LockID` com um tipo de`String`. Se isso não estiver configurado, o bloqueio de estado será desativado.
- Uma função do AWS Identity and Access Management (IAM) que tem permissões para configurar o back-end do Amazon S3 para o Terraform. Para obter instruções de configuração, consulte a documentação do Terraform.

Limitações

Esse código reutilizável foi testado somente com GitHub Actions.

Arquitetura

Pilha de tecnologias de destino

- Repositório do Amazon ECR
- GitHub Ações
- Terraform

Arquitetura de destino

O diagrama ilustra o seguinte:

1. Um usuário adiciona modelos do Dockerfile e do Terraform ao repositório. GitHub

2. Essas adições iniciam um fluxo de trabalho de GitHub ações.

3. O fluxo de trabalho verifica se existe um repositório Amazon ECR. Caso contrário, ele cria o repositório com base na GitHub organização e no nome do repositório.

4. O fluxo de trabalho cria o Dockerfile e envia a imagem para o repositório Amazon ECR.

Ferramentas

Serviço da Amazon

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de contêineres seguro, escalável e confiável.

Outras ferramentas

- GitHub O Actions é integrado à GitHub plataforma para ajudar você a criar, compartilhar e executar fluxos de trabalho em seus GitHub repositórios. Você pode usar o GitHub Actions para automatizar tarefas como criar, testar e implantar seu código.
- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar a infraestrutura na nuvem e no local.

Repositório de código

O código desse padrão está disponível no repositório GitHub Docker ECR Actions Workflow.

- Quando você cria GitHub ações, os arquivos do fluxo de trabalho do Docker são salvos na `/.github/workflows/` pasta desse repositório. O fluxo de trabalho dessa solução está no arquivo workflow.yaml.
- A `e2e-test` pasta fornece um exemplo de Dockerfile para referência e teste.

Práticas recomendadas

- Para ver as melhores práticas para escrever Dockerfiles, consulte a documentação do Docker.
- Use um VPC endpoint para o Amazon ECR. Os VPC endpoints são desenvolvidos pela AWS PrivateLink, uma tecnologia que permite que você acesse o Amazon APIs ECR de forma privada por meio de endereços IP privados. Para tarefas do Amazon ECS que usam o tipo de execução Fargate, o VPC endpoint permite que a tarefa extraia imagens privadas do Amazon ECR sem atribuir um endereço IP público à tarefa.

Épicos

Configurar o provedor e o repositório do OIDC GitHub

Tarefa	Descrição	Habilidades necessárias
Configure o OpenID Connect.	Crie um provedor OpenID Connect (OIDC). Você usará o provedor na política de confiança para a função do IAM usada nessa ação. Para obter instruções, consulte Configuração do OpenID Connect na Amazon Web Services GitHub na documentação.	Administrador da AWS, AWS DevOps, AWS geral
Clone o GitHub repositório.	Clone o repositório GitHub Docker ECR Actions Workflow em sua pasta local: `$git clone https://g ithub.com/aws-samp`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`les/docker-ecr-act ions-workflow`	

Personalize o fluxo de trabalho GitHub reutilizável e implante a imagem do Docker

Tarefa	Descrição	Habilidades necessárias
Personalize o evento que inicia o fluxo de trabalho do Docker.	O fluxo de trabalho dessa solução está em workflow.yaml. Atualmente, esse script está configurado para implantar recursos ao receber o `workflow_dispatch` evento. Você pode personalizar essa configuração alterando o evento para `workflow_call` e chamando o fluxo de trabalho de outro fluxo de trabalho principal.	DevOps engenheiro
Personalize o fluxo de trabalho.	O arquivo workflow.yaml está configurado para criar um fluxo de trabalho dinâmico e reutilizável. GitHub Você pode editar esse arquivo para personalizar a configuração padrão ou pode passar os valores de entrada do console GitHub Actions se estiver usando o `workflow_dispatch` evento para iniciar a implantação manualmente.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	• Certifique-se de especificar o ID da conta da AWS e a região de destino corretos.
	• Crie uma política de ciclo de vida do Amazon ECR (veja exemplo de política) e atualize o caminho padrão (`e2e-test/policy.json`) adequadamente.
	• O arquivo do fluxo de trabalho exige duas funções do IAM como entrada:
	  • Uma função do IAM que tem permissões para configurar o back-end do Amazon S3 para o Terraform (consulte a seção Pré-requisitos). Você pode atualizar o nome da função padrão `workload-assumable-role` no. `yaml`arquive adequadamente.
	  • Uma função do IAM que tem permissões de acesso GitHub. Essa função também é usada na política do Amazon ECR para restringir as operações do Amazon ECR. Para obter mais informações, consulte o arquivo data.tf.	

Tarefa	Descrição	Habilidades necessárias
Implante os modelos do Terraform.	O fluxo de trabalho implanta automaticamente os modelos do Terraform que criam o repositório Amazon ECR, com base no evento que você configurou. GitHub Esses modelos estão disponíveis como `.tf` arquivos na raiz do repositório Github.	AWS DevOps, DevOps engenheiro

Solução de problemas

Problema	Solução
Problemas ou erros ao configurar o Amazon S3 e o DynamoDB como o back-end remoto do Terraform.	Siga as instruções na documentação do Terraform para configurar as permissões necessárias nos recursos do Amazon S3 e do DynamoDB para a configuração do back-end remoto.
Não é possível executar ou iniciar o fluxo de trabalho com o `workflow_dispatch` evento.	O fluxo de trabalho configurado para implantação a partir do `workflow_dispatch` evento funcionará somente se o fluxo de trabalho também estiver configurado na ramificação principal.

Recursos relacionados

- Reutilização de fluxos de trabalho (documentação) GitHub
- Acionando um fluxo de trabalho (documentação) GitHub

Crie e teste aplicativos iOS com AWS CodeCommit CodePipeline, AWS e AWS Device Farm

Criado por Abdullahi Olaoye (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão descreve as etapas para criar um pipeline de integração contínua e entrega contínua (CI/CD) que usa CodePipeline a AWS para criar e testar aplicativos iOS em dispositivos reais na AWS. O padrão usa CodeCommit a AWS para armazenar o código do aplicativo, a ferramenta de código aberto Jenkins para criar o aplicativo iOS e o AWS Device Farm para testar o aplicativo criado em dispositivos reais. Essas três fases são orquestradas juntas em um pipeline usando a AWS. CodePipeline

Esse padrão é baseado na postagem Criando e testando aplicativos iOS e iPadOS com a AWS DevOps e serviços móveis no DevOps blog da AWS. Para obter instruções detalhadas, consulte a postagem do blog.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma conta de desenvolvedor da Apple
- Servidor de compilação (macOS)
- Xcode versão 11.3 (instalado e configurado no servidor de compilação)
- AWS Command Line Interface (AWS CLI), instalada e configurada na estação de trabalho
- Conhecimento básico do Git

Limitações

- O servidor de compilação do aplicativo deve estar executando o macOS.
- O servidor de compilação deve ter um endereço IP público, para que CodePipeline possa se conectar a ele remotamente para iniciar as compilações.

Arquitetura

Pilha de tecnologia de origem

- Um processo de criação de aplicativo iOS on-premises que envolve o uso de um simulador ou teste manual em dispositivos físicos

Pilha de tecnologias de destino

- Um CodeCommit repositório da AWS para armazenar o código-fonte do aplicativo
- Um servidor Jenkins para compilações de aplicativos usando o Xcode
- Um pool de dispositivos do AWS Device Farm para testar aplicativos em dispositivos reais

Arquitetura de destino

Quando um usuário confirma alterações no repositório de origem, o pipeline CodePipeline (AWS) busca o código do repositório de origem, inicia uma compilação do Jenkins e passa o código do aplicativo para o Jenkins. Após a construção, o pipeline recupera o artefato de construção e inicia um trabalho do AWS Device Farm para testar o aplicativo em um pool de dispositivos.

Ferramentas

- CodePipelineA AWS é um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura. CodePipeline automatiza as fases de criação, teste e implantação do seu processo de lançamento sempre que houver uma alteração no código, com base no modelo de lançamento que você define.
- CodeCommitA AWS é um serviço de controle de origem totalmente gerenciado que hospeda repositórios seguros baseados em Git. Isso facilita a colaboração das equipes no código em um ecossistema seguro e altamente escalável. CodeCommit elimina a necessidade de operar seu próprio sistema de controle de origem ou a preocupação com a escalabilidade de sua infraestrutura.
- O AWS Device Farm é um serviço de teste de aplicativos que permite melhorar a qualidade de seus aplicativos móveis e da web testando-os em uma ampla variedade de navegadores de desktop e dispositivos móveis reais, sem precisar provisionar e gerenciar nenhuma infraestrutura de teste.

- Jenkins: é um servidor de automação de código aberto que permite aos desenvolvedores construir, testar e implantar seu software.

Épicos

Configurar o ambiente de construção

Tarefa	Descrição	Habilidades necessárias
Instale o Jenkins no servidor de compilação que está executando o macOS.	O Jenkins será usado para criar o aplicativo, portanto, primeiro você deve instalá-lo no servidor de compilação. Para obter instruções detalhadas para essa tarefa e para as tarefas subsequentes, consulte a postagem do blog da AWS Criando e testando aplicativos iOS DevOps e iPadOS com a AWS e serviços móveis e outros recursos na seção Recursos relacionados no final desse padrão.	DevOps
Configure o Jenkins.	Siga as instruções da tela para configurar o Jenkins.	DevOps
Instale o CodePipeline plug-in da AWS para Jenkins.	Esse plug-in deve ser instalado no servidor Jenkins para que o Jenkins interaja com o serviço da AWS CodePipeline .	DevOps
Crie um projeto de estilo livre no Jenkins.	No Jerkins, crie um projeto de estilo livre. Configure o projeto para especificar acionadores e	DevOps

Tarefa	Descrição	Habilidades necessárias
	outras opções de configuração de compilação.	

Configurar o AWS Device Farm

Tarefa	Descrição	Habilidades necessárias
Crie um projeto Device Farm.	Abra o console do AWS Device Farm. Crie um projeto e um pool de dispositivos para testes. Para obter instruções, consulte a publicação do blog.	Desenvolvedor

Configurar o repositório de origem

Tarefa	Descrição	Habilidades necessárias
Crie um CodeCommit repositório.	Crie um repositório onde o código-fonte será armazenado.	DevOps
Confirma o código do seu aplicativo para o repositório.	Conecte-se ao CodeCommit repositório que você criou. Enviar o código de sua máquina local para o repositório.	DevOps

Configure o pipeline

Tarefa	Descrição	Habilidades necessárias
Crie um pipeline na AWS CodePipeline.	Abra o CodePipeline console da AWS e crie um pipeline.	DevOps

Tarefa	Descrição	Habilidades necessárias
	O pipeline orquestra todas as fases do processo de CI/CD. Para obter instruções, consulte a postagem do blog da AWS Criando e testando aplicativos iOS e iPadOS com a AWS DevOps e serviços móveis.	
Adicionar um estágio de teste ao pipeline.	Para adicionar um estágio de teste e integrá-lo ao AWS Device Farm, edite o pipeline.	DevOps
Inicie o pipeline.	Para iniciar o pipeline e o processo de CI/CD, escolha Release change.	DevOps

Veja os resultados dos testes de aplicativos

Tarefa	Descrição	Habilidades necessárias
Revisar os resultados do teste.	No console do AWS Device Farm, selecione o projeto que você criou e analise os resultados dos testes. O console mostrará os detalhes de cada teste.	Desenvolvedor

Recursos relacionados

Step-by-step instruções para esse padrão

- Criação e teste de aplicativos iOS e iPadOS com a AWS DevOps e serviços móveis (publicação DevOps no blog da AWS)

Configurar o AWS Device Farm

- Console AWS Device Farm

Configurar o repositório de origem

- Crie um CodeCommit repositório da AWS
- Conecte-se a um CodeCommit repositório da AWS

Configurar o pipeline

- CodePipeline Console da AWS

Recursos adicionais

- CodePipeline Documentação da AWS
- CodeCommit Documentação da AWS
- Documentação do AWS Device Farm
- Documentação do Jenkins
- Instalação do Jenkins no macOS
- CodePipeline Plug-in AWS para Jenkins
- Instalação do Xcode
- Instalação e configuração da AWS CLI
- Documentação do Git

Verifique os aplicativos ou CloudFormation modelos do AWS CDK para obter as melhores práticas usando pacotes de regras cdk-nag

Criado por Arun Donti

Resumo

Este padrão explica como você pode usar o utilitário cdk-nag para verificar as práticas recomendadas dos aplicativos do AWS Cloud Development Kit (AWS CDK) usando uma combinação de pacotes de regras. O cdk-nag é um projeto de código aberto inspirado no cfn_nag. Ele implementa regras em pacotes de avaliação, como a Biblioteca de Soluções da AWS, a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) e o Instituto Nacional de Padrões e Tecnologia (NIST) 800-53 usando AWS CDK Aspects. Você pode verificar as práticas recomendadas em seus aplicativos AWS CDK usando as regras desses pacotes, detectar e corrigir o código com base nas práticas recomendadas e suprimir as regras que você não deseja usar em suas avaliações.

Você também pode usar cdk-nag para verificar seus CloudFormation modelos da AWS usando o módulo cloudformation-include.

Para obter informações sobre todos os pacotes disponíveis, consulte a seção Regras do repositório cdk-nag. Os pacotes de avaliação estão disponíveis para:

- Biblioteca de soluções da AWS
- Segurança HIPAA
- NIST 800-53 rev 4
- NIST 800-53 rev 5
- Payment Card Industry Data Security Standard (PCI DSS) 3.2.1

Pré-requisitos e limitações

Pré-requisitos

- Um aplicativo que usa o AWS CDK

Ferramentas

- O AWS CDK — Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software para definir a infraestrutura de nuvem em código e provisioná-la por meio da AWS. CloudFormation
- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e suas dependências, além de iniciá-los e configurá-los juntos como uma pilha, em vez de gerenciar os recursos individualmente. Você pode gerenciar e provisionar pilhas em várias contas e regiões da AWS.

Épicos

Integrar o cdk-nag com seu aplicativo AWS CDK

Tarefa	Descrição	Habilidades necessárias
Saiba mais sobre cdk-nag.	Navegue até o GitHub repositório cdk-nag e leia a documentação.	Desenvolvedor de aplicativos
Instale o pacote cdk-nag em seu aplicativo AWS CDK.	Para usar o cdk-nag em seu aplicativo de CDK da AWS, você deve instalá-lo primeiro. O cdk-nag está disponível para download no PyPI, npm e Apache Maven. NuGet Para obter as informações mais recentes sobre as versões disponíveis e os locais de download, consulte o Arquivo leiame no repositório.	Desenvolvedor de aplicativos
Escolha o seu NagPacks.	cdk-nag tem diferentes pacotes de regras chamados. NagPacks Cada um NagPack contém regras que estão em	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	conformidade com um padrão específico. Por exemplo, as soluções da AWS NagPack contêm as melhores práticas gerais, e o NIST 800-53 rev 5 NagPack pode ajudar na conformidade. Você pode aplicar vários pacotes NagPacks ao seu aplicativo e adicionar e remover pacotes conforme necessário. Para obter uma lista dos pacotes disponíveis, consulte o arquivo Readme no GitHub repositório. Para obter informações sobre as regras individuais em cada pacote, consulte a seção Regras do GitHub repositório.	

Tarefa	Descrição	Habilidades necessárias

Integre o cdk-nag ao seu aplicativo AWS CDK.	Você pode integrar o cdk-nag em seu aplicativo no nível de todo o aplicativo ou integrá-lo em estágios ou pilhas individuais no seu aplicativo. Por exemplo, para integrar as soluções da AWS e a segurança da HIPAA NagPacks em um aplicativo AWS CDK v2 em nível de todo o TypeScript aplicativo, você pode usar o seguinte código:
	`import { App, Aspects } from 'aws-cdk-lib';`
	`import { CdkTestStack } from '../lib/cdk-test-stack';`
	`import { AwsSolutionsChecks, HIPAASecurityChecks } from 'cdk-nag';`
	
	`const app = new App();`
	`new CdkTestStack(app, 'CdkNagDemo');`
	`// Simple rule informational messages`
	`Aspects.of(app).add(new AwsSolutionsChecks());`
	`// Additional explanations on the purpose of triggered rules`
	`Aspects.of(app).add(new HIPAASecurityChecks({ verbose: true }));`
		Desenvolvedor de aplicativos

Recursos relacionados

- Repositório de código cdk-nag
- cdk-nag no Construct Hub

Configurar a autenticação de TLS mútuo para aplicativos em execução no Amazon EKS

Criado por Mahendra Siddappa (AWS)

Resumo

O Transport Layer Security (TLS) mútuo baseado em certificado é um componente opcional do TLS que fornece autenticação bidirecional entre servidores e clientes. Com o TLS mútuo, os clientes devem fornecer um certificado X.509 durante o processo de negociação da sessão. O servidor usa esse certificado para identificar e autenticar o cliente.

O TLS mútuo é um requisito comum para aplicativos da Internet das Coisas (IoT) e pode ser usado business-to-business para aplicativos ou padrões como o Open Banking.

Esse padrão descreve como configurar o TLS mútuo para aplicativos em execução em um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) usando um controlador de entrada NGINX. Você pode habilitar atributos de TLS mútuos integrados para o controlador de entrada NGINX anotando o recurso de entrada. Para obter mais informações sobre anotações de TLS mútuas em controladores NGINX, consulte Autenticação de certificado de cliente na documentação do Kubernetes.

> **Important**
>
> Esse padrão usa certificados autoassinados. Recomendamos que você use esse padrão apenas com clusters de teste e não em ambientes de produção. Se quiser usar esse padrão em um ambiente de produção, você pode usar a AWS Private Certificate Authority (AWS Private CA) ou seu padrão existente de infraestrutura de chave pública (PKI) para emitir certificados privados.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS).
- Um cluster do Amazon EKS existente.
- AWS Command Line Interface (AWS CLI) versão 1.7 ou superior, instalada e configurada no macOS, Linux ou Windows.

- O utilitário de linha de comando kubectl, instalado e configurado para acessar o cluster do Amazon EKS. Para obter mais informações , consulte Instalação do kubectl na documentação do Amazon EKS.
- Um nome de Sistema de Nomes de Domínio (DNS) existente para testar o aplicativo.

Limitações

- Esse padrão usa certificados autoassinados. Recomendamos que você use esse padrão apenas com clusters de teste e não em ambientes de produção.

Arquitetura

Pilha de tecnologia

- Amazon EKS
- Amazon Route 53
- Kubectl

Ferramentas

- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.
- Kubectl é um utilitário de linha de comando que você usa para interagir com um cluster do Amazon EKS.

Épicos

Gerar os certificados autoassinados

Tarefa	Descrição	Habilidades necessárias
Gerar o certificado e a chave de CA.	Gere a chave e o certificado da autoridade de certificação	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	(CA) executando o comando a seguir. `openssl req -x509 -sha256 -newkey rsa:4096 -keyout ca.key -out ca.crt -days 356 -nodes -subj '/CN=Test Cert Authority'`	
Gerar a chave e o certificado do servidor e assinar com o certificado CA.	Gerar a chave e o certificado do servidor e assinar com o certificado CA, executando o seguinte comando. `openssl req -new -newkey rsa:4096 -keyout server.key -out server.csr -nodes -subj '/CN= <your_domain_name> ' && openssl x509 -req -sha256 -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt` **Important** Certifique-se de substituir pelo nome `<your_domain_name>` de domínio existente.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Gerar a chave e o certificado de cliente e assinar com o certificado CA.	Gere a chave e o certificado do cliente e assine com o certificado CA, executando os seguintes comandos. `openssl req -new -newkey rsa:4096 -keyout client.key -out client.csr -nodes -subj '/CN=Test' && openssl x509 -req -sha256 -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -out client.crt`	DevOps engenheiro

Implementar o controlador de entrada NGINX

Tarefa	Descrição	Habilidades necessárias
Implantar o controlador de entrada do NGINX no seu cluster do Amazon EKS.	Implante o controlador de entrada do NGINX com o comando a seguir. `kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-v1.7.0/deploy/static/provider/aws/deploy.yaml`	DevOps engenheiro
Verificar se o serviço do controlador de entrada do NGINX está em execução.	Verifique se o serviço do controlador de entrada do NGINX está em execução.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`kubectl get svc -n ingress-nginx` **Important** Certifique-se de que o campo de endereço do serviço contenha o nome de domínio do Network Load Balancer.	

Criar um namespace no cluster do Amazon EKS para testar o TLS mútuo

Tarefa	Descrição	Habilidades necessárias
Criar um namespace no cluster do Amazon EKS.	Crie um namespace chamado `mtls` no seu cluster do Amazon EKS, executando o comando a seguir. `kubectl create ns mtls` Isso implanta o aplicativo de exemplo para testar o TLS mútuo.	DevOps engenheiro

Criar a implantação e o serviço para o aplicativo de exemplo

Tarefa	Descrição	Habilidades necessárias

Criar a implantação e o serviço do Kubernetes no namespace mtls.	Crie um arquivo chamado `mtls.yaml` . Cole o seguinte código no arquivo.
	
	`kind: Deployment`
	`apiVersion: apps/v1`
	`metadata:`
	`  name: mtls-app`
	`  labels:`
	`  app: mtls`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app: mtls`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: mtls`
	`  spec:`
	`  containers:`
	`  - name: mtls-app`
	`  image: hashicorp/http-echo`
	`  args:`
	`  - "-text=mTLS is working"`
	
	`---`
	
	`kind: Service`
	`apiVersion: v1`
	`metadata:`
	`  name: mtls-service`
	`spec:`
	`  selector:`
	`  app: mtls`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre>ports:
	  - port: 5678 #
	Default port for image</pre>
	Crie a implantação e o serviço do Kubernetes no `mtls` namespace, executando o comando a seguir.
	<pre>kubectl create -f
	mtls.yaml -n mtls</pre>	

Verificar se a implantação do Kubernetes foi criada.	Execute o comando a seguir para verificar se a implantação foi criada e se tem um pod no status disponível.
	<pre>kubectl get deploy -n
	mtls</pre>
		DevOps engenheiro

Verificar se o serviço Kubernetes foi criado.	Verifique se o serviço do Kubernetes foi criado, executando o comando a seguir.
	<pre>kubectl get service -n
	mtls</pre>
		DevOps engenheiro

Criar um segredo no namespace mtls

Tarefa	Descrição	Habilidades necessárias
Criar um segredo para o recurso de entrada.	Execute o comando a seguir para criar um segredo para o controlador de entrada NGINX	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	usando os certificados que você criou anteriormente. `kubectl create secret generic mtls-certs --from-file=tls.crt=server.crt --from-file=tls.key=server.key --from-file=ca.crt=ca.crt -n mtls` Seu segredo tem um certificado de servidor para o cliente identificar o servidor e um certificado CA para o servidor verificar os certificados do cliente.	

Criar o recurso de entrada no namespace mtls

Tarefa	Descrição	Habilidades necessárias

Criar o recurso de ingresso no namespace mtls.	Crie um arquivo chamado `ingress.yaml` . Cole o código a seguir no arquivo (substitua `<your_domain_name>` pelo nome de domínio existente).
	
	`apiVersion: networking.k8s.io/v1`
	`kind: Ingress`
	`metadata:`
	`  annotations:`
	`  nginx.ingress.kubernetes.io/auth-tls-verify-client: "on"`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre> nginx.ingress.kube
	rnetes.io/auth-tls-
	secret: mtls/mtls-certs
	  name: mtls-ingress
	spec:
	  ingressClassName:
	 nginx
	  rules:
	  - host: "*.<your_
	domain_name>"
	    http:
	      paths:
	      - path: /
	        pathType: Prefix
	        backend:
	          service:
	            name: mtls-
	service
	            port:
	              number:
	 5678
	  tls:
	  - hosts:
	    - "*.<your_
	domain_name>"
	    secretName: mtls-
	certs</pre>	

	Crie o recurso de entrada no namespace `mtls` executando o comando a seguir.
	
	<pre>kubectl create -f
	 ingress.yaml -n mtls</pre>	

	Isso significa que o controlador de ingresso NGINX pode rotear o tráfego para seu aplicativo de exemplo.	

Tarefa	Descrição	Habilidades necessárias
Verificar se o recurso de ingresso foi criado.	Verifique se o recurso de ingresso foi criado, executando o comando a seguir. `kubectl get ing -n mtls` **Important** Certifique-se de que o endereço do recurso de entrada mostre o balanceador de carga criado para o controlador de entrada NGINX.	DevOps engenheiro

Configurar o DNS para apontar o nome do host para o balanceador de carga

Tarefa	Descrição	Habilidades necessárias
Criar um registro CNAME que aponte para o balanceador de carga do controlador de entrada NGINX.	Faça login no Console de Gerenciamento da AWS, abra o console do Amazon Route 53 e crie um registro de nome canônico (CNAME) que aponta `mtls.<your_domain_name>` para o balanceador de carga do controlador de entrada NGINX. Para obter informações, consulte Criar registros usando o console do Route 53	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	no Guia do desenvolvedor do Amazon Route 53.	

Teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Testar a configuração de TLS mútuo sem certificados.	Execute o seguinte comando: `curl -k https://mtls.<your_domain_name>` Você deve receber a resposta de erro “400 Nenhum certificado SSL obrigatório foi enviado”.	DevOps engenheiro
Testar a configuração de TS mútuo com certificados.	Execute o seguinte comando: `curl -k https://mtls.<your_domain_name> --cert client.crt --key client.key` Você deve receber a resposta “O mTLS está processando”.	DevOps engenheiro

Recursos relacionados

- Criar registros usando o console do Amazon Route 53
- Usar um Network Load Balancer com o controlador de entrada NGINX no Amazon EKS
- Autenticação de certificado de cliente

Automatize a criação de recursos AppStream 2.0 usando a AWS CloudFormation

Criado por Ram Kandaswamy (AWS)

Resumo

Esse padrão fornece exemplos de código e etapas para automatizar a criação de recursos da Amazon AppStream 2.0 na nuvem da Amazon Web Services (AWS) usando um CloudFormation modelo da AWS. O padrão mostra como usar uma CloudFormation pilha da AWS para automatizar a criação de seus recursos de aplicativos AppStream 2.0, incluindo um construtor de imagens, imagem, instância de frota e pilha. Você pode transmitir seu aplicativo AppStream 2.0 para usuários finais em um navegador HTML5 compatível usando o modo desktop ou o modo de entrega de aplicativos.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma aceitação dos termos e condições AppStream 2.0
- Conhecimento básico de AppStream recursos, como pilhas, frotas e criadores de imagens

Limitações

- Você não pode modificar a função do AWS Identity and Access Management (IAM) associada a uma instância AppStream 2.0 após a criação dessa instância.
- Você não pode modificar propriedades (como a sub-rede ou o grupo de segurança) na instância do construtor de imagens AppStream 2.0 após a criação desse criador de imagens.

Arquitetura

O diagrama a seguir mostra como automatizar a criação de recursos AppStream 2.0 usando um CloudFormation modelo da AWS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Você cria um CloudFormation modelo da AWS com base no código YAML na seção Informações adicionais desse padrão.
2. O CloudFormation modelo da AWS cria uma pilha CloudFormation de testes da AWS.
   a. (Opcional) Você cria uma instância do construtor de imagens usando AppStream 2.0.
   b. (Opcional) Você cria uma imagem do Windows usando seu software personalizado.
3. A CloudFormation pilha da AWS cria uma instância e uma pilha de frota AppStream 2.0.
4. Você implanta seus recursos AppStream 2.0 para usuários finais em um HTML5 navegador compatível.

Pilha de tecnologia

- Amazon AppStream 2.0
- AWS CloudFormation

Ferramentas

- O Amazon AppStream 2.0 é um serviço de streaming de aplicativos totalmente gerenciado que fornece acesso instantâneo aos seus aplicativos de desktop de qualquer lugar. AppStream 2.0 gerencia os recursos da AWS necessários para hospedar e executar seus aplicativos, escala automaticamente e fornece acesso aos seus usuários sob demanda.
- CloudFormationA AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em várias contas e regiões da AWS.

Épicos

(Opcional) Crie uma imagem AppStream 2.0

Tarefa	Descrição	Habilidades necessárias
Instale um software personalizado e crie uma imagem.	1. Instale o aplicativo AppStream 2.0 que você	AWS DevOps, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	planeja implantar para seus usuários. 2. Use o agente de criação de imagens Photon ou um PowerShell script para criar uma nova imagem do Windows para seu software personalizado. **Note** Considere usar o AppLocker recurso do Windows para bloquear ainda mais a imagem.	

Implemente o CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Atualize o CloudFormation modelo da AWS.	1. Salve o código na seção Informações adicionais deste padrão como um arquivo YAML. 2. Atualize o arquivo YAML com os valores necessários para os parâmetros em seu ambiente.	Administrador de sistemas da AWS, administrador de nuvem, arquiteto de nuvem, AWS geral, administrador da AWS
Crie uma CloudFormation pilha da AWS usando o modelo.	1. Faça login no Console de Gerenciamento da AWS	Proprietário do aplicativo, administrador de sistemas da AWS, engenheiro do Windows

Tarefa	Descrição	Habilidades necessárias
	e abra o CloudFormation console da AWS. 2. No painel de navegação, selecione Pilhas. 3. Selecione Create stack (Criar pilha) e With new resources (standard) (Com novos recursos, padrão). 4. Na seção Preparar modelo, selecione O modelo está pronto. 5. Na seção Especificar modelo escolha Fazer upload de um arquivo de modelo. 6. Escolha Escolher arquivo e, em seguida, escolha seu CloudFormation modelo atualizado da AWS. 7. Conclua o restante das etapas do assistente para criar sua pilha.	

Recursos relacionados

Referências

- Comece a usar o Amazon AppStream 2.0: configure com aplicativos de amostra
- Crie uma frota AppStream 2.0 e empilhe

Tutoriais e vídeos

- Fluxo de trabalho do usuário da Amazon AppStream 2.0

- Como migrar um aplicativo Windows Forms antigo para a Amazon 2.0 AppStream
- AWS re:Invent 2018: entregue aplicativos de desktop com segurança com o Amazon 2.0 (01) AppStream BAP2

Mais informações

O código a seguir é um exemplo de um CloudFormation modelo da AWS que permite criar automaticamente recursos AppStream 2.0.

```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
  SubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
  testSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup::Id'
  ImageName:
    Type: String
Resources:

  AppStreamFleet:
    Type: 'AWS::AppStream::Fleet'
    Properties:
      ComputeCapacity:
        DesiredInstances: 5
      InstanceType: stream.standard.medium
      Name: appstream-test-fleet
      DisconnectTimeoutInSeconds: 1200
      FleetType: ON_DEMAND
      IdleDisconnectTimeoutInSeconds: 1200
      ImageName: !Ref ImageName
      MaxUserDurationInSeconds: 345600
      VpcConfig:
        SecurityGroupIds:
          - !Ref testSecurityGroup
        SubnetIds: !Ref SubnetIds
  AppStreamStack:
    Type: 'AWS::AppStream::Stack'
    Properties:
      Description: AppStream stack for test
      DisplayName: AppStream test Stack
      Name: appstream-test-stack
      StorageConnectors:
```

```
      - ConnectorType: HOMEFOLDERS
    UserSettings:
      - Action: CLIPBOARD_COPY_FROM_LOCAL_DEVICE
        Permission: ENABLED
      - Action: CLIPBOARD_COPY_TO_LOCAL_DEVICE
        Permission: ENABLED
      - Action: FILE_DOWNLOAD
        Permission: ENABLED
      - Action: PRINTING_TO_LOCAL_DEVICE
        Permission: ENABLED
AppStreamFleetAssociation:
  Type: 'AWS::AppStream::StackFleetAssociation'
  Properties:
    FleetName: appstream-test-fleet
    StackName: appstream-test-stack
  DependsOn:
    - AppStreamFleet
    - AppStreamStack
```

Crie um analisador de log personalizado para o Amazon ECS usando um roteador de log Firelens

Criado por Varun Sharma (AWS)

Resumo

O Firelens é um roteador de log do Amazon Elastic Container Service (Amazon ECS) e do AWS Fargate. Você pode usar o Firelens para rotear registros de contêineres do Amazon ECS para a Amazon CloudWatch e outros destinos (por exemplo, Splunk ou Sumo Logic). O Firelens funciona com o Fluentd ou o Fluent Bit como agente de registro, o que significa que você pode usar os parâmetros de definição de tarefas do Amazon ECS para rotear logs.

Ao optar por analisar os logs no nível da fonte, você pode analisar seus dados de registro e realizar consultas para responder de forma mais eficiente e eficaz aos problemas operacionais. Como aplicativos diferentes têm padrões de log diferentes, você precisa usar um analisador personalizado que estruture os logs e facilite a pesquisa em seu destino final.

Esse padrão usa um roteador de log Firelens com um analisador personalizado para enviar registros de um aplicativo Spring Boot CloudWatch de amostra executado no Amazon ECS. Em seguida, você pode usar o Amazon CloudWatch Logs Insights para filtrar os registros com base nos campos personalizados gerados pelo analisador personalizado.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS).
- AWS Command Line Interface (AWS CLI), instalada e configurada na sua máquina local.
- Docker, instalado e configurado em sua máquina local.
- Um aplicativo em contêineres existente baseado no Spring Boot no Amazon Elastic Container Registry (Amazon ECR).

Arquitetura

Pilha de tecnologia

- CloudWatch
- Amazon ECR
- Amazon ECS
- Fargate
- Docker
- Fluent Bit

Ferramentas

- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um serviço de registro de imagem de contêiner, seguro, escalável e confiável.
- Amazon ECS: o Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- AWS Identity and Access Management (IAM): o IAM é um serviço web que ajuda você a controlar, com segurança, o acesso a serviços da AWS.
- AWS CLI: a AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- Docker: o Docker é uma plataforma aberta para desenvolvimento, envio e execução de aplicativos.

Código

Os arquivos a seguir estão anexados a esse padrão:

- `customFluentBit.zip`: contém os arquivos para adicionar a análise e as configurações personalizadas.
- `firelens_policy.json`: contém o documento de política para criar uma política do IAM.
- `Task.json`: contém um exemplo de definição de tarefa para o Amazon.

Épicos

Crie uma imagem personalizada do Fluent Bit

Tarefa	Descrição	Habilidades necessárias
Crie um repositório do Amazon ECR.	Cadastre-se no Console de Gerenciamento da AWS, abra o console do Amazon ECR e crie um repositório chamado `fluentbit_custom` . Para obter mais informaçõ es sobre isso, consulte Criação de um repositório na documentação do Amazon ECR.	Administrador de sistemas, Desenvolvedor
Descompacte o customFlu entBit pacote.zip.	1. Faça download do pacote `customFluentBit.zip` (anexado) na sua máquina local. 2. Descompacte o diretório `customFluentBit` executando o seguinte comando: `unzip -d customFluentBit.zip` 3. O diretório contém os seguintes arquivos que são necessários para adicionar a análise e as configura ções personalizadas: • `parsers/springboot_parser.conf` :	

Tarefa	Descrição	Habilidades necessárias
	contém a diretiva do analisador e define o padrão de expressão regular (regex) do analisador personalizado. Você pode adicionar o padrão regex para seu analisador específico. • `conf/parse_springboot.conf` : contém o filtro e a diretiva de serviço. • O Dockerfile	

Tarefa	Descrição	Habilidades necessárias
Crie a imagem do Docker personalizada.	1. Altere o diretório para `customFluentBit .` 2. Abra o console do Amazon ECR, escolha o repositório `fluentbit_custom e`, em seguida, escolha Exibir comandos push. 3. Envie seu projeto 4. Após a conclusão do upload, copie o URL da versão. Esse URL é obrigatório quando você cria um contêiner no Amazon ECS Para obter mais informaçõ es, consulte Envio de uma imagem do Docker na documentação do Amazon ECR.	Administrador de sistemas, Desenvolvedor

Configure o cluster do Amazon ECS

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do Amazon ECS.	Crie um cluster do Amazon ECS seguindo as instruções da seção de Modelos somente para redes em Criação de um cluster na documentação do Amazon ECS.	Administrador de sistemas, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Note Certifique-se de escolher Create VPC para criar uma nova nuvem privada virtual (VPC) para seu cluster Amazon ECS.	

Configurar a tarefa do Amazon ECS

Tarefa	Descrição	Habilidades necessárias
Configure o perfil do IAM de execução de tarefas do Amazon ECS.	Crie um perfil do IAM de execução de tarefas do Amazon ECS usando a `AmazonECSTaskExecutionRolePolicy` política gerenciada. Para obter mais informações sobre isso, consulte Perfil do IAM para execução de tarefas do Amazon ECS na documentação do Amazon ECS. **Note** Certifique-se de registrar o Amazon Resource Name (ARN) da função do IAM.	Administrador de sistemas, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Anexe a política do IAM ao perfil do IAM de execução de tarefas do Amazon ECS.	1. Crie uma política do IAM usando o `firelens_policy.json` documento de política (anexado). Para obter mais informações, consulte Criar políticas na guia JSON na documentação do IAM. 2. Anexe essa política ao perfil do IAM de execução de tarefas do Amazon ECS que você criou anteriorm ente. Para obter mais informações sobre isso, consulte Adicionar políticas do IAM (AWS CLI) na documentação do IAM.	Administrador de sistemas, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Configuração da definição de tarefa do Amazon ECS.	1. Atualize as seções a seguir no `Task.json` exemplo de definição de tarefa (anexado): • Atualize o `executionRoleArn` e `taskRoleArn` com o ARN do perfil do IAM de execução de tarefas • Atualize a imagem `containerDefinitions` com a imagem do Docker Fluent Bit personalizada que você criou anteriormente • Atualize a imagem `containerDefinitions` com o nome da imagem do seu aplicativo 2. Abra o console do Amazon ECS, escolha Definições de tarefas, escolha Criar nova definição de tarefa e, em seguida, escolha Fargate na página Selecionar compatibilidades. 3. Escolha Configurar via Json, cole o arquivo `Task.json` atualizado na área de texto e escolha Salvar. 4. Crie a definição de tarefa	Administrador de sistemas, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações sobre isso, consulte Criação de uma definição de tarefa na documentação do Amazon ECR.	

Execute uma tarefa do Amazon ECS.

Tarefa	Descrição	Habilidades necessárias
Execute uma tarefa do Amazon ECS.	No console do Amazon ECS, escolha Clusters, escolha o cluster que você criou anteriormente e, em seguida, execute a tarefa autônoma. Para obter mais informações sobre isso, consulte Executar uma tarefa independente na documentação do Amazon ECR.	Administrador de sistemas, Desenvolvedor

Verifique os CloudWatch registros

Tarefa	Descrição	Habilidades necessárias
Verificar os logs.	1. Abra o CloudWatch console, escolha Grupos de registros e, em seguida, escolha `/aws/ecs/containerinsights/{{cluster_ARN}}/firelens/application`.	Administrador de sistemas, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	2. Verifique os logs, especialmente os campos personalizados adicionados pelo analisador personalizado. 3. Use CloudWatch para filtrar registros com base nos campos personalizados.	

Recursos relacionados

- Noções básicas do Docker para Amazon ECS
- Amazon ECS no AWS Fargate
- Configuração de parâmetros básicos de serviço

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie um pipeline e uma AMI usando CodePipeline um HashiCorp Packer

Criado por Akash Kumar (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão fornece exemplos de código e etapas para criar um pipeline na nuvem da Amazon Web Services (AWS) usando a AWS CodePipeline e uma Amazon Machine Image (AMI) usando o HashiCorp Packer. O padrão é baseado na prática de integração contínua, que automatiza a criação e o teste do código com um sistema de versionamento baseado em Git. Nesse padrão, você cria e clona um repositório de código usando a AWS. CodeCommit Em seguida, crie um projeto e configure seu código-fonte usando a AWS CodeBuild. Por fim, crie uma AMI que seja comprometida com seu repositório.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma AMI Amazon Linux para lançar instâncias do Amazon Elastic Compute Cloud (Amazon EC2)
- HashiCorp Packer 0.12.3 ou posterior
- CloudWatch Eventos da Amazon (opcional)
- Amazon CloudWatch Logs (opcional)

Arquitetura

O diagrama a seguir mostra um exemplo de código de aplicativo que automatiza a criação de uma AMI usando a arquitetura desse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. O desenvolvedor confirma as alterações de código em um repositório CodeCommit Git privado. Em seguida, CodePipeline usa CodeBuild para iniciar a construção e adicionar novos artefatos que estão prontos para implantação no bucket do Amazon Simple Storage Service (Amazon S3).

2. CodeBuild usa o Packer para agrupar e empacotar a AMI com base em um modelo JSON. Se ativado, o CloudWatch Events pode iniciar automaticamente o pipeline quando ocorrer uma alteração no código-fonte.

Pilha de tecnologia

- CodeBuild
- CodeCommit
- CodePipeline
- CloudWatch Eventos (opcional)

Ferramentas

- AWS CodeBuild — CodeBuild A AWS é um serviço de construção totalmente gerenciado na nuvem. CodeBuild compila seu código-fonte, executa testes de unidade e produz artefatos prontos para serem implantados.
- AWS CodeCommit — CodeCommit A AWS é um serviço de controle de versão que permite que você armazene e gerencie de forma privada repositórios Git na nuvem da AWS. CodeCommit elimina a necessidade de você gerenciar seu próprio sistema de controle de origem ou se preocupar com a escalabilidade de sua infraestrutura.
- AWS CodePipeline — CodePipeline A AWS é um serviço de entrega contínua que você pode usar para modelar, visualizar e automatizar as etapas necessárias para lançar seu software.
- HashiCorp Packer — O HashiCorp Packer é uma ferramenta de código aberto para automatizar a criação de imagens de máquina idênticas a partir de uma única configuração de origem. O Packer é leve, funciona em todos os principais sistemas operacionais e cria imagens de máquina para várias plataformas em paralelo.

Código

Esse padrão inclui os seguintes anexos:

- `buildspec.yml`— Esse arquivo é usado CodeBuild para criar e criar um artefato para implantação.
- `amazon-linux_packer-template.json`: este arquivo usa o Packer para criar uma Amazon Linux AMI.

Épicos

Configurar o repositório do código

Tarefa	Descrição	Habilidades necessárias
Criar o repositório.	Crie um CodeCommit repositório.	Administrador de sistemas AWS
Clonar o repositório.	Conecte-se ao CodeCommit repositório clonando o repositório.	Desenvolvedor de aplicativos
Envia o código-fonte para o repositório remoto.	1. Criar uma confirmação para adicionar os arquivos `buildspec.yml` e `amazon-linux_packer-template.json` ao seu repositório local. 2. Envie o commit do seu repositório local para o CodeCommit repositório remoto.	Desenvolvedor de aplicativos

Crie um CodeBuild projeto para o aplicativo

Tarefa	Descrição	Habilidades necessárias
Crie um projeto de compilação.	1. Faça login no console de gerenciamento da AWS, abra o CodeBuild console da AWS e escolha Create build project. 2. Em Nome do projeto, digite o nome de seu projeto.	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	3. Para provedor de origem, escolha AWS CodeCommit. 4. Em Repositório, escolha o repositório em que você deseja criar o pipeline de código. 5. Em Imagem do ambiente, escolha Imagem gerenciada ou Imagem personalizada. 6. Para Operating system, selecione Ubuntu. 7. Para RunTime(s), escolha Padrão. 8. Para Imagem, escolha: 4.0aws/codebuild/standard. 9. Na Versão da imagem, escolha Sempre usar a imagem mais recente para esta versão de runtime. 10. Em Ambiente, selecione Linux. 11. Marque a caixa de seleção Privilegiado. 12. Em Perfil de serviço, escolha Novo perfil de serviço ou Perfil de serviço existente. 13. Em Especificações da compilação, escolha Usar um arquivo de especificações da compilação	

Tarefa	Descrição	Habilidades necessárias
	,ou Inserir comandos de compilação. 14. (Opcional) Em Tipo na seção Artefatos, escolha Sem artefatos. 15. (Recomendado) Para fazer upload dos registros de saída da compilação para CloudWatch Logs, escolha CloudWatch logs. 16. (Opcional) Para fazer upload dos logs de saída da compilação para o Amazon S3, marque a caixa de seleção Logs do S3. 17. Selecione Create build project (Criar projeto de compilação).	

Configurar o pipeline

Tarefa	Descrição	Habilidades necessárias
Nome do pipeline	1. Faça login no console de gerenciamento da AWS, abra o CodePipeline console da AWS e escolha Create pipeline. 2. Em Nome do pipeline, insira um nome para o pipeline. 3. Em Perfil de serviço, escolha Novo perfil de	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	serviço ou Perfil de serviço existente. 4. Em Role name (Nome da função), digite um nome para sua função. 5. Na seção Configurações avançadas, em Armazenamento de artefatos, escolha Localização padrão se quiser que o Amazon S3 crie um bucket e armazene os artefatos no bucket. Para usar um bucket S3 existente, escolha Custom location (Local personalizado). Escolha Próximo. 6. Para provedor de origem, escolha AWS CodeCommit. 7. Em Nome do repositório, escolha o repositório que você clonou anteriormente. Em Nome da ramificação, escolha sua ramificação do código-fonte. 8. Para opções de detecção de alterações, escolha Amazon CloudWatch Events (recomendado) para iniciar o pipeline ou AWS CodePipeline para verificar periodicamente as alterações. Escolha Próximo.	

Tarefa	Descrição	Habilidades necessárias
	9. Em Build provider, escolha AWS CodeBuild. 10. Em Nome do projeto, escolha o projeto de construção que você criou no épico Criar um CodeBuild projeto para o aplicativo. 11. Escolha suas opções de compilação, e, em seguida, escolha Próximo. 12. Escolha Ignorar estágio de implantação. 13. Selecione Criar pipeline.	

Recursos relacionados

- Trabalhando com repositórios na AWS CodeCommit
- Trabalhar com projetos de compilação
- Trabalhando com oleodutos em CodePipeline

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie um pipeline e implante atualizações de artefatos em instâncias locais usando EC2 CodePipeline

Criado por Akash Kumar (AWS) e Sandeep Reddy Jogammagari (AWS)

Resumo

Esse padrão fornece exemplos de código e etapas para criar um pipeline na nuvem da Amazon Web Services (AWS) e implantar artefatos atualizados em instâncias locais da Amazon Elastic Compute Cloud (Amazon EC2) na AWS. CodePipeline O padrão é baseado na prática de integração contínua. Essa prática automatiza a criação e o teste de código com um sistema de controle de versão baseado em Git. Nesse padrão, você cria e clona um repositório de código usando a AWS. CodeCommit Em seguida, você cria um projeto e configura seu código-fonte usando a AWS CodeBuild. Por fim, você cria seu aplicativo e configura seu ambiente de destino para EC2 instâncias locais usando a AWS CodeDeploy.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Tags definidas pelo usuário para identificar EC2 instâncias durante a implantação
- CodeDeploy agente, instalado em EC2 instâncias
- Seu software de tempo de execução necessário, instalado nas EC2 instâncias
- Amazon Corretto 8 para o Java Development Kit
- Servidor web Apache Tomcat, instalado
- CloudWatch Eventos da Amazon (opcional)
- Um par de chaves para fazer login no servidor da web (opcional)
- Um projeto de aplicativo Apache Maven para um aplicativo web

Arquitetura

O diagrama a seguir mostra um exemplo de aplicativo Web Java que é implantado em EC2 instâncias locais usando a arquitetura desse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. O desenvolvedor confirma as alterações de código em um repositório CodeCommit Git privado.
2. CodePipeline usa CodeBuild para iniciar a construção e adicionar novos artefatos que estão prontos para implantação no bucket do Amazon Simple Storage Service (Amazon S3).
3. CodePipeline usa o CodeDeploy agente para pré-instalar todas as dependências necessárias para as alterações do artefato de implantação.
4. CodePipeline usa o CodeDeploy agente para implantar os artefatos do bucket do S3 nas instâncias de destino EC2 . Se ativado, o CloudWatch Events pode iniciar automaticamente o pipeline quando ocorrer uma alteração no código-fonte.

Pilha de tecnologia

- CodeBuild
- CodeCommit
- CodeDeploy
- CodePipeline
- CloudWatch Eventos (opcional)

Ferramentas

- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação. CodeBuild compila seu código-fonte, executa testes de unidade e produz artefatos prontos para serem implantados.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- A AWS CodeDeploy automatiza implantações no Amazon Elastic Compute Cloud (Amazon EC2) ou em instâncias locais, funções do AWS Lambda ou serviços Amazon Elastic Container Service (Amazon ECS).
- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.

Código

Esse padrão inclui os seguintes anexos:

- `buildspec.yml`— Esse arquivo especifica as ações CodeBuild necessárias para criar e criar um artefato para implantação.
- `appspec.yml`— Esse arquivo especifica as ações CodeDeploy necessárias para criar um aplicativo e configurar um ambiente de destino para instâncias locais EC2 .
- `install_dependencies.sh`: esse arquivo instala dependências para o servidor web Apache Tomcat.
- `start_server.sh`: esse arquivo inicia o servidor web Apache Tomcat.
- `stop_server.sh`: esse arquivo inicia o servidor web Apache Tomcat.

Épicos

Configurar o repositório do código

Tarefa	Descrição	Habilidades necessárias
Criar o repositório.	Crie um CodeCommit repositório.	Administrador de sistemas AWS
Clonar o repositório.	Conecte-se ao CodeCommit repositório clonando o repositório.	Desenvolvedor de aplicativos
Envia o código-fonte para o repositório remoto.	1. Criar uma confirmação para adicionar os arquivos `buildspec.yml` e `appspec.yml` ao seu repositório local. 2. Envie o commit do seu repositório local para o CodeCommit repositório remoto.	Desenvolvedor de aplicativos

Crie um CodeBuild projeto para o aplicativo

Tarefa	Descrição	Habilidades necessárias
Crie um projeto de compilação.	1. Faça login no AWS Management Console, abra o CodeBuild console da AWS e escolha Create build project. 2. Em Nome do projeto, digite o nome de seu projeto. 3. Para provedor de origem, escolha AWS CodeCommit. 4. Em Repositório, escolha o repositório em que você deseja criar o pipeline de código. 5. Em Environment image (Imagem do ambiente), escolha Managed image (Imagem gerenciada) ou Custom image (Imagem personalizada). 6. Em Sistema operacional, escolha Amazon Linux 2. **Note** O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs.	Administrador da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	7. Para RunTime(s), escolha Padrão. 8. Para Imagem, escolha aws/codebuild/amazonlinux2-aarch64-standard:2.0. 9. Na Image version (Versão da imagem), escolha Always use the latest image for this runtime version (Sempre usar a imagem mais recente para esta versão de tempo de execução). 10. Em Perfil de serviço, escolha Novo perfil de serviço ou Perfil de serviço existente. 11. Em Especificações da compilação, escolha Usar um arquivo de especificações da compilação ,ou Inserir comandos de compilação. 12. (Opcional) Escolha Adicionar artefato para configurar artefatos. 13. (Opcional) Para fazer upload dos registros de saída da compilação para a Amazon CloudWatch, escolha CloudWatch logs.	

Tarefa	Descrição	Habilidades necessárias
	14. Selecione Create build project (Criar projeto de compilação).	

Configurar a implantação de artefatos para instâncias locais EC2

Tarefa	Descrição	Habilidades necessárias
Crie o aplicativo.	1. Faça login no AWS Management Console, abra o CodeDeploy console da AWS e escolha Create application. 2. Em Nome do aplicativo, insira um nome para seu aplicativo. 3. Para a plataforma de computação, escolha EC2/On-premises. 4. Escolha Criar aplicativo e, em seguida, escolha Criar grupo de implantação. 5. Em Nome do grupo de implantação, insira um nome. 6. **Note** Crie uma função de serviço para CodeDeploy. : a função de serviço deve ter permissões para conceder	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	CodeDeploy acesso ao seu ambiente de destino. 7. Em Service role (Perfil de serviço), escolha o perfil de serviço criado na etapa 6. 8. Para o Tipo de implantação, escolha In-loco ou Azul/verde com base nos requisitos de sua empresa. 9. Em Configuração do ambiente, escolha as opções que atendam aos requisitos da sua empresa. 10. (Opcional) Crie um grupo-alvo para seu load balancer separadamente no EC2 console da Amazon e, em seguida, volte para a página Create deployment group do CodeDeploy console da AWS para escolher seu load balancer e seu grupo-alvo. 11. Selecione Criar grupo de implantação.	

Configure o pipeline

Tarefa	Descrição	Habilidades necessárias
Crie o pipeline.	1. Faça login no AWS Management Console, abra o CodePipeline console da AWS e escolha Create pipeline. 2. Em Nome do pipeline, insira um nome para o pipeline. 3. Em Perfil de serviço, escolha Novo perfil de serviço ou Perfil de serviço existente. 4. Em Role name (Nome da função), digite um nome para sua função. 5. Na seção Configurações avançadas, em Armazenamento de artefatos, escolha Localização padrão se quiser que o Amazon S3 crie um bucket e armazene os artefatos no bucket. Para usar um bucket S3 existente, escolha Custom location (Local personalizado). Escolha Próximo. 6. Para provedor de origem, escolha AWS CodeCommit. 7. Em Nome do repositório, escolha o repositório que você clonou anteriormente. Em Nome da ramificação,	Administrador de sistemas da AWS, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	escolha sua ramificação do código-fonte. 8. Para opções de detecção de alterações, escolha Amazon CloudWatch Events (recomendado) ou AWS CodePipeline. Escolha Próximo. 9. Para o provedor de compilação, escolha AWS CodeBuild. 10. Em Nome do projeto, escolha o projeto de construção que você criou na seção Criar um CodeBuild projeto para o aplicativo desse padrão. 11. Escolha suas opções de compilação, e, em seguida, escolha Próximo. 12. Para o provedor Deploy, escolha AWS CodeDeploy. 13. Escolha um nome de aplicativo e um grupo de implantação e, em seguida, escolha Avançar. 14. Selecione Criar pipeline.	

Recursos relacionados

- Trabalhando com repositórios na AWS CodeCommit
- Trabalhar com projetos de compilação

- Trabalhando com aplicativos em CodeDeploy
- Trabalhando com oleodutos em CodePipeline

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Criar pipelines dinâmicos de CI para projetos Java e Python automaticamente

Criado por Aromal Raj Jayarajan (AWS), Amarnath Reddy (AWS), Mahesh Raghunandanan (AWS) e Vijesh Vijayakumaran Nair (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Este padrão mostra como criar pipelines dinâmicos de integração contínua (CI) para projetos Java e Python automaticamente usando as ferramentas de desenvolvedor da AWS.

À medida que as pilhas de tecnologia se diversificam e as atividades de desenvolvimento aumentam, pode se tornar difícil criar e manter pipelines de CI consistentes em toda a organização. Ao automatizar o processo no AWS Step Functions, você pode garantir que o uso e a abordagem de seus pipelines de CI sejam consistentes.

Para automatizar a criação de pipelines dinâmicos de CI, esse padrão usa as seguintes entradas variáveis:

- Linguagem de programação (somente Java ou Python)
- Nome do pipeline
- Etapas necessárias do pipeline

> **Note**
>
> O Step Functions orquestra a criação do pipeline usando vários serviços da AWS. Para obter mais informações sobre os serviços da AWS usados nesta solução, consulte a seção Ferramentas deste padrão.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do Amazon S3 na mesma região da AWS em que essa solução está sendo implantada

- Um diretor do AWS Identity and Access Management (IAM) que tem as CloudFormation permissões da AWS necessárias para criar os recursos necessários para essa solução

Limitações

- Este padrão é compatível somente com projetos Java e Python.
- Os perfis do IAM provisionados neste padrão seguem o princípio do privilégio mínimo. As permissões deste perfil do IAM devem ser atualizadas com base nos recursos específicos que seu pipeline precisa criar.

Arquitetura

Pilha de tecnologias de destino

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Systems Manager
- AWS Step Functions
- AWS Lambda
- Amazon DynamoDB

Arquitetura de destino

O diagrama a seguir mostra um exemplo de fluxo de trabalho para criar automaticamente pipelines dinâmicos de CI para projetos Java e Python usando ferramentas de desenvolvedor da AWS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário da AWS fornece os parâmetros de entrada para a criação do pipeline de CI no formato JSON. Esta entrada inicia um fluxo de trabalho do Step Functions (máquina de estado) que cria um pipeline de CI usando as ferramentas de desenvolvedor da AWS.

2. Uma função do Lambda lê uma pasta chamada input-reference, que é armazenada em um bucket do Amazon S3 e, em seguida, gera um arquivo buildspec.yml. Esse arquivo gerado define os estágios do pipeline de CI e é armazenado novamente no mesmo bucket do Amazon S3 que armazena as referências de parâmetros.
3. O Step Functions verifica se há alterações nas dependências do fluxo de trabalho de criação do pipeline de CI e atualiza a pilha de dependências conforme necessário.
4. O Step Functions cria os recursos do pipeline de CI em uma CloudFormation pilha, incluindo um CodeCommit repositório, um CodeBuild projeto e um CodePipeline pipeline.
5. A CloudFormation pilha copia o código-fonte de amostra para a pilha de tecnologia selecionada (Java ou Python) e o arquivo buildspec.yml para o repositório. CodeCommit
6. Os detalhes do runtime do pipeline de CI são armazenados em uma tabela do DynamoDB.

Automação e escala

- Este padrão deve ser usado somente em um único ambiente de desenvolvimento. As alterações de configuração são necessárias para uso em vários ambientes de desenvolvimento.
- Para adicionar suporte para mais de uma CloudFormation pilha, você pode criar CloudFormation modelos adicionais. Para obter mais informações, consulte Conceitos básicos da AWS CloudFormation na CloudFormation documentação.

Ferramentas

Ferramentas

- O AWS Step Functions é um serviço de orquestração de tecnologia sem servidor que permite combinar funções do AWS Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação.

- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O AWS Systems Manager Parameter Store oferece armazenamento hierárquico seguro para o gerenciamento de dados de configuração e gerenciamento de segredos.

Código

O código desse padrão está disponível no GitHub automated-ci-pipeline-creationrepositório. O repositório contém os CloudFormation modelos necessários para criar a arquitetura de destino descrita nesse padrão.

Práticas recomendadas

- Não insira credenciais (segredos), como tokens ou senhas, diretamente nos CloudFormation modelos ou nas configurações de ação do Step Functions. Se você fizer isso, as informações serão exibidas nos logs do DynamoDB. Em vez disso, use o AWS Secrets Manager para configurar e armazenar segredos. Em seguida, faça referência aos segredos armazenados no Secrets Manager nos CloudFormation modelos e nas configurações de ação do Step Functions, conforme necessário. Para obter mais informações, consulte O que é o AWS Secrets Manager? na documentação do Secrets Manager.

- Configure a criptografia do lado do servidor para CodePipeline artefatos armazenados no Amazon S3. Para obter mais informações, consulte Configurar a criptografia do lado do servidor para artefatos armazenados no Amazon S3 na documentação. CodePipeline CodePipeline
- Aplique permissões de privilégio mínimo ao configurar perfis do IAM. Para obter mais informações, consulte Aplicar permissões de privilégios mínimos na documentação do IAM.
- Certifique-se de que seu bucket do Amazon S3 não esteja acessível publicamente. Para obter mais informações, consulte Configuração da definição de bloqueio de acesso público para seus buckets do S3 na documentação do Amazon S3.
- Certifique-se de ativar o versionamento do seu bucket do Amazon S3. Para obter mais informações, consulte Usar o versionamento em buckets do S3 na documentação do Amazon S3.
- Use o IAM Access Analyzer ao configurar políticas do IAM. A ferramenta fornece recomendações práticas para ajudar você a criar políticas do IAM seguras e funcionais. Para obter mais informações, consulte Usar o AWS Identity and Access Management na documentação do IAM.
- Quando possível, defina condições de acesso específicas ao configurar as políticas do IAM.
- Ative o CloudWatch registro na Amazon para fins de monitoramento e auditoria. Para obter mais informações, consulte O que é o Amazon CloudWatch Logs? na CloudWatch documentação.

Épicos

Configurar os pré-requisitos

Tarefa	Descrição	Habilidades necessárias
Crie um bucket do Amazon S3.	Crie um bucket do Amazon S3 (ou use um bucket existente) para armazenar os CloudFormation modelos, o código-fonte e os arquivos de entrada necessários para a solução. Para obter mais informações, consulte Etapa 1: Criar o seu primeiro bucket do S3 na documentação do Amazon S3.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Note O bucket do Amazon S3 deve estar na mesma região da AWS na qual você está implantando a solução.	
Clone o GitHub repositório.	Clone o GitHub automated-ci-pipeline-creationrepositório executando o seguinte comando em uma janela de terminal: `git clone https://github.com/aws-samples/automated-ci-pipeline-creation.git` Para obter mais informações, consulte Clonar um repositório na GitHub documentação.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Faça o upload da pasta Solution Templates do GitHub repositório clonado para seu bucket do Amazon S3.	Copie o conteúdo da pasta Solution-Templates clonada e faça o upload no bucket do Amazon S3 que você criou. Para obter mais informações, consulte Fazendo upload de objetos na documentação do Amazon S3. **Note** Certifique-se de carregar somente o conteúdo da pasta Solution-Templates . Você pode fazer upload dos arquivos somente no nível raiz do bucket do Amazon S3.	AWS DevOps

Implante a solução

Tarefa	Descrição	Habilidades necessárias
Crie uma CloudFormation pilha para implantar a solução usando o arquivo template.yml no repositório clonado. GitHub	1. Faça login no Console de Gerenciamento da AWS e, em seguida, abra o CloudFormation console da AWS. 2. Selecione Criar pilha. Uma lista suspensa aparece.	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	3. Na lista suspensa, selecione Com novos recursos (padrão). A página Criar pilha é aberta. 4. Na seção Especificar modelo escolha a caixa de seleção junto ao Fazer upload de um arquivo de modelo. 5. Selecione Escolher arquivo. Em seguida, navegue até a pasta raiz do GitHub repositório clonado e selecione o arquivo template.yml. Em seguida, selecione Open (Abrir). 6. Escolha Próximo. A página Especificar detalhes da pilha é exibida. 7. Na seção Parâmetros, especifique os parâmetros a seguir: • Para o S3 TemplateBucketName, insira o nome do bucket do Amazon S3 que você criou anteriormente, que contém o código-fonte e as referências dessa solução. Verifique se o parâmetro do nome do bucket está em letras minúsculas.	

Tarefa	Descrição	Habilidades necessárias
	• Para o Dynamo DBTable, insira um nome para a tabela do DynamoDB que a pilha cria. CloudForm ation • Para StateMachineName, insira um nome para a máquina de estado Step Functions que a CloudFormation pilha cria. 8. Escolha Próximo. A página Configurar opções adicionai s se abre. 9. Na página Configurar opções de pilha, selecione Próximo. Não altere nenhum dos valores padrão. A página Revisar se abre. 10. Revise as configurações de criação da pilha. Em seguida, escolha Criar pilha para iniciar sua pilha. **Note** Enquanto sua pilha está sendo criada, ela é listada na página Pilhas com o status CREATE_IN _PROGRESS.	

Tarefa	Descrição	Habilidades necessárias
	Certifique-se de esperar que o status da pilha mude para CREATE_COMPLETE antes de concluir as etapas restantes desse padrão.	

Testar a configuração

Tarefa	Descrição	Habilidades necessárias
Selecione a função que você criou.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Step Functions. 2. Selecione a função que você criou. 3. Selecione Iniciar execução. Em seguida, insira seus valores de entrada para o fluxo de trabalho no formato JSON (veja os exemplos de entradas a seguir). 4. Selecione Iniciar execução. Formatação JSON `{ "details": { "tech_stack": "Name of the Tech Stack (python/java)",`	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	<pre>"project_name": "Name of the Project that you want to create with", "pre_build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "post_build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "reports": "Choose the step if it required in the buildspec.yml file i.e., yes/no", } }</pre> Exemplo de entrada em Java JSON <pre>{ "details": { "tech_stack": "java", "project_name": "pipeline-java-pjt", "pre_build": "yes", "build": "yes", "post_build": "yes", "reports": "yes" }</pre>	

Tarefa	Descrição	Habilidades necessárias

	<pre>}</pre>
	Exemplo de entrada em Python JSON
	<pre>{
	  "details": {
	    "tech_stack":
	 "python",
	    "project_name":
	 "pipeline-python-p
	jt",
	    "pre_build": "yes",
	    "build": "yes",
	    "post_build":
	 "yes",
	    "reports": "yes"
	  }
	}</pre>	

Tarefa	Descrição	Habilidades necessárias
Confirme se o CodeCommit repositório do pipeline de CI foi criado.	1. Faça login no AWS Management Console e, em seguida, abra o CodeCommit console. 2. Na página Repositórios, verifique se o nome do CodeCommit repositório que você criou aparece na lista de repositórios. O nome do repositório é anexado com o seguinte: - Repo pipeline-java-pjt 3. Abra o CodeCommit repositório e valide se o código-fonte de amostra junto com os arquivos buildspec.yml foram enviados para a ramificação principal.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Verifique os recursos CodeBuild do projeto.	1. Faça login no AWS Management Console e, em seguida, abra o CodeBuild console. 2. Na página Criar projetos, verifique se o nome do CodeBuild projeto que você criou aparece na lista de projetos. O nome do projeto é anexado com o seguinte: pipeline-java-pjt -Build 3. Selecione o nome do seu CodeBuild projeto para abri-lo. Em seguida, revise e valide as seguintes configurações: • Configuração de projeto • Origem • Ambiente • BuildSpec • Configuração do lote • Artefatos	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Valide os CodePipeline estágios.	1. Faça login no AWS Management Console e, em seguida, abra o CodePipeline console. 2. Na página Pipelines, verifique se o nome do pipeline que você criou aparece na lista de pipelines. O nome do pipeline é anexado com o seguinte: pipeline-java-pjt - Pipeline 3. Selecione o nome do seu pipeline para abri-lo. Em seguida, revise e valide cada estágio do pipeline, incluindo Confirmar e Implantar.	AWS DevOps
Confirme se o pipeline de CI foi executado com êxito.	1. No CodePipeline console, na página Pipelines, selecione o nome do seu funil para ver o status do funil. 2. Verifique se cada estágio do pipeline tem um status de Sucesso.	AWS DevOps

Limpe os seus recursos

Tarefa	Descrição	Habilidades necessárias
Exclua a pilha de recursos. CloudFormation	Exclua a pilha de recursos do pipeline de CI. CloudFormation Para obter mais informações, consulte Excluir uma pilha no CloudFormation console da AWS na CloudFormation documentação. **Note** Certifique-se de excluir a pilha chamada - stack<project_name>.	AWS DevOps
Exclua as dependências do pipeline de CI no Amazon S3 e. CloudFormation	1. Esvazie o bucket do Amazon S3 chamado. DeploymentArtifactBucket Para obter mais informações, consulte Esvaziar o bucket na documentação do Amazon S3. 2. Exclua a pilha de dependências do pipeline de CI. CloudFormation Para obter mais informações, consulte Excluir uma pilha no CloudFormation console da AWS na CloudFormation documentação.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Note Certifique-se de excluir a pilha chamada pipeline-creation-dependencies-stack.	
Consulte Excluir o bucket do modelo do Amazon S3.	Exclua o bucket do Amazon S3 que você criou na seção Configurar os pré-requisitos deste padrão, que armazena os modelos para esta solução. Para obter mais informações, consulte Excluir o bucket na documentação do Amazon S3.	AWS DevOps

Recursos relacionados

- Criação de uma máquina de estado do Step Functions que usa o Lambda (documentação do AWS Step Functions)
- AWS Step Functions WorkFlow Studio (documentação do AWS Step Functions)
- DevOps e AWS
- Como a AWS CloudFormation funciona? (CloudFormation Documentação da AWS)
- CI/CD completo com AWS, CodeCommit AWS CodeDeploy, CodeBuild AWS e AWS (publicação no blog CodePipeline da AWS)
- Cotas, requisitos de nome e limites de caracteres do IAM e do AWS STS (documentação do IAM)

Implante canários CloudWatch Synthetics usando o Terraform

Criado por Dhrubajyoti Mukherjee (AWS) e Jean-Francois Landreau (AWS)

Resumo

É importante validar a integridade de um sistema do ponto de vista do cliente e confirmar se os clientes conseguem se conectar. Isso é mais difícil quando os clientes não chamam constantemente o endpoint. A Amazon CloudWatch Synthetics apoia a criação de canários, que podem testar endpoints públicos e privados. Ao usar canários, você pode saber o status de um sistema mesmo que ele não esteja em uso. Esses canários são scripts Node.js Puppeteer ou scripts Python Selenium.

Esse padrão descreve como usar o HashiCorp Terraform para implantar canários que testam endpoints privados. Incorpora um script do Puppeteer que testa se um URL retorna. `200-OK` O script do Terraform pode então ser integrado ao script que implanta o endpoint privado. Também é possível modificar a solução para monitorar endpoints públicos.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS) com uma nuvem privada virtual (VPC) e sub-redes privadas
- O URL do endpoint que pode ser acessado a partir das sub-redes privadas
- Terraform instalado no ambiente de implantação

Limitações

A solução atual funciona para as seguintes versões de tempo de execução do CloudWatch Synthetics:

- syn-nodejs-puppeteer-3,4
- syn-nodejs-puppeteer-3,5
- syn-nodejs-puppeteer-3,6
- syn-nodejs-puppeteer-3,7

À medida que novas versões de runtime forem lançadas, talvez você precise atualizar a solução atual. Você também precisará modificar a solução para acompanhar as atualizações de segurança.

Versões do produto

- Terraform 1.3.0

Arquitetura

O Amazon CloudWatch Synthetics é baseado no CloudWatch Lambda e no Amazon Simple Storage Service (Amazon S3). A Amazon CloudWatch oferece um assistente para criar os canários e um painel que exibe o status das corridas de canários. A função do Lambda executa o script. O Amazon S3 armazena os logs e as capturas de tela das execuções canárias.

Esse padrão simula um endpoint privado por meio de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) implantada nas sub-redes de destino. A função do Lambda requer interfaces de rede elásticas na VPC em que o endpoint privado é implantado.

O diagrama mostra o seguinte:

1. O canário Synthetics inicializa a função do Lambda do canário.
2. A função do Lambda canário se conecta à interface de rede elástica.
3. A função do Lambda canário monitora o status do endpoint.
4. O canário Synthetics envia os dados de execução para o bucket e as métricas do S3. CloudWatch
5. Um CloudWatch alarme é iniciado com base nas métricas.
6. O CloudWatch alarme inicia o tópico Amazon Simple Notification Service (Amazon SNS).

Ferramentas

Serviços da AWS

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS. Esse padrão usa endpoints da VPC e interfaces de rede elástica.

Outros serviços

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) de código aberto que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem. Esse padrão usa o Terraform para implantar a infraestrutura.
- O Puppeteer é uma biblioteca Node.js. O tempo de execução do CloudWatch Synthetics usa a estrutura do Puppeteer.

Código

A solução está disponível no watch-synthetics-canary-terraform repositório na GitHub nuvem. Para obter mais informações, consulte a seção Informações adicionais.

Épicos

Implemente a solução para monitorar um URL privado

Tarefa	Descrição	Habilidades necessárias
Reúna os requisitos para monitorar o URL privado.	Reúna a definição completa do URL: domínio, parâmetros e cabeçalhos. Para se comunicar de forma privada com o Amazon S3 e a CloudWatch Amazon, use endpoints VPC. Observe como a VPC e as sub-redes	Arquiteto de nuvem, administrador de rede

Tarefa	Descrição	Habilidades necessárias
	são acessíveis ao endpoint. Considere a frequência das corridas de canários.	

Tarefa	Descrição	Habilidades necessárias
Modificar a solução existente para monitorar o URL privado.	Modificar o arquivo `terraform.tfvars` • `name`: o nome do seu canário. • `runtime_version` : a versão de runtime do canário. Recomendamos usar syn-nodejs-puppeteer -3.7. • `take_screenshot` : se uma captura de tela deve ser feita. • `api_hostname` : o nome do host do endpoint que é monitorado. • `api_path`: o caminho do endpoint que é monitorado. • `vpc_id`: o ID da VPC usado pela função canary do Lambda. • `subnet_ids` — A sub-rede IDs usada pela função canary Lambda. • `frequency` : a frequênci a de corrida do canário em minutos. • `alert_sns_topic` — O tópico do SNS para o qual a notificação CloudWatch de alarme é enviada.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

Implanta e opera a solução.	Para implantar a solução, faça o seguinte:
	1. No diretório `cloudwatch-synthetics-canary-terraform` em seu ambiente de desenvolvimento, inicialize o Terraform.
	`terraform init`
	2. Planeje e analise as mudanças.
	`terraform plan`
	3. Implante a solução.
	`terraform apply`
		Arquiteto de nuvem, DevOps engenheiro

Solução de problemas

Problema	Solução
A exclusão dos recursos provisionados é interrompida.	Exclua manualmente a função do Lambda canário, a interface de rede elástica correspondente e o grupo de segurança, nessa ordem.

Recursos relacionados

- Usar monitoramento sintético
- Monitore os endpoints do API Gateway com o Amazon CloudWatch Synthetics (publicação no blog)

Mais informações

Artefatos do repositório

Os artefatos do repositório estão na seguinte estrutura.

```
.
### README.md
### main.tf
### modules
#   ### canary
#   ### canary-infra
### terraform.tfvars
### tf.plan
### variable.tf
```

O arquivo `main.tf` contém o módulo principal e implanta dois submódulos:

- `canary-infra` implanta a infraestrutura necessária para as canárias.
- `canary` implanta os canários.

Os parâmetros de entrada da solução estão localizados no arquivo `terraform.tfvars`. Você pode usar o exemplo de código a seguir para criar um canário.

```
module "canary" {
    source = "./modules/canary"
    name   = var.name
    runtime_version = var.runtime_version
    take_screenshot = var.take_screenshot
    api_hostname = var.api_hostname
    api_path = var.api_path
    reports-bucket = module.canary_infra.reports-bucket
    role = module.canary_infra.role
    security_group_id = module.canary_infra.security_group_id
    subnet_ids = var.subnet_ids
    frequency = var.frequency
    alert_sns_topic = var.alert_sns_topic
}
```

O arquivo .var correspondente segue.

```
name   = "my-canary"
runtime_version = "syn-nodejs-puppeteer-3.7"
take_screenshot = false
api_hostname = "mydomain.internal"
api_path = "/path?param=value"
vpc_id = "vpc_id"
subnet_ids = ["subnet_id1"]
frequency = 5
alert_sns_topic = "arn:aws:sns:eu-central-1:111111111111:yyyyy"
```

Como limpar a solução

Se você estiver testando em um ambiente de desenvolvimento, poderá limpar a solução para evitar custos acumulados.

1. No Console de Gerenciamento da AWS, navegue até o console do Amazon S3. Esvazie o bucket do Amazon S3 que a solução criou. Certifique-se de fazer um backup dos dados, se necessário.
2. No seu ambiente de desenvolvimento, a partir do diretório `cloudwatch-synthetics-canary-terraform`, execute o comando `destroy`.

   ```
   terraform destroy
   ```

Implementar um pipeline de CI/CD para microsserviços Java no Amazon ECS

Criado por Vijay Thompson (AWS) e Sankar Sangubotla (AWS)

Resumo

Esse padrão orienta você pelas etapas de implantação de uma integração e entrega contínuas (o CI/CD) pipeline for Java microservices on an existing Amazon Elastic Container Service (Amazon ECS) cluster by using AWS CodeBuild. When the developer commits the changes, the CI/CD pipeline é iniciado e o processo de criação começa). CodeBuild Quando a compilação é concluída, o artefato é enviado para o Amazon Elastic Container Registry (Amazon ECR) e a versão mais recente do Amazon ECR é coletada e enviada para o serviço Amazon ECS.

Pré-requisitos e limitações

Pré-requisitos

- Um aplicativo de microsserviços Java existente em execução no Amazon ECS
- Familiaridade com a AWS CodeBuild e a AWS CodePipeline

Arquitetura

Pilha de tecnologia de origem

- Microsserviços Java em execução no Amazon ECS
- Repositório de código no Amazon ECR
- AWS Fargate

Arquitetura de origem

Pilha de tecnologias de destino

- Amazon ECR
- Amazon ECS
- AWS Fargate

- AWS CodePipeline
- AWS CodeBuild

Arquitetura de destino

Automação e escala

Arquivo CodeBuild `buildspec.yml`:

```
version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws --version
      - $(aws ecr get-login --region $AWS_DEFAULT_REGION --no-include-email)
      - REPOSITORY_URI=$AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/
$IMAGE_REPO
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=build-$(echo $CODEBUILD_BUILD_ID | awk -F":" '{print $2}')
  build:
    commands:
      - echo Build started on `date`
      - echo building the Jar file
      - mvn clean install
      - echo Building the Docker image...
      - docker build -t $REPOSITORY_URI:$BUILD_TAG .
      - docker tag $REPOSITORY_URI:$BUILD_TAG $REPOSITORY_URI:$IMAGE_TAG
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $REPOSITORY_URI:$BUILD_TAG
      - docker push $REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      - printf '[{"name":"%s","imageUri":"%s"}]' $DOCKER_CONTAINER_NAME
 $REPOSITORY_URI:$IMAGE_TAG > imagedefinitions.json
      - cat imagedefinitions.json
artifacts:
    files:
```

```
    - imagedefinitions.json
    - target/DockerDemo.jar
```

Ferramentas

Serviços da AWS

- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação. A AWS CodeBuild escala continuamente e processa várias compilações simultaneamente, para que suas compilações não fiquem na fila.
- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente. Você pode integrar a AWS CodePipeline com serviços de terceiros GitHub, como, ou usar um serviço da AWS, como o Amazon ECR.
- O Amazon Elastic Container Registry (Amazon ECR) é um registro de contêiner do Docker totalmente gerenciado que facilita aos desenvolvedores o armazenamento, o gerenciamento e a implantação de imagens de contêiner do Docker. O Amazon ECR é integrado ao Amazon ECS para simplificar seu development-to-production fluxo de trabalho. O Amazon ECR hospeda as imagens em uma arquitetura altamente disponível e escalável, o que permite que você implante contêineres para seus aplicativos de modo confiável. A integração com o AWS Identity and Access Management (IAM) fornece controle em nível de recurso de cada repositório.
- Amazon Elastic Container Service (Amazon ECS) serviço altamente dimensionável de orquestração de contêineres que suporta contêineres do Docker e permite executar e escalar facilmente aplicativos em contêineres na AWS. O Amazon ECS elimina a necessidade de instalar e operar seu próprio software de orquestração de contêineres, gerenciar e escalar um cluster de máquinas virtuais ou programar contêineres nessas máquinas virtuais.
- AWS Fargate é um mecanismo de computação para o Amazon ECS que permite que você execute contêineres sem precisar gerenciar servidores ou clusters. Com o AWS Fargate, você não precisa mais provisionar, configurar e escalar clusters de máquinas virtuais para executar contêineres. Isso elimina a necessidade de escolher tipos de servidor, decidir quando dimensionar clusters ou otimizar o agrupamento de clusters.

Outras ferramentas

- Docker é uma plataforma que permite criar, testar e entregar aplicativos em pacotes chamados contêineres.

- Git é um sistema distribuído de controle de versão para rastrear alterações no código-fonte durante o desenvolvimento do software. Ele foi projetado para coordenar o trabalho entre programadores, mas pode ser usado para rastrear alterações em nenhum conjunto de arquivos. Seus objetivos incluem velocidade, integridade de dados e suporte para fluxos de trabalho distribuídos e não lineares.

Épicos

Configure o projeto de construção na AWS CodeBuild

Tarefa	Descrição	Habilidades necessárias
Crie um projeto de CodeBuild construção.	No CodeBuild console da AWS, crie um projeto de compilação e especifique seu nome.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Selecione a origem.	Esse padrão usa o Git para o repositório de código, então escolha na lista GitHub de opções disponíveis. Escolha um repositório público ou da sua GitHub conta.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Selecione um repositório.	Selecione o repositório a partir do qual você deseja compilar o código.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Selecione o ambiente.	Você pode selecionar em uma lista de imagens gerenciadas ou optar por uma imagem personalizada usando o Docker. Esse padrão usa a seguinte imagem gerenciada:	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	• **Note** Amazon Linux 2 (: O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs.) • Runtime: Padrão • Imagem versão 1.0	
selecione um perfil de serviço.	Você pode criar um perfil de serviço ou selecionar em uma lista de funções existentes.	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Adicionar variáveis de ambiente.	Na seção Configuração adicional, configure as seguintes variáveis de ambiente: • AWS_DEFAULT_REGION para a região padrão da AWS • AWS_ACCOUNT_ID para o número da conta do usuário • IMAGE_REPO para o repositório privado Amazon ECR • BUILD_TAG para a versão da compilação (a compilação mais recente é o valor dessa variável) • DOCKER_CONTAINER_NAME para o nome do contêiner na tarefa Essas variáveis são espaços reservados no arquivo `buildspec.yml` e serão substituídas por seus respectivos valores.	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Crie um arquivo buildspec.	Você pode criar um arquivo `buildspec.yml` no mesmo local de `pom.xml` e adicionar a configuração fornecida nesse padrão ou usar o editor buildspec on-line e adicionar a configuração. Configure as variáveis ambientais com os valores apropriados seguindo as etapas fornecidas.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Configure o projeto para artefatos.	(Opcional) Configure o projeto de construção para artefatos, se necessário.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Configure o Amazon CloudWatch Logs.	(Opcional) Configure o Amazon CloudWatch Logs para o projeto de compilaçã o, se necessário. Esta etapa é opcional, mas recomendada.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Configurar logs do Amazon S3.	(Opcional) Configure logs do Amazon Simple Storage Service (Amazon S3) para o projeto de compilação, se quiser armazenar logs.	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Configure o pipeline na AWS CodePipeline

Tarefa	Descrição	Habilidades necessárias
Crie um pipeline.	No CodePipeline console da AWS, crie um pipeline e especifique seu nome. Para obter mais informações sobre	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	a criação de um pipeline, consulte a CodePipeline documentação da AWS.	
Selecionar um perfil de serviço.	Crie um perfil de serviço ou selecione na lista de perfis de serviço existentes. Se você estiver criando uma função de serviço, forneça um nome para a função e selecione a opção CodePipeline para criar a função.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Selecione uma loja de artefatos.	Em Configurações avançadas , se você quiser que o Amazon S3 crie um bucket e armazene os artefatos nele, use o local padrão para o armazenamento de artefatos. Ou selecione um local personalizado e especifiq ue um bucket existente. Você também pode optar por criptografar o artefato usando uma chave de criptografia.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Especificar o provedor de origem	Em Provedor de origem, escolha GitHub (Versão 2).	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Selecione o repositório e a ramificação do código.	Se você não estiver conectado , forneça os detalhes da conexão à qual se conectar GitHub e selecione o nome do repositório e o nome da ramificação.	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Altere as opções de detecção.	selecione Iniciar o pipeline na alteração do código-fonte e vá para a próxima página.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Selecione um provedor de compilação.	Para provedor de compilação, escolha AWS e CodeBuild, em seguida, forneça os detalhes da região da AWS e do nome do projeto para o projeto de construção. Em Tipo de compilação, selecione Compilação única.	Desenvolvedor de aplicativos, administrador de sistemas da AWS
Selecione um provedor de implantação.	Em Provedor de implantaç ão, selecione Amazon ECS. Selecione o nome do cluster, o nome do serviço, o arquivo de definições de imagens, se houver, e um valor de tempo limite de implantação, se necessário. Selecione Criar pipeline.	Desenvolvedor de aplicativos, administrador de sistemas da AWS

Recursos relacionados

- Documentação do AWS ECS
- Documentação do AWS ECR
- CodeBuild Documentação da AWS
- CodePipeline Documentação da AWS
- Crie um pipeline de entrega contínua para suas imagens de contêiner com o Amazon ECR como Fonte (postagem no blog)

Implemente uma ChatOps solução para gerenciar os resultados do escaneamento SAST usando o Amazon Q Developer em aplicativos de bate-papo, ações personalizadas e AWS CloudFormation

Criado por Anand Bukkapatnam Tirumala (AWS)

Resumo

Esse padrão apresenta uma solução abrangente que usa o Amazon Q Developer em aplicativos de bate-papo para agilizar o gerenciamento de falhas de verificação de testes estáticos de segurança de aplicativos (SAST) relatadas. SonarQube Essa abordagem inovadora integra ações e notificações personalizadas em uma interface conversacional, permitindo processos eficientes de colaboração e tomada de decisão nas equipes de desenvolvimento.

No ambiente de desenvolvimento de software acelerado de hoje, gerenciar os resultados da verificação SAST com eficiência é crucial para manter a qualidade e a segurança do código. No entanto, muitas organizações enfrentam os seguintes desafios significativos:

- Atraso na conscientização de vulnerabilidades críticas devido a sistemas de notificação ineficientes
- Processos lentos de tomada de decisão causados por fluxos de trabalho de aprovação desconectados
- Falta de respostas imediatas e acionáveis às falhas do escaneamento SAST
- Comunicação e colaboração fragmentadas em torno das descobertas de segurança
- Configuração manual de infraestrutura demorada e propensa a erros para ferramentas de segurança

Esses problemas geralmente levam ao aumento dos riscos de segurança, atrasos nos lançamentos e à redução da produtividade da equipe. Para enfrentar esses desafios de forma eficaz, é necessária uma solução que possa agilizar o gerenciamento de resultados do SAST, aprimorar a colaboração em equipe e automatizar o provisionamento da infraestrutura.

Os principais recursos da solução incluem:

- Notificações personalizadas — alertas e notificações em tempo real são enviados diretamente aos canais de bate-papo da equipe, garantindo o conhecimento e a ação imediatos sobre as vulnerabilidades ou falhas do escaneamento SAST.

- Aprovações conversacionais — As partes interessadas podem iniciar e concluir fluxos de trabalho de aprovação dos resultados do escaneamento SAST sem problemas na interface de bate-papo, acelerando os processos de tomada de decisão.
- Ações personalizadas — As equipes podem definir e executar ações personalizadas com base nos resultados da verificação do SAST, como acionar automaticamente mensagens de e-mail em caso de falhas no Quality Gate, melhorando a capacidade de resposta aos problemas de segurança.
- Colaboração centralizada — Todas as discussões, decisões e ações relacionadas ao escaneamento SAST são mantidas em um ambiente de bate-papo unificado, promovendo melhor colaboração e compartilhamento de conhecimento entre os membros da equipe.
- Infraestrutura como código (IaC) — Toda a solução está repleta de AWS CloudFormation modelos, permitindo um provisionamento de infraestrutura mais rápido e confiável, ao mesmo tempo que reduz os erros de configuração manual.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Uma função AWS Identity and Access Management (IAM) com permissões para criar e gerenciar recursos associados aos Serviços da AWS listados em Ferramentas.
- Um espaço de trabalho do Slack.
- O Amazon Q Developer em aplicativos de bate-papo foi adicionado ao espaço de trabalho necessário do Slack como um plug-in. Para obter mais informações, consulte Adicionar aplicativos ao seu espaço de trabalho do Slack na documentação do Slack. Anote o ID do espaço de trabalho do Slack, conforme mostrado AWS Management Console após o registro bem-sucedido.
- Um Amazon Q Developer configurado no cliente de aplicativos de bate-papo, com o ID do espaço de trabalho prontamente disponível para entrada no AWS CloudFormation console. Para obter instruções, consulte Configurar um cliente Slack no Guia do administrador do Amazon Q Developer em aplicativos de bate-papo.
- Uma conta de e-mail de origem criada e verificada no Amazon Simple Email Service (Amazon SES) para enviar mensagens de e-mail de aprovação. Para obter instruções de configuração, consulte Criação e verificação de identidades de e-mail no Guia do desenvolvedor do Amazon Simple Email Service.

- Um endereço de e-mail de destino para receber notificações de aprovação. Esse endereço pode ser uma caixa de entrada compartilhada ou uma lista específica de distribuição da equipe.
- Uma SonarQube instância operacional que pode ser acessada a partir do seu Conta da AWS. Para obter mais informações, consulte as instruções SonarQube de instalação.
- Um token de SonarQube usuário com permissões para acionar e criar projetos por meio do pipeline.

Limitações

- A criação de botões de ação personalizados é um processo manual nessa solução.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

O diagrama mostra o fluxo de trabalho automatizado de garantia de qualidade do código:

1. Preparação e upload do código:
   - O desenvolvedor compacta a base de código em um arquivo.zip.
   - O desenvolvedor carrega manualmente o arquivo.zip em um bucket designado do Amazon Simple Storage Service (Amazon S3).
2. Gatilho e orquestração de eventos do Amazon S3: AWS Step Functions
   - O evento de upload do Amazon S3 aciona um fluxo de trabalho Step Functions.
   - Step Functions orquestra uma verificação SAST usando. SonarQube
   - O fluxo de trabalho monitora o status do AWS CodeBuild trabalho para determinar as próximas ações. Se for CodeBuild bem-sucedido (Quality Gate Pass), o fluxo de trabalho será encerrado. Se CodeBuild falhar, uma AWS Lambda função será invocada para diagnóstico. Para obter mais detalhes, consulte a AWS Step Functions lógica posteriormente nesta seção.
3. AWS CodeBuild execução:
   - O CodeBuild trabalho executa uma SonarQube varredura na base de código carregada.

- Os artefatos de digitalização são armazenados em um bucket separado do Amazon S3 para auditoria e análise.

4. Análise de falhas (função Lambda):
   - Em CodeBuild caso de falha, a função `CheckBuildStatus` Lambda é acionada.
   - Em CodeBuild caso de sucesso, o processo é encerrado e nenhuma ação adicional é necessária.
5. A função Lambda analisa a causa da falha (falha na porta de qualidade ou outros problemas)
   - A `CheckBuildStatus` função cria uma carga personalizada com informações detalhadas sobre falhas.
   - A `CheckBuildStatus` função publica a carga personalizada em um tópico do Amazon Simple Notification Service (Amazon SNS).
6. Sistema de notificação:
   - O Amazon SNS encaminha a carga para o Amazon Q Developer em aplicativos de bate-papo para integração com o Slack.
7. Integração com o Slack:
   - O Amazon Q Developer em aplicativos de bate-papo publica uma notificação no canal designado do Slack.
8. Processo de aprovação:
   - Os aprovadores analisam os detalhes da falha na notificação do Slack.
   - Os aprovadores podem iniciar a aprovação usando o botão Aprovar no Slack.
9. Manipulador de aprovação:
   - Uma função do Approval Lambda processa a ação de aprovação do Slack.
   - A função de aprovação publica a mensagem personalizada no Amazon SES.
10. Mensagem gerada:
    - A função de aprovação gera uma mensagem personalizada para notificação ao desenvolvedor.
11. Notificação ao desenvolvedor:
    - O Amazon SES envia uma mensagem de e-mail ao desenvolvedor com as próximas etapas ou ações necessárias.

Esse fluxo de trabalho combina o upload manual de código com verificações de qualidade automatizadas, fornece feedback imediato por meio do Slack e permite a intervenção humana quando necessário, garantindo um processo de revisão de código robusto e flexível.

AWS Step Functions lógica

Conforme mostrado no diagrama de arquitetura anterior, se a passagem do portal de qualidade SonarQube falhar, o fluxo de trabalho vai para a função `CheckBuildStatus` Lambda. A `CheckBuildStatus` função aciona uma notificação no canal do Slack. Cada notificação inclui informações com as próximas etapas sugeridas. A seguir estão os tipos de notificações:

- O aplicativo falhou na verificação de segurança do código — O usuário recebe essa notificação quando o código carregado não passou pela verificação SonarQube de segurança. O usuário pode escolher APROVAR para aceitar a compilação. No entanto, a notificação aconselha o usuário a tomar cuidado com possíveis riscos de baixa qualidade do código e de segurança. A notificação inclui os seguintes detalhes:
  - Próximas etapas: Erro: Status do Quality Gate: FALHOU — Veja os detalhes no URL fornecido.
  - Faça a triagem das vulnerabilidades conforme mencionado no documento no URL fornecido.
  - CodeBuild os detalhes estão disponíveis no local no URL fornecido.
- O pipeline de verificação do aplicativo falhou por algum outro motivo — O usuário recebe essa notificação quando o pipeline falhou por algum motivo que não seja a falha na verificação de segurança do código. A notificação inclui os seguintes detalhes:
  - Para ver as próximas etapas, acesse o link fornecido para obter mais informações sobre a solução de problemas.

Para ver as capturas de tela das notificações conforme elas aparecem em um canal do Slack, acesse a pasta de ativos no repositório GitHub chatops-slack.

O diagrama a seguir mostra um exemplo do status da etapa do Step Functions após a falha na aprovação do portão de qualidade.

Ferramentas

Serviços da AWS

- O Amazon Q Developer em aplicativos de bate-papo permite que você use os canais de bate-papo Amazon Chime, Microsoft Teams e Slack para monitorar e responder a eventos operacionais em seus aplicativos. AWS Aviso de fim do suporte: em 20 de fevereiro de 2026, AWS encerrará o suporte para o serviço Amazon Chime. Depois de 20 de fevereiro de 2026, você não poderá mais acessar o console do Amazon Chime ou os recursos do aplicativo Amazon Chime. Para obter

mais informações, acesse a postagem do blog. Isso não afeta a disponibilidade do serviço Amazon Chime SDK.

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação.
- O Amazon Simple Email Service (Amazon SES) ajuda você a enviar e receber mensagens de e-mail usando seus próprios endereços de e-mail e domínios.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.

Outras ferramentas

- O Slack, uma oferta da Salesforce, é uma plataforma conversacional baseada em IA que fornece colaboração por chat e vídeo, automatiza processos sem código e oferece suporte ao compartilhamento de informações.
- SonarQubeé uma ferramenta de análise local projetada para detectar problemas de codificação em mais de 30 linguagens, estruturas e plataformas de IaC.

Repositório de código

O código desse padrão está disponível no repositório GitHub chatops-slack.

Práticas recomendadas

- CloudFormation gerenciamento de pilha — Se você encontrar alguma falha durante a execução da CloudFormation pilha, recomendamos que você exclua a pilha com falha. Em seguida, recrie-o com os valores corretos dos parâmetros. Essa abordagem oferece suporte a uma implantação limpa e ajuda a evitar possíveis conflitos ou implementações parciais.
- Configuração de e-mail de caixa de entrada compartilhada — Ao configurar o `SharedInboxEmail` parâmetro, use uma lista de distribuição comum que seja acessível a todos os desenvolvedores relevantes. Essa abordagem promove transparência e ajuda notificações importantes a chegarem aos membros relevantes da equipe.
- Fluxo de trabalho de aprovação de produção — Para ambientes de produção, restrinja o acesso ao canal do Slack usado para aprovações de criação. Somente aprovadores designados devem ser membros desse canal. Essa prática mantém uma cadeia clara de responsabilidade e aumenta a segurança ao limitar quem pode aprovar mudanças críticas.
- Permissões do IAM — siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Execute a configuração inicial

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Para clonar o repositório chatops-slack para esse padrão, use o comando a seguir. `git clone “git@github.com:aws-samples/chatops-slack.git“`	AWS DevOps, líder de construção, DevOps engenheiro, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

Crie os arquivos.zip que contêm o código Lambda.	Crie os arquivos.zip para o código da AWS Lambda função da `ApprovalEmail` funcionalidade `CheckBuildStatus` e. Para criar `notification.zip` `eapproval.zip` , use os comandos a seguir.
	`cd chatops-slack/src`
	`chmod -R 775 *`
	`zip -r approval.zip approval`
	`zip -r notification.zip notification`
		AWS DevOps, líder de construção, DevOps engenheiro, administrador de nuvem

Implante o arquivo de pilha pre-requisite.yml

Tarefa	Descrição	Habilidades necessárias
Execute o arquivo `pre-requisite.yml` de pilha.	O arquivo de `pre-requisite.yml` CloudFormation pilha implanta os recursos iniciais necessários antes de você executar o arquivo de `app-security.yml` pilha. Para executar o `pre-requisite.yml` arquivo, faça o seguinte:	Administrador da AWS, AWS DevOps, líder de construção, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	1. Faça login no AWS Management Console e abra o AWS CloudFormationconsole. Escolha Criar pilha e, em seguida, escolha Com novos recursos (padrão) na lista suspensa. 2. Na página Criar pilha, escolha Escolher um modelo existente e Carregar um arquivo de modelo. Em seguida, escolha Escolher arquivo e selecione pre-requisite.yml. Escolha Próximo. 3. Na página Especificar detalhes da pilha, insira valores para os parâmetros conforme descrito em Informações adicionais. Em seguida, escolha Próximo. 4. Na página Configurar opções de pilha, escolha a função do IAM para criar os recursos, conforme descrito em Pré-requisitos. Em seguida, escolha Próximo. 5. Na página Revisar e criar, escolha Enviar. 6. Na página de detalhes da pilha, escolha as guias Recursos e Saídas. Anote os valores dos	

Tarefa	Descrição	Habilidades necessárias
	`CKMSKeyId` parâmetro s `S3LambdaCKMSKeyAr n` , e que são usados nas etapas a seguir.	
Faça o upload dos arquivos. zip para o bucket do Amazon S3.	Faça upload dos `approval. zip` arquivos `notificat ion.zip` e que você criou anteriormente para o bucket do Amazon S3 chamado. `S3LambdaBucket` O arquivo `app-security.yml` CloudFormation de pilha é usado `S3LambdaBucket` para provisionar a função Lambda.	AWS DevOps, líder de construção, DevOps engenheiro, administrador de sistemas da AWS

Execute o arquivo de pilha app-security.yml

Tarefa	Descrição	Habilidades necessárias
Execute o arquivo `app-secur ity.yml` de pilha.	Os arquivos da `app-secur ity.yml` pilha implantam a infraestrutura restante para o sistema de notificação e aprovação. Para executar o `app-security.yml` arquivo, faça o seguinte: 1. Faça login no AWS Management Console e abra o AWS CloudForm ationconsole. Escolha Criar pilha e, em seguida, escolha Com novos	AWS DevOps, administrador de sistemas da AWS, DevOps engenheiro, líder de criação

Tarefa	Descrição	Habilidades necessárias
	recursos (padrão) na lista suspensa. 2. Na página Criar pilha, escolha Escolher um modelo existente e Carregar um arquivo de modelo. Em seguida, escolha Escolher arquivo e selecione app-security.yml. Escolha Próximo. 3. Na página Especificar detalhes da pilha, insira valores para os parâmetros conforme descrito em Informações adicionais. Em seguida, escolha Próximo. 4. Na página Configurar opções de pilha, escolha a função do IAM para criar os recursos, conforme descrito em Pré-requisitos. Em seguida, escolha Próximo. 5. Na página Revisar e criar, escolha Enviar.	

Tarefa	Descrição	Habilidades necessárias
Teste a configuração da notificação.	Para testar a configuração da notificação, faça o seguinte: 1. Abra o console do Amazon SNS. No painel de navegação à esquerda, selecione Tópicos. 2. Selecione o nome do tópico que termina com LambdaToAWSSlackChatbot. 3. Na página de detalhes do tópico, escolha Publicar mensagem. 4. Na página Publicar mensagem no tópico, em Corpo da mensagem a ser enviada ao endpoint, digite o seguinte: `{ "version": "1.0", "source": "custom", "content": { "description": ":warning: This is a test notification" } }` 5. Selecione Publish message (Publicar mensagem).	AWS DevOps, administrador de sistemas da AWS, DevOps engenheiro, líder de criação

Tarefa	Descrição	Habilidades necessárias
	Depois que a mensagem de teste for entregue com sucesso, você verá uma notificação no canal do Slack. Para obter mais informaçõ es, consulte Notificações de teste do Serviços da AWS Slack no Guia do administr ador do Amazon Q Developer em aplicativos de bate-papo.	

Configurar fluxo de aprovação

Tarefa	Descrição	Habilidades necessárias
Configure a ação personali zada do Lambda.	Para configurar a AWS Lambda ação personalizada, faça o seguinte: 1. Escolha o botão de reticências verticais na parte inferior da notificação de entrega em seu canal do Slack. 2. Em Gerenciar ações, escolha Criar. 3. Insira um nome de ação personalizado, por exemplo, Aprovar. Esse nome é um identificador exclusivo para sua ação personalizada. 4. Insira um nome para seu botão de ação personali	Administrador da AWS, AWS DevOps, líder de construção, DevOps engenheiro, administr ador do Slack

Tarefa	Descrição	Habilidades necessárias
	zado, por exemplo, Aprovar. Esse nome é exibido em um botão na sua notificação. Esse nome deve ter 20 caracteres ou menos e pode incorporar emojis. 5. Em Tipo de ação personali zada, selecione Ação Lambda. 6. Escolha Próximo. 7. Selecione Conta da AWS e Região da AWS onde você deseja implantar essa ação. 8. Escolha Carregar Lambdas. 9. Em Definir função Lambda, selecione uma função Lambda que termine com. ApprovalEmailLambdaEm seguida, escolha Próximo. 10. Para criar o botão Aprovar, escolha Salvar na página Exibir critérios.	

Tarefa	Descrição	Habilidades necessárias
Valide o fluxo de aprovação.	Para validar se o fluxo de aprovação funciona conforme o esperado, escolha o botão Aprovar no Slack. O Slackbot deve enviar uma notificação no tópico da mensagem com a string de confirmação E-mail de aprovação enviado com sucesso.	Administrador da AWS, AWS DevOps, DevOps engenheiro, administrador do Slack

Solução de problemas

Problema	Solução
Configurações incorretas do Slack	Para obter informações sobre como soluciona r problemas relacionados a configurações incorretas do Slack, consulte Solução de problemas do Amazon Q Developer no Guia do administrador do Amazon Q Developer em aplicativos de bate-papo.
A verificação falhou devido a algum outro motivo	Esse erro significa que a tarefa de criação do código falhou. Para solucionar o problema, acesse o link que está na mensagem. A falha na tarefa de criação de código pode ter as seguintes causas possíveis: • O aplicativo não está empacotado corretame nte. O `sonar-scanner` comando não consegue encontrar o `sonar.pro ject.env.properties` arquivo.

Problema	Solução
	• Os valores dos `SonarToken` parâmetros `SonarFileName` `SonarFileDirectory` , ou estão incorretos. Verifique os valores e, em seguida, execute os arquivos da pilha novamente. • O host do Sonar não está acessível. • Outros problemas que você pode usar os registros para solucionar.

Recursos relacionados

AWS documentação

- Configurar um cliente Slack
- Criação de uma ação personalizada
- Criando um procedimento de identidade de endereço de e-mail
- Tutorial: Comece a usar o Slack

Outros recursos

- Adicione aplicativos ao seu espaço de trabalho do Slack (documentação do Slack)
- Geração e uso de tokens (SonarQube documentação)
- Introdução à instalação do servidor (SonarQube documentação)

Mais informações

Essa solução enfatiza as ações personalizadas do Amazon Q Developer em aplicativos de bate-papo para fins de gerenciamento de lançamentos. No entanto, você pode reutilizar a solução modificando o código Lambda para seu caso de uso específico e construindo com base nela.

Parâmetros dos arquivos de CloudFormation pilha

A tabela a seguir mostra os parâmetros e suas descrições para o arquivo `pre-requisite.yml` de CloudFormation pilha.

Chave	Descrição
`StackName`	O nome da CloudFormation pilha.
`S3LambdaBucket`	O nome do bucket do Amazon S3 em que você carrega o código Lambda. O nome precisa ser globalmente exclusivo.
`SonarToken`	O token SonarQube do usuário, conforme descrito em Pré-requisitos.

A tabela a seguir mostra os parâmetros e suas descrições para o arquivo `app-security.yml` de CloudFormation pilha.

Chave	Descrição
`CKMSKeyArn`	O AWS KMS key Amazon Resource Name (ARN) usado nas funções do IAM e nas funções do Lambda criadas nessa pilha.
`CKMSKeyId`	O AWS KMS key ID usado no tópico do Amazon SNS criado nessa pilha.
`EnvironmentType`	O nome do ambiente do cliente para implantação do pipeline de verificação de aplicativos. Selecione o nome do ambiente na lista suspensa de valores permitidos.
`S3LambdaBucket`	O nome do bucket do Amazon S3 que contém os arquivos `approval.zip` e. `notification.zip`
`SESEmail`	O nome da identidade de e-mail registrada no Amazon SES, conforme descrito em Pré-requisitos. Essa identidade é o endereço de e-mail de origem.

`SharedInboxMail`	O endereço de e-mail de destino para o qual as notificações de escaneamento são enviadas.
`SlackChannelId`	O ID do canal do Slack para o qual você deseja que as notificações sejam enviadas. Para encontrar o ID do canal, clique com o botão direito do mouse no nome do canal em Detalhes do canal no app Slack. O ID do canal está na parte inferior.
`SlackWorkspaceId`	O ID do espaço de trabalho do Slack, conforme descrito em Pré-requisitos. Para encontrar o ID do espaço de trabalho do Slack, faça login no AWS Management Console, abra o Amazon Q Developer no console de aplicativos de bate-papo e escolha Clientes configurados, Slack, WorkspaceID.
`StackName`	O nome da CloudFormation pilha.
`SonarFileDirectory`	O diretório que contém o `sonar.project.<env>.properties` arquivo.
`SonarFileName`	O nome do `sonar.project.<env>properties` arquivo.
`SourceCodeZip`	O nome do arquivo.zip que contém o `sonar.project.<env>properties` arquivo e o código-fonte.

Implante um firewall usando o AWS Network Firewall e o AWS Transit Gateway

Criado por Shrikant Patil (AWS)

Resumo

Esse padrão mostra como implantar um firewall usando o AWS Network Firewall e o AWS Transit Gateway. Os recursos do Network Firewall são implantados usando um CloudFormation modelo da AWS. O Network Firewall se expande automaticamente com seu tráfego de rede e pode suportar centenas de milhares de conexões, para que você não precise se preocupar em criar e manter sua própria infraestrutura de segurança de rede. Um gateway de trânsito é um hub de trânsito de rede que você pode usar para interconectar suas nuvens privadas virtuais (VPCs) e redes locais.

Nesse padrão, você também aprende a incluir uma VPC de inspeção em sua arquitetura de rede. Por fim, esse padrão explica como usar a Amazon CloudWatch para fornecer monitoramento de atividades em tempo real para seu firewall.

> **Tip**
>
> É uma prática recomendada evitar o uso de uma sub-rede do Network Firewall para implantar outros serviços da AWS. Isso ocorre porque o Network Firewall não pode inspecionar o tráfego de origens ou destinos na sub-rede de um firewall.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões de políticas do perfil do AWS Identity and Access Management (IAM).
- CloudFormation permissões de modelo

Limitações

Você pode ter problemas com a filtragem de domínio e um tipo diferente de configuração pode ser necessário. Para obter mais informações, consulte Grupos de regras de domínio com estado no AWS Network Firewall na documentação do Network Firewall.

Arquitetura

Pilha de tecnologia

- CloudWatch Registros da Amazon
- Amazon VPC
- AWS Network Firewall
- AWS Transit Gateway

Arquitetura de destino

O diagrama a seguir mostra como usar o Network Firewall e o Gateway de trânsito para inspecionar o tráfego:

A arquitetura inclui os seguintes componentes:

- Seu aplicativo está hospedado em dois raios VPCs. Eles VPCs são monitorados pelo Network Firewall.
- A VPC de saída tem acesso direto ao gateway da Internet, mas não é protegida pelo Network Firewall
- A VPC de inspeção é onde o Network Firewall é implantado.

Automação e escala

Você pode usar CloudFormationpara criar esse padrão usando a infraestrutura como código.

Ferramentas

Serviços da AWS

- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas, aplicativos e serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.
- O AWS Network Firewall é um firewall de rede gerenciado e monitorado, além de um serviço de detecção e prevenção de intrusões VPCs na nuvem da AWS.

- O AWS Transit Gateway é um hub central que conecta VPCs redes locais.

Código

O código desse padrão está disponível na implantação do GitHub AWS Network Firewall com o repositório Transit Gateway. Você pode usar o CloudFormation modelo desse repositório para implantar uma única VPC de inspeção que usa o Network Firewall.

Épicos

Crie a VPC spoke e a VPC de inspeção

Tarefa	Descrição	Habilidades necessárias
Prepare e implante o CloudFormation modelo.	1. Baixe o `cloudformation/aws_nw_fw.yml` modelo do GitHub repositório. 2. Atualize o modelo com seus valores. 3. Implante o modelo.	AWS DevOps

Crie o gateway e as rotas de trânsito

Tarefa	Descrição	Habilidades necessárias
Criar um gateway de trânsito.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. 2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito). 3. Selecione Criar gateway de trânsito.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	4. Para Name tag (Tag de nome), insira um nome para o gateway de trânsito. 5. Para Description (Descrição), insira uma descrição para o gateway de trânsito. 6. Para Amazon side número de sistema autônomo (ASN), deixe o valor ASN padrão. 7. Selecione a opção suporte de DNS. 8. Selecione a opção suporte VPN ECMP. 9. Selecione a opção Associação de tabela de rotas padrão. Essa opção associa automaticamente os anexos do gateway de trânsito à tabela de rotas padrão para o gateway de trânsito. 10. Selecione a opção propagação da tabela de rotas padrão. Essa opção propaga automaticamente os anexos do gateway de trânsito à tabela de rotas padrão para o gateway de trânsito. 11. Selecione Criar gateway de trânsito.	

Tarefa	Descrição	Habilidades necessárias
Criar anexo do gateway de trânsito.	Crie um anexo do gateway de trânsito para o seguinte: • Um anexo de inspeção na sub-rede VPC e Transit Gateway de inspeção • Um anexo SpokeVPCA VPCA spoke e na sub-rede privada • Um anexo SpokeVPCB no VPCB spoke e na sub-rede privada • Um anexo EgressVPC na VPC de saída e na sub-rede privada	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Criar uma tabela de rotas do gateway de trânsito.	1. Criar uma tabela de rotas para o gateway de trânsito para a VPC spoke. Essa tabela de rotas deve estar associada a todas as VPCs outras, exceto à VPC de inspeção. 2. Criar uma tabela de rotas para o gateway de trânsito para o firewall. Essa tabela de rotas deve estar associada somente à VPC de inspeção. 3. Adicionar uma rota à tabela de rotas do gateway de trânsito para o firewall: • Para`0.0.0/0`, use o anexo EgressVPC. • Para o bloco CIDR SpokeVPCA, use o anexo Spoke. VPC1 • Para o bloco CIDR SpokeVPCB, use o anexo Spoke. VPC2 4. Adicionar uma rota à tabela de rotas do gateway de trânsito para a VPC spoke. Para `0.0.0/0`, use o anexo VPC de inspeção.	AWS DevOps

Crie o firewall e as rotas

Tarefa	Descrição	Habilidades necessárias
Crie um firewall na VPC de inspeção.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. 2. No painel de navegação , em Network Firewall, escolha Firewalls. 3. Escolha Criar firewall. 4. Em Name (Nome), insira o nome que deseja usar para identificar este firewall. Não é possível alterar o nome de um firewall depois de criá-lo. 5. Para VPC, selecione sua VPC de inspeção. 6. Em Zona de disponibilidade e Sub-rede, selecione a zona e a sub-rede do firewall que você identificou. 7. Na seção Política de firewall associada, escolha Associar uma política de firewall existente e selecione a política de firewall que você criou anteriormente. 8. Escolha Criar firewall.	AWS DevOps
Criar uma política de firewall.	1. Faça login no Console de Gerenciamento da AWS e	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	abra o console do Amazon VPC. 2. No painel de navegação, em Network Firewall, escolha Políticas de firewall. 3. Na página Descrever a política de firewall, escolha Criar política de firewall. 4. Em Nome, digite o nome que você deseja usar na política de firewall. Você usará o nome para identificar a política ao associar a política ao seu firewall posteriormente nesse padrão. Você não pode alterar o nome de uma política de firewall depois de criá-la. 5. Escolha Próximo. 6. Na página Adicionar grupos de regras, na seção Grupo de regras sem estado, escolha Adicionar grupos de regras sem estado. 7. Na caixa de diálogo Adicionar de grupos de regras existentes, marque a caixa de seleção do grupo de regras sem estado que você criou anteriormente. Escolha Adicionar grupos de regras. Observação: na	

Tarefa	Descrição	Habilidades necessárias
	parte inferior da página, o contador de capacidad e da política de firewall mostra a capacidade consumida ao adicionar esse grupo de regras ao lado da capacidade máxima permitida para uma política de firewall. 8. Defina a ação padrão sem estado como Encaminhar para regras com estado. 9. Na seção Grupo de regras com estado, escolha Adicionar grupos de regras com estado e, em seguida, marque a caixa de seleção do grupo de regras com estado que você criou anteriormente. Escolha Adicionar grupos de regras. 10 Escolha Avançar para percorrer o restante do assistente de configura ção e, em seguida, escolha Criar política de firewall.	

Tarefa	Descrição	Habilidades necessárias
Atualizar a tabela de rotas da VPC.	Inspeção: Tabelas de rotas da VPC 1. Na tabela de rotas da sub-rede ANF (`Inspection-ANFRT`), adicione `0.0.0/0` ao ID do Transit Gateway. 2. Na tabela de rotas de sub-rede do Transit Gateway (`Inspection-TGWRT`), adicione `0.0.0/0` ao EgressVPC. Tabela de rotas SpokeVPCA Na tabela de rotas privadas, adicione `0.0.0.0/0` à ID do Transit Gateway. Tabela de rotas Spoke VPCB Na tabela de rotas privadas, adicione `0.0.0.0/0` à ID do Transit Gateway. Tabelas de rotas da VPC de saída Na tabela de rotas públicas de saída, adicione o bloco CIDR SpokeVPCA e SpokeVPCB ao ID do gateway de trânsito. Repita a mesma etapa para a sub-rede privada.	AWS DevOps

Configurado CloudWatch para realizar inspeção de rede em tempo real

Tarefa	Descrição	Habilidades necessárias
Atualize a configuração de registro do firewall.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. 2. No painel de navegação , em Network Firewall, escolha Firewalls. 3. Na página Firewalls, escolha o nome do firewall que você deseja editar. 4. Escolha a guia Detalhes do firewall. Na seção Logs, selecione Edit (Editar). 5. Ajuste as seleções do tipo de registro conforme necessário. Você pode configurar o registro para registros de alertas e fluxos. • Alerta: envia registros de tráfego que correspon dem a qualquer regra de estado em que a ação esteja definida como Alerta ou Descartar. Para obter mais informações sobre regras com estado e grupos de regras, consulte Grupos de regras no AWS Network Firewall.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• Fluxo: envia logs de todo o tráfego de rede que o mecanismo sem estado encaminha para o mecanismo de regras com estado. 6. Para cada tipo de registro selecionado, escolha o tipo de destino e, em seguida, forneça as informações do destino de registro. Para obter mais informações, consulte os destinos de registro do AWS Network Firewall na documentação do Network Firewall. 7. Escolha Salvar.	

Verifique a configuração.

Tarefa	Descrição	Habilidades necessárias
Execute uma EC2 instância para testar a configuração.	Lance duas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) na VPC spoke: uma para o Jumpbox e outra para testar a conectividade.	AWS DevOps
Verifique as métricas.	As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, por várias combinações de dimensão dentro de cada	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	namespace. O CloudWatch namespace do Network Firewall é. `AWS/NetworkFirewall` 1. Faça login no Console de Gerenciamento da AWS e abra o console do CloudWatch . 2. No painel de navegação, selecione Métricas. 3. Na guia Todas as métricas, escolha a Região e, em seguida, escolha AWS/NetworkFirewall.	

Recursos relacionados

- Arquitetura simples de zona única com um gateway da internet
- Arquitetura de várias zonas com um gateway da Internet
- Arquitetura com um gateway da internet e um gateway NAT

Implante um trabalho do AWS Glue com um pipeline de CodePipeline CI/CD da AWS

Criado por Bruno Klein (AWS) e Luis Henrique Massao Yamada (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão demonstra como você pode integrar a AWS CodeCommit e a AWS CodePipeline com o AWS Glue e usar o AWS Lambda para iniciar trabalhos assim que um desenvolvedor envia suas alterações para um repositório remoto da AWS. CodeCommit

Quando um desenvolvedor envia uma alteração para um repositório de extração, transformação e carregamento (ETL) e envia as alterações para a AWS CodeCommit, um novo pipeline é invocado. O pipeline inicia uma função do Lambda que inicia um trabalho do AWS Glue com essas alterações. O trabalho do AWS Glue executa a tarefa de ETL.

Essa solução é útil na situação em que empresas, desenvolvedores e engenheiros de dados desejam iniciar tarefas assim que as alterações forem confirmadas e enviadas aos repositórios de destino. Isso ajuda a alcançar um nível mais alto de automação e reprodutibilidade, evitando erros durante o lançamento e o ciclo de vida do trabalho.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Git instalado na máquina local
- Amazon Cloud Development Kit (Amazon CDK) instalado na máquina local
- Python instalado na máquina local
- O código na seção Anexos

Limitações

- O pipeline é concluído assim que o trabalho do AWS Glue for lançado com sucesso. Ele não vai esperar chegar ao fim do trabalho.
- O código fornecido no anexo é destinado apenas para fins de demonstração.

Arquitetura

Pilha de tecnologias de destino

- AWS Glue
- AWS Lambda
- AWS CodePipeline
- AWS CodeCommit

Arquitetura de destino

O processo consiste nestas etapas:

1. O desenvolvedor ou engenheiro de dados faz uma modificação no código ETL, confirma e envia a alteração para a AWS. CodeCommit
2. O push inicia o pipeline.
3. O pipeline inicia uma função do Lambda, que chama `codecommit:GetFile` no repositório e faz upload do arquivo para o Amazon Simple Storage Service (Amazon S3).
4. A função do Lambda lança um novo trabalho do AWS Glue com o código ETL.
5. A função do Lambda finaliza o pipeline.

Automação e escala

O exemplo de anexo demonstra como você pode integrar o AWS Glue com a AWS CodePipeline. Ele fornece um exemplo básico que você pode personalizar ou estender para seu próprio uso. Consulte a seção Épicos para obter detalhes.

Ferramentas

- AWS CodePipeline — CodePipeline A AWS é um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura.
- AWS CodeCommit — CodeCommit A AWS é um serviço de controle de origem totalmente gerenciado que hospeda repositórios seguros baseados em Git.

- AWS Lambda: o AWS Lambda é um serviço de computação com tecnologia sem servidor que pode ser usado para executar código sem provisionamento ou gerenciamento de servidores.
- AWS Glue: o AWS Glue é um serviço de integração de dados com tecnologia sem servidor que facilita a descoberta, preparação e combinação de dados para análise, machine learning e desenvolvimento de aplicações.
- Cliente Git — O Git fornece ferramentas de GUI, ou você pode usar a linha de comando ou uma ferramenta de desktop para verificar os artefatos necessários. GitHub
- CDK da AWS: o CDK da AWS é um framework de desenvolvimento de software de código aberto que ajuda a definir recursos de aplicativos em nuvem usando linguagens de programação familiares.

Épicos

Implantar o código de exemplo

Tarefa	Descrição	Habilidades necessárias
Configure a AWS CLI.	Configure a AWS Command Line Interface (AWS CLI) para direcionar e autenticar com sua conta da AWS atual. Para obter instruções, consulte a documentação da AWS CLI.	Desenvolvedor, DevOps engenheiro
Extraia os arquivos de exemplo do projeto.	Extraia os arquivos do anexo para criar uma pasta que contém os arquivos de exemplo do projeto.	Desenvolvedor, DevOps engenheiro

Implantar o código de exemplo.	Depois de extrair os arquivos, execute os seguintes comandos no local da extração para criar um exemplo básico:
	`cdk bootstrap`
	`cdk deploy`
		Desenvolvedor, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`git init`
	`git remote add origin <code-commit-repository-url>`
	`git stage .`
	`git commit -m "adds sample code"`
	`git push --set-upstream origin main`
	
	Depois do último comando, é possível monitorar o status do pipeline e do trabalho do AWS Glue.	

Personalize o código.	Personalize o código do arquivo etl.py de acordo com seus requisitos comerciais. Você pode revisar o código ETL, modificar os estágios do pipeline ou estender a solução.	Engenheiro de dados

Recursos relacionados

- Conceitos básicos dos AWS CDK
- Adicionar trabalhos no AWS Glue
- Integrações de ações de origem em CodePipeline
- Invoque uma função do AWS Lambda em um pipeline no CodePipeline
- Programação do AWS Glue
- CodeCommit GetFile API DA AWS

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Implante um cluster Amazon EKS a partir do AWS Cloud9 usando um perfil de instância EC2

Criado por Sagar Panigrahi (AWS)

Resumo

Aviso: não AWS Cloud9 está mais disponível para novos clientes. Os clientes existentes do AWS Cloud9 podem continuar usando o serviço normalmente. Saiba mais

Esse padrão descreve como usar o AWS Cloud9 e o CloudFormation AWS para criar um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) que pode ser operado sem permitir o acesso programático para usuários em sua conta da Amazon Web Services (AWS).

O AWS Cloud9 é um ambiente de desenvolvimento integrado (IDE) baseado em nuvem que ajuda você a escrever, executar e depurar código por meio de um navegador. O AWS Cloud9 é usado como um centro de controle que provisiona um cluster Amazon EKS usando perfis de instância do Amazon Elastic Compute Cloud (EC2Amazon) e modelos da AWS. CloudFormation

Você pode usar esse padrão se não quiser criar usuários do Identity and Access Management (IAM) na AWS e desejar usar perfis do IAM. O controle de acesso com base em função (RBAC) regula o acesso a recursos com base nas funções de usuários individuais. Esse padrão demonstra como atualizar o RBAC em um cluster do Amazon EKS para permitir o acesso a um perfil do IAM específico.

A configuração do padrão também ajuda sua DevOps equipe a usar os recursos do AWS Cloud9 para manter e desenvolver recursos de infraestrutura como código (IaC) para criar a infraestrutura do Amazon EKS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões para criar perfis do IAM e políticas do IAM para a conta. O perfil do IAM para o usuário deve incluir a política `AWSCloud9Administrator`. Os perfis `AWSServiceRoleForAmazonEKS` e `eksNodeRoles` também devem ser criados porque são necessários para criar um cluster do Amazon EKS.

- Conhecimento dos conceitos do Kubernetes.

Limitações

- Esse padrão descreve como criar um cluster do Amazon EKS. Para clusters de produção, você deve atualizar o CloudFormation modelo da AWS.
- O padrão não implanta componentes adicionais do Kubernetes (por exemplo, Fluentd, controladores de entrada ou controladores de armazenamento).

Arquitetura

Pilha de tecnologia

- AWS Cloud9
- AWS CloudFormation
- Amazon EKS
- IAM

Automação e escala

Você pode expandir esse padrão e incorporá-lo aos pipelines de integração contínua e implantação contínua (CI/CD) para automatizar o provisionamento completo do Amazon EKS.

Ferramentas

- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos.
- AWS Cloud9: o AWS Cloud9 oferece uma experiência de edição de código completa com suporte para várias linguagens de programação e depuradores de runtime, além de um terminal integrado.
- AWS CLI: a AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

- Kubectl: `kubectl` é um utilitário de linha de comando que você usa para interagir com um cluster do Amazon EKS.

Épicos

Crie as funções do IAM para o perfil da EC2 instância

Tarefa	Descrição	Habilidades necessárias
Crie a política do IAM.	Faça login no Console de Gerenciamento da AWS, abra o console do IAM, selecione Políticas e selecione Criar política. Escolha a guia JSON e cole o conteúdo do arquivo policy-role-eks-instance - profile-for-cloud 9.json (anexado). Resolva quaisquer avisos de segurança, erros ou avisos gerais gerados durante a validação de política e, depois, escolha Revisar política. Insira um Nome para a política. Recomendamos usar o nome da política `eks-instance-profile-for-cloud9` . Revise o Resumo da política para ver as permissões que são concedidas pela política. Selecione Criar política.	Administrador de nuvem
Crie um perfil do IAM usando a política.	No console do IAM, escolha Perfis e Criar perfil. Escolha AWS Service e, em seguida, escolha EC2na lista.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Escolha Avançar: Permissões e pesquise a política do IAM que você criou anteriormente. Escolha as tags apropriadas para suas necessidades. Na seção Revisar, digite um nome para o perfil. Recomendamos que você use `role-eks-instance-profile-for-cloud9` como nome do perfil. Então, escolha Criar perfil.	

Crie a política do IAM e o perfil para o Amazon EKS RBAC.

Tarefa	Descrição	Habilidades necessárias
Crie a política do IAM.	No console do IAM, escolha Políticas e escolha Criar política. Escolha a guia JSON e cole o conteúdo do policy-for-eks-rbac arquivo.json (anexado). Resolva quaisquer avisos de segurança, erros ou avisos gerais gerados durante a validação de política e, depois, escolha Revisar política. Insira um Nome para a política. Recomendamos usar o nome da política `policy-for-eks-rbac` . Revise o Resumo da política para	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	ver as permissões que são concedidas pela política. Selecione Criar política.	
Crie um perfil do IAM usando a política.	No console do IAM, escolha Perfis e Criar perfil. Escolha AWS Service e, em seguida, escolha EC2na lista. Escolha Avançar: Permissões e pesquise a política do IAM que você criou anteriormente. Escolha as tags apropriadas para suas necessidades. Na seção Revisar, digite um nome para o perfil. Recomendamos que você use `role-eks-admin-for-rbac` como nome do perfil. Então, escolha Criar perfil.	Administrador de nuvem

Crie o ambiente AWS Cloud9

Tarefa	Descrição	Habilidades necessárias
Crie o ambiente AWS Cloud9.	Abra o console do AWS Cloud9 e escolha Criar ambiente. Na página Nomear ambiente, em Nome, digite um nome para o ambiente. Recomendamos que você use `eks-management-env` para o nome do ambiente. Defina as configurações restantes de acordo com seus	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	requisitos e escolha Próxima etapa. Na página Revisar, selecione Criar ambiente. Aguarde enquanto o AWS Cloud9 cria o ambiente. Isso pode demorar vários minutos. Para obter mais informações sobre as opções de configuração disponíveis, consulte Criação de um EC2 ambiente na documentação do AWS Cloud9.	
Remova as credenciais temporárias do IAM para o AWS Cloud9.	Depois que seu ambiente AWS Cloud9 for provisionado, escolha Configurações no ícone de engrenagem. Em Preferências, escolha as configurações da AWS e, em seguida, escolha Credenciais. Desative as credenciais temporárias gerenciadas pela AWS e feche a guia.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Anexe o perfil da EC2 instância à EC2 instância subjacente.	Abra o EC2 console da Amazon e escolha a EC2 instância que correspon de ao seu ambiente no AWS Cloud9. Se você usou o nome que recomenda mos, a EC2 instância será chamada`aws-cloud9-eks-management-env` . Escolha a EC2 instância, escolha Ações e, em seguida, escolha Configurações da instância. Escolha Anexar/su bstituir perfil do IAM. Pesquise `role-eks-instance-profile-for-cloud9` ou o nome do perfil do IAM que você criou anteriormente e escolha Aplicar.	Administrador de nuvem

Crie o cluster do Amazon EKS.

Tarefa	Descrição	Habilidades necessárias
Crie o cluster do Amazon EKS.	Baixe e abra o modelo eks-cfn.yaml (em anexo) para a AWS. CloudFormation Edite o modelo de acordo com suas necessidades. Abra o console do AWS Cloud9 e escolha Novo arquivo. Cole o CloudForm ation modelo da AWS que	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	você criou anteriormente no campo. Recomendamos usar eks-cfn.yaml para o nome do modelo. No terminal do AWS Cloud9, execute o seguinte comando para criar o cluster do Amazon EKS: `aws cloudformation create-stack --stack-name eks-cluster --template-body file://eks-cfn.yaml --region <your_AWS_Region>` Se a CloudFormation chamada da AWS for bem-sucedida, você receberá o Amazon Resource Name (ARN) da CloudFormation pilha da AWS em sua saída. A criação da pilha pode levar de 10 a 20 minutos.	

Tarefa	Descrição	Habilidades necessárias
Verifique o status do cluster do Amazon EKS.	No CloudFormation console da AWS, abra a página Stacks e escolha o nome da pilha. A pilha é criada quando o código de status da pilha exibe `CREATE_COMPLETE` . Para obter mais informaçõ es, consulte Visualização de dados e recursos do AWS CloudFormation Stack na CloudFormation documenta ção da AWS.	Administrador de nuvem

Acesse os recursos do Kubernetes no cluster Amazon EKS

Tarefa	Descrição	Habilidades necessárias
Instale o kubectl no ambiente AWS Cloud9.	Instale `kubectl` em seu ambiente AWS Cloud9 seguindo as instruções de Como instalar o kubectl na documentação do Amazon EKS.	Administrador de nuvem
Atualize a nova configuração do Amazon EKS no AWS Cloud9.	Execute o seguinte comando no terminal AWS Cloud9 para atualizar o `kubeconfig` do cluster Amazon EKS para o ambiente AWS Cloud9: `aws eks update-ku beconfig --name EKS-DEV2 --region <your_AWS_Region>`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Important `EKS-DEV2`é o nome do cluster Amazon EKS no CloudFormation modelo da AWS que você usou para criar o cluster. Execute o comando `kubectl get all -A` para ver todos os recursos do Kubernetes.	

Tarefa	Descrição	Habilidades necessárias

Adicione o perfil do IAM de administrador ao RBAC do Kubernetes.	Execute o seguinte comando em seu terminal do AWS Cloud9 para abrir o mapa de configuração do RBAC para o Amazon EKS no modo de edição:
	`kubectl edit cm/aws-auth -n kube-system`
	Anexe as seguintes linhas abaixo da seção `mapRoles`:
	`- groups:`
	`- system:masters`
	`rolearn: <ARN_of_IAM_role _from_second_epic>`
	`username: eksadmin`
	Limite o arquivo formatado em YAML para evitar erros de sintaxe. Salve o arquivo usando `vi` comandos e saia do arquivo.
	Note
	Ao adicionar esta seção, você informa ao Kubernetes RBAC que `<ARN_of_IAM_role _from_second_epic>` receberá acesso total
		Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	de administrador no cluster Amazon EKS. Isso significa que o perfil do IAM identific ado pode realizar ações administr ativas no cluster Kubernetes. A AWS adiciona a seção `mapRoles` existente abaixo enquanto o cluster Amazon EKS é provisionado.	

Recursos relacionados

Referências

- Arquitetura modular e escalável do Amazon EKS (Quick Start)
- Gerenciamento de usuários ou perfis do IAM para o cluster de seu Amazon EKS
- CloudFormation Modelo da AWS para criar um novo plano de controle do Amazon EKS

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Implante código em várias regiões da AWS usando AWS CodePipeline CodeCommit, AWS e AWS CodeBuild

Criado por Anand Krishna Varanasi (AWS)

Resumo

Esse padrão demonstra como criar infraestrutura ou arquitetura em várias regiões da Amazon Web Services (AWS) usando a AWS CloudFormation. Inclui integração contínua (CI) /implantação contínua (CD) em várias regiões da AWS para implantações mais rápidas. As etapas desse padrão foram testadas para a criação de um CodePipeline trabalho da AWS para implantação em três regiões da AWS, como exemplo. Você pode alterar o número de regiões com base no caso de uso.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- • Uma CodeBuild função com o AmazonS3 FullAccess e as políticas. CloudWatchFullAccess Essas políticas dão CodeBuild acesso para assistir eventos da AWS CodeCommit por meio da Amazon CloudWatch e usar o Amazon Simple Storage Service (Amazon S3) como um armazenamento de artefatos.
  - Uma CloudFormation função da AWS com as seguintes políticas, que dão à AWS CloudFormation, no estágio final de criação, a capacidade de criar ou atualizar funções do AWS Lambda, enviar ou observar CloudWatch registros da Amazon e criar e atualizar conjuntos de alterações.
    - AWSLambdaFullAccess
    - AWSCodeDeployFullAccess
    - CloudWatchFullAccess
    - AWSCloudFormationFullAccess
    - AWSCodePipelineFullAccess

> **Note**
>
> Duas funções do AWS Identity and Access Management (IAM) para a AWS CodeBuild e a AWS CloudFormation com políticas adequadas CodeBuild para realizar as tarefas de CI de testar, agrupar, empacotar os artefatos e implantá-los em várias regiões da AWS

em paralelo. Verifique as políticas criadas por CodePipeline para verificar se a CodeBuild AWS CloudFormation tem as permissões adequadas nas fases de CI e CD.

Arquitetura

A arquitetura e o fluxo de trabalho de várias regiões deste padrão abrangem as etapas a seguir.

1. Você envia seu código para um CodeCommit repositório.
2. Ao receber qualquer atualização ou confirmação de código, CodeCommit invoca um CloudWatch evento que, por sua vez, inicia um CodePipeline trabalho.
3. CodePipeline envolve o CI que é tratado por. CodeBuild As tarefas a seguir são executadas.
   - Teste dos CloudFormation modelos da AWS (opcional)
   - Empacotamento dos CloudFormation modelos da AWS para cada região incluída na implantação. Por exemplo, esse padrão é implantado paralelamente em três regiões da AWS, então CodeBuild empacota os CloudFormation modelos da AWS em três buckets S3, um em cada região especificada. Os buckets do S3 são usados somente CodeBuild como repositórios de artefatos.
4. CodeBuild empacota os artefatos como entrada para a próxima fase de implantação, que é executada paralelamente nas três regiões da AWS. Se você especificar um número diferente de regiões, CodePipeline será implantado nessas regiões.

Ferramentas

Ferramentas

- AWS CodePipeline — CodePipeline é um serviço de entrega contínua que você pode usar para modelar, visualizar e automatizar as etapas necessárias para liberar suas alterações de software continuamente.
- AWS CodeBuild — CodeBuild é um serviço de construção totalmente gerenciado que compila seu código-fonte, executa testes unitários e produz artefatos prontos para implantação.
- AWS CodeCommit — CodeCommit é um serviço de controle de versão hospedado pela Amazon Web Services que você pode usar para armazenar e gerenciar de forma privada ativos (como código-fonte e arquivos binários) na nuvem.

- AWS CloudFormation — CloudFormation A AWS é um serviço que ajuda você a modelar e configurar seus recursos da Amazon Web Services para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos que são executados na AWS.
- AWS Identity and Access Management: o AWS Identity and Access Management (IAM) é um serviço da web que ajuda você a controlar o acesso aos recursos da AWS com segurança.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet. Ele foi projetado para facilitar a computação de escala na web para os desenvolvedores.

Código

O código de exemplo a seguir é para o arquivo `BuildSpec.yaml` (fase de compilação).

```
---
artifacts:
discard-paths: true
files:
- packaged-first-region.yaml
- packaged-second-region.yaml
- packaged-third-region.yaml
phases:
build:
commands:
- echo "********BUILD PHASE - CF PACKAGING**********"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_FIRST_REGION --output-template-file packaged-first-region.yaml --region
 $FIRST_REGION"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_SECOND_REGION --output-template-file packaged-second-region.yaml --region
 $SECOND_REGION"
- "aws cloudformation package --template-file sam-template-anand.yaml --s3-bucket
 $S3_THIRD_REGION --output-template-file packaged-third-region.yaml --region
 $THIRD_REGION"
install:
commands:
- echo "********BUILD PHASE - PYTHON SETUP**********"
runtime-versions:
python: 3.8
post_build:
commands:
- echo "********BUILD PHASE - PACKAGING COMPLETION**********"
```

```
pre_build:
commands:
- echo "********BUILD PHASE - DEPENDENCY SETUP**********"
- "npm install --silent --no-progress"
- echo "********BUILD PHASE - DEPENDENCY SETUP DONE**********"
version: 0.2
```

Épicos

Prepare o código e o CodeCommit repositório

Tarefa	Descrição	Habilidades necessárias
Selecione a principal região da AWS para a implantação.	Faça login em sua conta da AWS e escolha a região principal para a implantação. O CodeCommit repositório estará na região principal.	DevOps
Crie o CodeCommit repositór io.	Crie o CodeCommit repositór io e insira o código necessári o nele. O código geralment e inclui os modelos da AWS CloudFormation ou do AWS SAM, o código Lambda, se houver, e os CodeBuild `buildspec.yaml` arquivos como entrada para a AWS. CodePipeline	DevOps
Envie o código para o CodeCommit repositório.	Na seção Anexos, baixe o código desse exemplo e, em seguida, insira o código necessário nele. Geralmente, o código pode incluir modelos AWS CloudFormation ou AWS SAM, código Lambda e os CodeBuild `buildspec`	DevOps

Tarefa	Descrição	Habilidades necessárias
	`.yaml` arquivos como entrada para o pipeline.	

Fase de origem: criar o pipeline

Tarefa	Descrição	Habilidades necessárias
Crie o CodePipeline trabalho.	No CodePipeline console, escolha Criar pipeline.	DevOps
Dê um nome ao CodePipeline trabalho e escolha a configuração da função de serviço.	Insira um nome para o trabalho e mantenha a configuração padrão da função de serviço para CodePipeline criar a função com as políticas necessárias anexadas.	DevOps
Especifique a localização do armazenamento de artefatos.	Em Configurações avançadas, mantenha a opção padrão para CodePipeline criar um bucket S3 para usar no armazenamento de artefatos de código. Se você usar um bucket S3 existente em vez disso, o bucket deverá estar na região principal que você especificou no primeiro épico.	DevOps
Especifique a chave de criptografia.	Mantenha a opção padrão, Chave gerenciada pela AWS padrão, ou opte por usar sua própria chave gerenciada pelo cliente do AWS Key	DevOps

Tarefa	Descrição	Habilidades necessárias
	Management Service (AWS KMS).	
Especificar o provedor de origem.	Em Provedor de origem, escolha AWS CodeCommit.	DevOps
Especificar o repositório.	Escolha o CodeCommit repositório que você criou no primeiro épico. Se você inseriu o código em uma ramificação, escolha a ramificação.	DevOps
Especifique como as alteraçõe s no código são detectadas.	Mantenha o padrão, Amazon CloudWatch Events, como o gatilho de mudança CodeCommit para iniciar o CodePipeline trabalho.	DevOps

Fase de compilação: configurar o pipeline

Tarefa	Descrição	Habilidades necessárias
Especifique o provedor de compilação.	Para o provedor de compilaçã o, escolha AWS CodeBuild.	DevOps
Especifique a região da AWS.	Escolha a região principal, que você especificou no primeiro épico.	DevOps

Fase de compilação: criar e configurar o projeto

Tarefa	Descrição	Habilidades necessárias
Criar o projeto	Escolha Criar projeto e insira um nome para o projeto.	DevOps

Tarefa	Descrição	Habilidades necessárias
Especifique a imagem do ambiente.	Para essa demonstração de padrão, use a imagem CodeBuild gerenciada padrão. Também há a opção de usar uma imagem do Docker personalizada, se tiver uma.	DevOps
Especifique o sistema operacional.	Escolha Amazon Linux 2 ou Ubuntu. **Note** O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs.	DevOps
Especifique o perfil de serviço.	Escolha a função para a qual você criou CodeBuild antes de começar a criar a CodePipel ine tarefa. (Consulte a seção Pré-requisitos.)	DevOps
Configure opções adicionais.	Para Tempo limite e Tempo limite em fila, mantenha os valores padrão. Para ter um certificado, mantenha a configuração padrão, a menos que você tenha um certifica do personalizado que queira usar.	DevOps

Tarefa	Descrição	Habilidades necessárias
Crie as variáveis de ambiente.	Para cada região da AWS na qual você deseja implantar , crie variáveis de ambiente fornecendo o nome do bucket do S3 e o nome da região (por exemplo, us-east-1).	DevOps
Forneça o nome do arquivo buildspec, se não for buildspec.yml.	Mantenha esse campo em branco se o nome do arquivo for o padrão, `buildspec .yaml` . Se você renomeou o arquivo buildspec, insira o nome aqui. Verifique se ele corresponde ao nome do arquivo que está no CodeCommit repositório.	DevOps
Especifique o registro.	Para ver os registros do Amazon CloudWatch Events, mantenha a configuração padrão. ou você pode definir qualquer nome específico de grupo ou registrador.	DevOps

Ignore a fase de Implantação

Tarefa	Descrição	Habilidades necessárias
Pule a fase de implantação e conclua a criação do pipeline.	Quando você configura o pipeline, CodePipeline permite criar apenas um estágio na fase de implantação. Para implantar em várias regiões da AWS, pule esta fase. Depois	DevOps

Tarefa	Descrição	Habilidades necessárias
	que o pipeline for criado, você poderá adicionar vários estágios da fase de Implantação.	

Fase de Implantação: configurar o pipeline para implantação na primeira região

Tarefa	Descrição	Habilidades necessárias
Adicione um estágio à fase de Implantação.	Edite o pipeline e escolha Adicionar estágio na fase de Implantação. Essa primeira etapa é para a região principal.	DevOps
Forneça um nome de ação para o estágio.	Insira um nome exclusivo que reflita o primeiro estágio (principal) e a região. Por exemplo, insira primary_<region>_deploy.	DevOps
Especificar o provedor de ação.	Para o provedor Action, escolha AWS CloudFormation.	DevOps
Configure a região para o primeiro estágio.	Escolha a primeira região (primária), a mesma região em que CodePipeline CodeBuild estão configurados. Essa é a região principal na qual você deseja implantar a pilha.	DevOps
Especifique o artefato de entrada.	Selecione BuildArtifact. Esse é o resultado da fase de compilação.	DevOps

Tarefa	Descrição	Habilidades necessárias
Especifique a ação a ser tomada.	Para o Modo de ação, escolha Criar ou atualizar uma pilha.	DevOps
Insira um nome para a CloudFormation pilha.		DevOps
Especifique o modelo para a primeira região.	Selecione o nome do pacote específico da região que foi empacotado CodeBuild e despejado no bucket do S3 para a primeira região (primária).	DevOps
Especifique os recursos.	Os recursos são necessários se o modelo de pilha incluir recursos do IAM ou se você criar uma pilha diretamente de um modelo que contém macros. Para esse padrão, use CAPABILITY_IAM, CAPABILITY_NAMED_IAM, CAPABILITY_AUTO_EX PAND.	DevOps

Fase de implantação: configurar o pipeline para implantação na segunda região

Tarefa	Descrição	Habilidades necessárias
Adicione o segundo estágio à fase de Implantação.	Para adicionar um estágio para a segunda região, edite o pipeline e escolha Adicionar estágio na fase de Implantaç ão. Importante: o processo de criação da segunda região é	DevOps

Tarefa	Descrição	Habilidades necessárias
	o mesmo da primeira região, exceto pelos valores a seguir.	
Forneça um nome de ação para o segundo estágio.	Insira um nome exclusivo que reflita o segundo estágio e a segunda região.	DevOps
Configure a região para o segundo estágio.	Selecione a segunda região onde você deseja implantar a pilha.	DevOps
Especifique o modelo para a segunda região.	Selecione o nome do pacote específico da região que foi empacotado CodeBuild e despejado no bucket do S3 para a segunda região.	DevOps

Fase de Implantação: configurar o pipeline para implantação na terceira região

Tarefa	Descrição	Habilidades necessárias
Adicione o terceiro estágio à fase de Implantação.	Para adicionar um estágio para a terceira região, edite o pipeline e escolha Adicionar estágio na fase de Implantação. Importante: o processo de criação da segunda região é o mesmo das duas regiões anteriores, exceto pelos valores a seguir.	DevOps
Forneça um nome de ação para o terceiro estágio.	Insira um nome exclusivo que reflita o terceiro estágio e a terceira região.	DevOps

Tarefa	Descrição	Habilidades necessárias
Configure a região para o terceiro estágio.	Selecione a região onde você deseja implantar a pilha.	DevOps
Especifique o modelo para a terceira região.	Selecione o nome do pacote específico da região que foi empacotado CodeBuild e despejado no bucket do S3 para a terceira região.	DevOps

Limpar a implantação

Tarefa	Descrição	Habilidades necessárias
Excluir os recursos da AWS.	Para limpar a implantação, exclua as CloudFormation pilhas em cada região. Em seguida CodeCommit CodeBuild, exclua CodePipeline os recursos, e da região primária.	DevOps

Recursos relacionados

- O que é a AWS CodePipeline?
- Modelo de aplicativo sem servidor da AWS
- AWS CloudFormation
- Referência de estrutura de CloudFormation arquitetura da AWS para AWS CodePipeline

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Execute consultas SQL do Amazon Redshift usando o Terraform

Criado por Sylvia Qi (AWS) e Aditya Ambati (AWS)

Resumo

Usar a infraestrutura como código (IaC) para a implantação e o gerenciamento do Amazon Redshift é uma prática predominante na empresa. DevOps O IaC facilita a implantação e a configuração de vários recursos do Amazon Redshift, como clusters, snapshots e grupos de parâmetros. No entanto, o IaC não se estende ao gerenciamento de recursos de banco de dados, como tabelas, esquemas, visualizações e procedimentos armazenados. Esses elementos do banco de dados são gerenciados por meio de consultas SQL e não são diretamente suportados pelas ferramentas do IaC. Embora existam soluções e ferramentas para gerenciar esses recursos, talvez você prefira não introduzir ferramentas adicionais em sua pilha de tecnologia.

Esse padrão descreve uma metodologia que usa o Terraform para implantar recursos de banco de dados do Amazon Redshift, incluindo tabelas, esquemas, visualizações e procedimentos armazenados. O padrão distingue entre dois tipos de consultas SQL:

- Consultas não repetíveis — Essas consultas são executadas uma vez durante a implantação inicial do Amazon Redshift para estabelecer os componentes essenciais do banco de dados.
- Consultas repetíveis — Essas consultas são imutáveis e podem ser executadas novamente sem afetar o banco de dados. A solução usa o Terraform para monitorar alterações em consultas repetíveis e aplicá-las adequadamente.

Para obter mais detalhes, consulte Passo a passo da solução em Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

Você deve ter um ativo Conta da AWS e instalar o seguinte em sua máquina de implantação:

- AWS Command Line Interface (AWS CLI)
- Um AWS CLI perfil configurado com permissões de leitura/gravação do Amazon Redshift
- Terraform versão 1.6.2 ou posterior
- Python 3

- Boto3

Limitações

- Essa solução oferece suporte a um único banco de dados Amazon Redshift porque o Terraform só permite a criação de um banco de dados durante a criação do cluster.
- Esse padrão não inclui testes para validar as alterações nas consultas repetíveis antes de aplicá-las. Recomendamos que você incorpore esses testes para aumentar a confiabilidade.
- Para ilustrar a solução, esse padrão fornece um arquivo de amostra que usa um `redshift.tf` arquivo de estado local do Terraform. No entanto, para ambientes de produção, é altamente recomendável que você empregue um arquivo de estado remoto com um mecanismo de bloqueio para melhorar a estabilidade e a colaboração.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

Essa solução foi desenvolvida e testada no patch 179 do Amazon Redshift.

Repositório de código

O código desse padrão está disponível no repositório GitHub amazon-redshift-sql-deploy-terraform.

Arquitetura

O diagrama a seguir ilustra como o Terraform gerencia os recursos do banco de dados do Amazon Redshift ao lidar com consultas SQL irrepetíveis e repetíveis.

O diagrama mostra as seguintes etapas:

1. O Terraform aplica consultas SQL não repetíveis durante a implantação inicial do cluster Amazon Redshift.
2. O desenvolvedor confirma as alterações nas consultas SQL repetíveis.
3. O Terraform monitora as mudanças nas consultas SQL repetíveis.
4. O Terraform aplica consultas SQL repetíveis ao banco de dados do Amazon Redshift.

A solução fornecida por esse padrão é criada com base no módulo Terraform para o Amazon Redshift. O módulo Terraform provisiona um cluster e um banco de dados do Amazon Redshift. Para aprimorar o módulo, usamos `terraform_data` recursos, que invocam um script Python personalizado para executar consultas SQL usando a operação de API do Amazon Redshift. ExecuteStatement Como resultado, o módulo pode fazer o seguinte:

- Implante qualquer número de recursos de banco de dados usando consultas SQL após o provisionamento do banco de dados.
- Monitore continuamente as alterações nas consultas SQL repetíveis e aplique essas alterações usando o Terraform.

Para obter mais detalhes, consulte Passo a passo da solução em Informações adicionais.

Ferramentas

Serviços da AWS

- O Amazon Redshift é um serviço de armazém de dados totalmente gerenciado em escala de petabytes no. Nuvem AWS

Outras ferramentas

- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.
- Python é uma linguagem de programação de uso geral usada nesse padrão para executar consultas SQL.

Práticas recomendadas

- Melhores práticas do Amazon Redshift
- Usando a API de dados do Amazon Redshift para interagir com clusters do Amazon Redshift

Épicos

Implemente a solução usando o Terraform

Tarefa	Descrição	Habilidades necessárias
Clone o repositório.	Para clonar o repositório Git contendo o código do Terraform para provisionar um cluster do Amazon Redshift, use o comando a seguir. `git clone https://github.com/aws-samples/amazon-redshift-sql-deploy-terraform.git`	DevOps engenheiro

Atualize as variáveis do Terraform.	Para personalizar a implantação do cluster do Amazon Redshift de acordo com seus requisitos específicos, atualize os seguintes parâmetros no `terraform.tfvars` arquivo.
	`region = "<AWS_REGION>"`
	`cluster_identifier = "<REDSHIFT_CLUSTER_IDENTIFIER>"`
	`node_type = "<REDSHIFT_NODE_TYPE>"`
	`number_of_nodes = "<REDSHIFT_NODE_COUNT>"`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	database_name = "<REDSHIFT_DB_NAME>" subnet_ids = "<REDSHIFT_SUBNET_IDS>" vpc_security_group_ids = "<REDSHIFT_SECURITY_GROUP_IDS>" run_nonrepeatable_queries = true run_repeatable_queries = true sql_path_bootstrap = "<BOOTSTRAP_SQLS_PATH>" sql_path_nonrepeatable = "<NON-REPEATABLE_SQLS_PATH>" sql_path_repeatable = "<REPEATABLE_SQLS_PATH>" sql_path_finalize = "<FINALIZE_SQLS_PATH>" create_random_password = false master_username = "<REDSHIFT_MASTER_USERNAME>"	

Tarefa	Descrição	Habilidades necessárias

Implante os recursos usando o Terraform.	1. Para se preparar para o processo de implantação, use o comando a seguir para inicializar o Terraform dentro do repositório clonado.
	`terraform init`
	2. Para visualizar as alterações que o Terraform aplicará à infraestrutura, use o comando a seguir para criar um plano de execução.
	`terraform plan -var-file terraform.tfvars`
	3. Para provisionar o cluster do Amazon Redshift e os recursos associados, use o comando a seguir para aplicar o plano de execução do Terraform.
	`terraform apply -var-file terraform.tfvars`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

(Opcional) Execute consultas SQL adicionais.	O repositório de amostra fornece várias consultas SQL para fins de demonstração. Para executar suas próprias consultas SQL, adicione-as às seguintes pastas:
	`/bootstrap`
	`/nonrepeatable`
	`/repeatable`
	`/finalize`	

Monitore a execução de instruções SQL

Tarefa	Descrição	Habilidades necessárias
Monitore a implantação de instruções SQL.	Você pode monitorar os resultados das execuções de SQL em um cluster do Amazon Redshift. Para obter exemplos de saídas que mostram uma falha e uma execução bem-sucedida de SQL, consulte Exemplos de instruções SQL em Informações adicionais.	DBA, engenheiro DevOps
Limpar recursos.	Para excluir todos os recursos implantados pelo Terraform, execute o comando a seguir. `terraform destroy`	DevOps engenheiro

Valide os resultados

Tarefa	Descrição	Habilidades necessárias
Valide os dados no cluster do Amazon Redshift.	1. Faça login no AWS Management Console e abra o console do Amazon Redshift. 2. No menu de navegação, escolha Clusters. Escolha o nome do cluster relevante na lista. 3. Siga as instruções em Consultar um banco de dados usando o editor de consultas v2 do Amazon Redshift na documentação do Amazon Redshift.	DBA, AWS DevOps

Recursos relacionados

AWS documentação

- Clusters provisionados pelo Amazon Redshift
- Solução de problemas com a API de dados do Amazon Redshift

Outros recursos

- Comando: aplicar (documentação do Terraform)

Mais informações

Passo a passo da solução

Para usar a solução, você deve organizar suas consultas SQL do Amazon Redshift de uma forma específica. Todas as consultas SQL devem ser armazenadas em arquivos com uma `.sql` extensão.

No exemplo de código fornecido com esse padrão, as consultas SQL são organizadas na estrutura de pastas a seguir. Você pode modificar o código (`sql-queries.tfesql-queries.py`) para trabalhar com qualquer estrutura que se ajuste ao seu caso de uso exclusivo.

```
/bootstrap
     |- Any # of files
     |- Any # of sub-folders
/nonrepeatable
     |- Any # of files
     |- Any # of sub-folders
/repeatable
     /udf
          |- Any # of files
          |- Any # of sub-folders
     /table
          |- Any # of files
          |- Any # of sub-folders
     /view
          |- Any # of files
          |- Any # of sub-folders
     /stored-procedure
          |- Any # of files
          |- Any # of sub-folders
/finalize
     |- Any # of files
     |- Any # of sub-folders
```

Dada a estrutura de pastas anterior, durante a implantação do cluster Amazon Redshift, o Terraform executa as consultas na seguinte ordem:

1. `/bootstrap`
2. `/nonrepeatable`
3. `/repeatable`
4. `/finalize`

A `/repeatable` pasta contém quatro subpastas: `/udf/table`,`/view`, e. `/stored-procedure` Essas subpastas indicam a ordem na qual o Terraform executa as consultas SQL.

O script Python que executa as consultas SQL é. `sql-queries.py` Primeiro, o script lê todos os arquivos e subpastas de um diretório de origem específico, por exemplo, o `sql_path_bootstrap`

parâmetro. Em seguida, o script executa as consultas chamando a operação da API do Amazon ExecuteStatementRedshift. Você pode ter uma ou mais consultas SQL em um arquivo. O trecho de código a seguir mostra a função Python que executa instruções SQL armazenadas em um arquivo em um cluster do Amazon Redshift.

```
def execute_sql_statement(filename, cluster_id, db_name, secret_arn, aws_region):
    """Execute SQL statements in a file"""
    redshift_client = boto3.client(
        'redshift-data', region_name=aws_region)
    contents = get_contents_from_file(filename),
    response = redshift_client.execute_statement(
        Sql=contents[0],
        ClusterIdentifier=cluster_id,
        Database=db_name,
        WithEvent=True,
        StatementName=filename,
        SecretArn=secret_arn
    )
    ...
```

O script Terraform `sql-queries.tf` cria os recursos terraform_data que invocam o script. `sql-queries.py` Há um `terraform_data` recurso para cada uma das quatro pastas: `/bootstrap` `/nonrepeatable/repeatable`,, `/finalize` e. O trecho de código a seguir mostra o `terraform_data` recurso que executa as consultas SQL na pasta. `/bootstrap`

```
locals {
  program               = "${path.module}/sql-queries.py"
  redshift_cluster_name = try(aws_redshift_cluster.this[0].id, null)
}

resource "terraform_data" "run_bootstrap_queries" {
  count      = var.create && var.run_nonrepeatable_queries && (var.sql_path_bootstrap !
= "") && (var.snapshot_identifier == null) ? 1 : 0
  depends_on = [aws_redshift_cluster.this[0]]

  provisioner "local-exec" {
    command = "python3 ${local.program} ${var.sql_path_bootstrap}
 ${local.redshift_cluster_name} ${var.database_name} ${var.redshift_secret_arn}
 ${local.aws_region}"
  }
}
```

Você pode controlar se essas consultas devem ser executadas usando as variáveis a seguir. Se você não quiser executar consultas em`sql_path_bootstrap`,,, ou `sql_path_nonrepeatable` `sql_path_repeatable``sql_path_finalize`, defina `""` seus valores como.

```
  run_nonrepeatable_queries = true
  run_repeatable_queries    = true
  sql_path_bootstrap        = "src/redshift/bootstrap"
  sql_path_nonrepeatable    = "src/redshift/nonrepeatable"
  sql_path_repeatable       = "src/redshift/repeatable"
  sql_path_finalize         = "src/redshift/finalize"
```

Quando você executa`terraform apply`, o Terraform considera o `terraform_data` recurso adicionado após a conclusão do script, independentemente dos resultados do script. Se algumas consultas SQL falharem e você quiser executá-las novamente, você pode remover manualmente o recurso do estado do Terraform e executá-las novamente. `terraform apply` Por exemplo, o comando a seguir remove o `run_bootstrap_queries` recurso do estado do Terraform.

```
terraform state rm module.redshift.terraform_data.run_bootstrap_queries[0]
```

O exemplo de código a seguir mostra como o `run_repeatable_queries` recurso monitora as alterações na `repeatable` pasta usando o hash sha256. Se algum arquivo dentro da pasta for atualizado, o Terraform marcará o diretório inteiro para uma atualização. Em seguida, o Terraform executa as consultas no diretório novamente durante a próxima. `terraform apply`

```
resource "terraform_data" "run_repeatable_queries" {
  count      = var.create_redshift && var.run_repeatable_queries &&
 (var.sql_path_repeatable != "") ? 1 : 0
  depends_on = [terraform_data.run_nonrepeatable_queries]

  # Continuously monitor and apply changes in the repeatable folder
  triggers_replace = {
    dir_sha256 = sha256(join("", [for f in fileset("${var.sql_path_repeatable}",
 "**") : filesha256("${var.sql_path_repeatable}/${f}")]))
  }

  provisioner "local-exec" {
    command = "python3 ${local.sql_queries} ${var.sql_path_repeatable}
 ${local.redshift_cluster_name} ${var.database_name} ${var.redshift_secret_arn}"
  }
}
```

Para refinar o código, você pode implementar um mecanismo para detectar e aplicar alterações somente aos arquivos que foram atualizados na `repeatable` pasta, em vez de aplicar as alterações a todos os arquivos indiscriminadamente.

Exemplos de instruções SQL

A saída a seguir mostra uma falha na execução do SQL, junto com uma mensagem de erro.

```
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Executing:
 ["/bin/sh" "-c" "python3 modules/redshift/sql-queries.py src/redshift/nonrepeatable
 testcluster-1 db1 arn:aws:secretsmanager:us-east-1:XXXXXXXXXXXX:secret:/redshift/
master_user/password-8RapGH us-east-1"]
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): src/redshift/
nonrepeatable/table/admin/admin.application_family.sql
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Status:
 FAILED
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): SQL execution
 failed.
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Error
 message: ERROR: syntax error at or near ")"
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):   Position:
 244
module.redshift.terraform_data.run_nonrepeatable_queries[0]: Creation complete after 3s
 [id=ee50ba6c-11ae-5b64-7e2f-86fd8caa8b76]
```

A saída a seguir mostra uma execução bem-sucedida do SQL.

```
module.redshift.terraform_data.run_bootstrap_queries[0]: Provisioning with 'local-
exec'...
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): Executing:
 ["/bin/sh" "-c" "python3 modules/redshift/sql-queries.py src/redshift/bootstrap
 testcluster-1 db1 arn:aws:secretsmanager:us-east-1:XXXXXXXXXXXX:secret:/redshift/
master_user/password-8RapGH us-east-1"]
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): src/redshift/
bootstrap/db.sql
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec):
 ----------------------------------------------------------------
```

```
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): Status: FINISHED
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): SQL execution
 successful.
module.redshift.terraform_data.run_bootstrap_queries[0]: Creation complete after 2s
 [id=d565ef6d-be86-8afd-8e90-111e5ea4a1be]
```

Exporte relatórios do AWS Backup de toda a organização no AWS Organizations como um arquivo CSV

Criado por Aromal Raj Jayarajan (AWS) e Purushotham G K (AWS)

Resumo

Esse padrão mostra como exportar relatórios de trabalho do AWS Backup de toda a organização para o AWS Organizations como um arquivo CSV. A solução usa o AWS Lambda e EventBridge a Amazon para categorizar os relatórios de trabalho do AWS Backup com base em seu status, o que pode ajudar na configuração de automações baseadas em status.

O AWS Backup ajuda organizações a gerenciar e automatizar centralmente a proteção de dados nos serviços da AWS, na nuvem e em ambientes on-premises. No entanto, para trabalhos do AWS Backup configurados dentro do AWS Organizations, os relatórios consolidados estão disponíveis somente no Console de Gerenciamento da AWS da conta de gerenciamento de cada organização. Trazer esses relatórios para fora da conta de gerenciamento pode reduzir o esforço necessário para a auditoria e aumentar o escopo de automações, notificações e alertas.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma organização ativa no AWS Organizations que inclui pelo menos uma conta de gerenciamento e uma conta de membro
- AWS Backup configurado no nível da organização no AWS Organizations (para obter mais informações, consulte Automatizar o backup centralizado em grande escala em todos os serviços da AWS usando o AWS Backup no blog da AWS)
- O Git instalado e configurado em sua máquina local

Limitações

A solução fornecida nesse padrão identifica os recursos da AWS que estão configurados somente para trabalhos do AWS Backup. O relatório não consegue identificar recursos da AWS que não estão configurados para backup por meio do AWS Backup.

Arquitetura

Pilha de tecnologias de destino

- AWS Backup
- AWS CloudFormation
- Amazon EventBridge
- AWS Lambda
- AWS Security Token Service (AWS STS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Identity and Access Management (IAM)

Arquitetura de destino

O diagrama a seguir mostra um exemplo de fluxo de trabalho para exportar relatórios de trabalho do AWS Backup de toda a organização para o AWS Organizations como um arquivo CSV.

O diagrama mostra o seguinte fluxo de trabalho:

1. Uma regra de EventBridge evento programado invoca uma função Lambda na conta membro (de relatórios) da AWS.
2. A função do Lambda então usa o AWS STS para presumir um perfil do IAM que tem as permissões necessárias para se conectar à conta de gerenciamento.
3. A função do Lambda faz o seguinte:
   - Solicita o relatório consolidado de trabalhos do AWS Backup para o serviço AWS Backup
   - Categoriza os resultados com base no status do trabalho do AWS Backup
   - Converte a resposta em um arquivo CSV
   - Carrega os resultados em um bucket do Amazon S3 na conta de relatórios dentro de pastas que são rotuladas com base na data de criação

Ferramentas

Ferramentas

- O AWS Backup é um serviço totalmente gerenciado que ajuda você a centralizar e automatizar a proteção de dados nos serviços da AWS, na nuvem e em ambientes on-premises.
- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, funções do Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras contas da AWS.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Código

O código desse padrão está disponível no GitHub aws-backup-report-generatorrepositório.

Práticas recomendadas

- Práticas recomendadas de segurança para o Amazon S3 (Guia do usuário do Amazon S3)
- Práticas recomendadas para trabalhar com funções do AWS Lambda (Guia do desenvolvedor do AWS Lambda)
- Práticas recomendadas para a conta de gerenciamento (Guia do usuário do AWS Organizations)

Épicos

Implante os componentes da solução

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Clone o GitHub aws-backup-report-generatorrepositório executando o seguinte comando em uma janela de terminal: `git clone https://github.com/aws-samples/aws-backup-report-generator.git` Para obter mais informações, consulte Clonar um repositório no GitHub Docs.	AWS DevOps, DevOps engenheiro
Implante os componentes da solução na conta membro (de relatórios) da AWS.	1. Na conta do membro (de relatórios), faça login no AWS Management Console e, em seguida, abra o CloudFormation console. 2. Selecione Criar pilha e, depois, Com novos recursos (padrão). 3. Na página Criar pilha, na seção Especificar modelo, selecione Fazer upload de um arquivo de modelo. 4. Selecione Escolher arquivo. Em seguida, navegue até a pasta raiz do GitHub repositório clonado em sua	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	estação de trabalho local e escolha template-reporting .yaml. 5. Selecione Abrir e, em seguida, escolha Próximo. 6. Na página Especificar detalhes da pilha, em Nome da pilha, insira um nome para sua CloudFormation pilha. 7. Para ManagementAccountID, insira o ID da conta da AWS para a conta de gerenciamento da sua organização no AWS Organizations. 8. Escolha Avançar. 9. Na página Configurar opções de pilha, selecione Próximo. 10. Na página Revisar, marque a caixa de seleção para confirmar que você revisou a configuração. 11. Selecione Criar pilha. A pilha mostra o status CREATE_COMPLETE quando os componentes da solução são implantados na conta membro (de relatórios).	

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Certifique-se de que a EventBridge regra seja executada antes do teste.	Certifique-se de que a EventBridge regra seja executada aguardando pelo menos 24 horas ou aumentando a frequênci a do relatório no arquivo CloudFormation template-reporting.yml do modelo. Como aumentar a frequência do relatório 1. Abra o arquivo template-reporting.yml no repositório clonado. 2. Na regra do evento com o ID lógico 'LambdaSc hedule', encontre o 'ScheduleExpression'. 3. Edite a tecla ScheduleE xpression'' para que ela inclua uma expressão cron válida. Por exemplo, esta expressão cron programa a execução da regra de evento a cada cinco minutos: “`cron (* /5 * * * *)`”	AWS DevOps, DevOps engenheiro
Verifique o bucket do Amazon S3 para ver o relatório gerado.	1. Na conta do membro (de relatórios), faça login no AWS Management Console	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	e, em seguida, abra o CloudFormation console. 2. No painel Pilhas, selecione o nome da pilha que você criou. Então, selecione a guia Resources (Recursos). 3. No painel Recursos, na coluna ID lógica, localize BackupReportS3Buck et. Em seguida, abra o bucket do Amazon S3 associado em uma nova guia selecionando o link na coluna ID físico ao lado desse ID lógico. 4. Certifique-se de que o bucket contenha um relatório gerado no seguinte formato: BackupReports//// BackupReport- - - - .csv <yyyy><mm><dd><BAC KUP JOB STATUS><d d><Mon><yyyy>	

Limpe os seus recursos

Tarefa	Descrição	Habilidades necessárias
Exclua os componentes da solução da conta membro (de relatórios).	1. Na conta membro (de relatórios), abra o bucket do Amazon S3 da solução. Para obter instruções, consulte as etapas 2 a 4 na seção Verificar o bucket	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	do S3 para ver o relatório gerado na seção Testar a solução desse padrão. 2. Exclua o conteúdo do bucket e esvazie-o. Para obter instruções, consulte Esvaziar um bucket no Guia do usuário do Amazon S3. 3. Na conta do membro (de relatórios), faça login no AWS Management Console e, em seguida, abra o CloudFormation console. 4. No painel Pilhas, marque a caixa de seleção ao lado do nome da pilha que você criou. Em seguida, selecione Excluir.	
Exclua os componentes da solução da conta de gerenciamento.	1. Na conta de gerenciamento, faça login no AWS Management Console e, em seguida, abra o CloudFormation console. 2. No painel Pilhas, marque a caixa de seleção ao lado do nome da pilha que você criou. Em seguida, selecione Excluir.	AWS DevOps, DevOps engenheiro

Recursos relacionados

- Tutorial: Usando o AWS Lambda com eventos programados (documentação do AWS Lambda)

- Criação de eventos programados para executar funções do AWS Lambda (SDK da AWS para documentação) JavaScript
- Tutorial do IAM: delegue o acesso em todas as contas da AWS usando funções do IAM (documentação do IAM)
- Terminologia e conceitos do AWS Organizations (documentação do AWS Organizations)
- Criação de planos de relatórios usando o console do AWS Backup (documentação do AWS Backup)
- Crie um relatório de auditoria (documentação do AWS Backup)
- Criação de relatórios sob demanda (documentação do AWS Backup)
- O que é o AWS Backup? (Documentação do AWS Backup)
- Automatize o backup centralizado em grande escala em todos os serviços da AWS usando o AWS Backup (publicação no blog da AWS)

Exportar tags de uma lista de EC2 instâncias da Amazon para um arquivo CSV

Criado por Sida Ju (AWS) e Pac Joonhyun (AWS)

Resumo

Esse padrão mostra como exportar programaticamente tags de uma lista de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) para um arquivo CSV.

Ao usar o script Python de exemplo fornecido, você pode reduzir o tempo necessário para revisar e categorizar suas EC2 instâncias da Amazon por tags específicas. Por exemplo, você pode usar o script para identificar e categorizar rapidamente uma lista de instâncias que sua equipe de segurança sinalizou para atualizações de software.

Pré-requisitos e limitações

Pré-requisitos

- Python 3 instalado e configurado
- AWS Command Line Interface (AWS CLI) instalado e configurado

Limitações

O exemplo de script Python fornecido nesse padrão pode pesquisar EC2 instâncias da Amazon com base somente nos seguintes atributos:

- Instância IDs
- IPv4 Endereços privados
- IPv4 Endereços públicos

Ferramentas

- O Python é uma linguagem de programação de computador de uso geral.
- O virtualenv ajuda você a criar ambientes do Python isolados.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

Repositório de código

O script Python de exemplo para esse padrão está disponível no repositório GitHub search-ec2 -. instances-export-tags

Épicos

Instalar e configurar os pré-requisitos

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	**Note** Se você receber erros ao executar comandos da AWS CLI, verifique se está usando a versão mais recente da AWS CLI. Clone o instances-export-tags repositório GitHub search-ec2- executando o seguinte comando Git em uma janela de terminal: `git clone https://github.com/aws-samples/search-ec2-instances-export-tags.git`	DevOps engenheiro
Instale e ative o virtualenv.	1. Instale o virtualenv executando o seguinte comando:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`python3 -m pip install virtualenv`
	2. Crie um novo ambiente virtual executando o comando a seguir:
	`python3 -m venv env`
	3. Ative o novo ambiente virtual executando o seguinte comando:
	`source env/bin/activate`
	Para obter mais informações, consulte o Guia do usuário do virtualenv.	

Instale as dependências.	1. Abra o diretório de código executando o seguinte comando no terminal:
	`cd search-ec2-instances-export-tags`
	2. Instale o arquivo `requirements.txt` executando o seguinte comando pip:
	`pip3 install -r requirements.txt`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Configure um perfil nomeado da AWS.	Se ainda não o fez, configure um perfil nomeado da AWS que inclua as credenciais necessárias para executar o script. Para criar um perfil nomeado, execute o comando configurar a AWS. Para obter mais informaçõ es, consulte Uso de perfis nomeados na documentação da AWS CLI.	DevOps engenheiro

Configure e execute o script do Python

Tarefa	Descrição	Habilidades necessárias
Crie o arquivo de entrada.	Crie um arquivo de entrada que contenha uma lista das EC2 instâncias da Amazon para as quais você deseja que o script pesquise e exporte tags. Você pode listar instâncias IDs, IPv4 endereços privados ou IPv4 endereços públicos. **Important** Certifique-se de que cada EC2 instância da Amazon esteja listada em sua própria linha no arquivo de entrada.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	Exemplo de arquivo de entrada
	
	`1 i-0547c351bdfe85b9f`
	`2 54.157.194.156`
	`3 172.31.85.33`
	`4 54.165.198.144`
	`5 i-0b6223b5914111a4b`
	`6 172.31.85.44`
	`7 54.165.198.145`
	`8 172.31.80.219`
	`9 172.31.94.199`	

Tarefa	Descrição	Habilidades necessárias
Execute o script do Python.	Execute o script executando o comando a seguir no terminal: `python search_instances.py -i INPUTFILE -o OUTPUTFILE -r REGION [-p PROFILE]` **Note** `INPUTFILE` Substitua pelo nome do seu arquivo de entrada. Substitua `OUTPUTFILE` pelo nome que você deseja dar ao arquivo de saída CSV. `REGION`Substitua pela região da AWS em que seus EC2 recursos da Amazon estão. Se você estiver usando um perfil nomeado da AWS, substitua `PROFILE` pelo perfil nomeado que você está usando. Para obter uma lista com os parâmetros compatíveis e a descrição deles, execute o comando a seguir:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`python search_instances.py -h` Para obter mais informações e ver um exemplo de arquivo de saída, consulte o `README.md` arquivo no repositório GitHub search-ec2-instances-export-tags.	

Recursos relacionados

- Configuração da AWS CLI (Guia do usuário da AWS CLI)

Gere um CloudFormation modelo da AWS contendo regras gerenciadas do AWS Config usando o Troposphere

Criado por Lucas Nation (AWS) e Freddie Wilson (AWS)

Resumo

Muitas organizações usam regras gerenciadas do AWS Config para avaliar a conformidade de seus recursos da Amazon Web Services (AWS) em relação às melhores práticas em geral. No entanto, a manutenção dessas regras pode ser demorada e esse padrão ajuda você a aproveitar a Troposphere, uma biblioteca Python, para gerar e gerenciar regras gerenciadas do AWS Config.

O padrão ajuda você a gerenciar suas regras gerenciadas do AWS Config usando um script Python para converter uma planilha do Microsoft Excel contendo regras gerenciadas da AWS em um modelo da AWS. CloudFormation O Troposphere atua como infraestrutura como código (IaC) e isso significa que você pode atualizar a planilha do Excel com regras gerenciadas, em vez de usar um arquivo no formato JSON ou YAML. Em seguida, você usa o modelo para iniciar uma CloudFormation pilha da AWS que cria e atualiza as regras gerenciadas na sua conta da AWS.

O CloudFormation modelo da AWS define cada regra gerenciada do AWS Config usando a planilha do Excel e ajuda você a evitar a criação manual de regras individuais no AWS Management Console. O script padroniza os parâmetros de cada regra gerenciada para um dicionário vazio e os `ComplianceResourceTypes` padrões do escopo são de. `THE_RULE_IDENTIFIER.template file` Para obter mais informações sobre o identificador da regra, consulte Criação de regras gerenciadas do AWS Config com CloudFormation modelos da AWS na documentação do AWS Config.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Familiaridade com o uso de CloudFormation modelos da AWS para criar regras gerenciadas do AWS Config. Para obter mais informações sobre isso, consulte Criação de regras gerenciadas do AWS Config com CloudFormation modelos da AWS na documentação do AWS Config.
- Python 3 instalado e configurado. Para obter mais informações sobre isso, consulte a documentação do Python.
- Um ambiente de desenvolvimento integrado (IDE) existente.

- Identifique suas unidades organizacionais (OUs) em uma coluna na amostra de planilha `excel_config_rules.xlsx` do Excel (anexada).

Épicos

Personalize e configure as regras gerenciadas do AWS Config

Tarefa	Descrição	Habilidades necessárias
Atualize o exemplo da planilha do Excel.	Faça o download do exemplo da planilha `excel_config_rules.xlsx` do Excel (anexada) e identifique como as regras gerenciadas as `Implemented` do AWS Config que você deseja usar. As regras marcadas como `Implemented` serão adicionadas ao CloudFormation modelo da AWS.	Desenvolvedor
(Opcional) Atualize o arquivo config_rules_params.json com os parâmetros de regra do AWS Config.	Algumas regras gerenciadas do AWS Config exigem parâmetros e devem ser passadas para o script Python como um arquivo JSON usando a opção `--param-file`. Por exemplo, a regra `access-keys-rotated` gerenciada usa o seguinte parâmetro `maxAccessKeyAge`: `{ "access-keys-rotated": {`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias

	<pre>"InputPar
	ameters": {
	
	"maxAccessKeyAge": 90
	}
	}
	}</pre>
	Neste parâmetro de exemplo, o `maxAccessKeyAge` é definido para 90 dias. O script lê o arquivo de parâmetros e adiciona qualquer `InputParameters` encontrado.	

Tarefa	Descrição	Habilidades necessárias
(Opcional) Atualize o arquivo config_rules_params.json com o AWS Config. ComplianceResourceTypes	Por padrão, o script Python recupera `ComplianceResourceTypes` a partir dos modelos definidos pela AWS. Se você quiser substituir o escopo de uma regra gerenciada específica do AWS Config, precisará passá-la para o script Python como um arquivo JSON usando a opção `--param-file` . Por exemplo, o código de exemplo a seguir mostra como o `ComplianceResourceTypes` para `ec2-volume-inuse-check` é definido na lista `["AWS::EC2::Volume"]` : `{ "ec2-volume-inuse-check": { "Scope": { "ComplianceResourceTypes": [ "AWS::EC2::Volume" ] } } }`	Desenvolvedor

Execute o script do Python

Tarefa	Descrição	Habilidades necessárias
Instale os pacotes pip do arquivo requirements.txt.	Baixe o arquivo `requirements.txt` (anexado) e execute o seguinte comando em seu IDE para instalar os pacotes Python: `pip3 install -r requirements.txt`	Desenvolvedor
Execute o script do Python.	1. Faça download do `aws_config_rules.py` arquivo (anexado) na sua máquina local. 2. **Note** Execute o `- python3 aws_config_rules.py --ou <OU_NAME>` comando.: `--ou` define qual coluna OU escolher na planilha do Excel. Você também pode adicionar os seguintes parâmetros opcionais: • `--config-rule-option` : define as regras para escolher na planilha	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	do Excel. O padrão é o parâmetro `Implemented` . • `--excel-file` : o caminho para a planilha do Excel. O padrão é `aws_config_rules.xlsx` . • `--param-file` : o caminho do arquivo JSON do parâmetro. O padrão é `config_rules_params.json` . • `--max-execution-frequency` : define com que frequência as regras gerenciadas do AWS Config são avaliadas. As opções são `One_Hour`, `Three_Hours` , `Six_Hours` , `Twelve_Hours` , ou `TwentyFour_Hours` . O padrão é `TwentyFour_Hours` .	

Implantar as regras gerenciadas do AWS Config

Tarefa	Descrição	Habilidades necessárias
Inicie o AWS CloudFormation stack.	1. Faça login no AWS Management Console, abra o CloudFormation console da AWS e escolha Create stack.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	2. Na página Especificar modelo, escolha Carregar um arquivo de modelo e, em seguida, carregue seu CloudFormation modelo da AWS. 3. Especifique o nome da pilha e escolha Próximo. 4. Especifique as tags e escolha Avançar. 5. Selecione Criar pilha.	

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Conceda às instâncias do SageMaker notebook acesso temporário a um CodeCommit repositório em outra conta da AWS

Criado por Helge Aufderheide (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão mostra como conceder aos usuários e instâncias de SageMaker notebooks da Amazon acesso temporário a um CodeCommit repositório da AWS que está em outra conta da AWS. Esse padrão também mostra como você pode conceder permissões granulares para ações específicas que cada entidade pode realizar em cada repositório.

As organizações geralmente armazenam CodeCommit repositórios em uma conta da AWS diferente da conta que hospeda seu ambiente de desenvolvimento. Essa configuração de várias contas ajuda a controlar o acesso aos repositórios e reduz o risco de sua exclusão acidental. Para conceder essas permissões entre contas, é uma melhor prática usar perfis do Identity and Access Management (IAM) da AWS. Em seguida, identidades predefinidas do IAM em cada conta da AWS podem assumir temporariamente as funções para criar uma cadeia de confiança controlada em todas as contas.

> **Note**
>
> Você pode aplicar um procedimento semelhante para conceder acesso entre contas a outras identidades do IAM a um CodeCommit repositório. Para obter mais informações, consulte Configurar o acesso entre contas a um CodeCommit repositório da AWS usando funções no Guia CodeCommit do usuário da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da AWS com um CodeCommit repositório (conta A)
- Uma segunda conta ativa da AWS com uma instância de SageMaker notebook (conta B)
- Um usuário da AWS com permissões suficientes para criar e modificar perfis do IAM na conta A
- Um segundo usuário da AWS com permissões suficientes para criar e modificar perfis do IAM na conta B

Arquitetura

O diagrama a seguir mostra um exemplo de fluxo de trabalho para conceder acesso cruzado a um repositório a uma instância de SageMaker notebook e aos usuários em uma CodeCommit conta da AWS:

O diagrama mostra o seguinte fluxo de trabalho:

1. A função de usuário da AWS e a função de instância do SageMaker notebook na conta B assumem um perfil nomeado.
2. A política de permissões do perfil nomeado especifica uma função de CodeCommit acesso na conta A que o perfil então assume.
3. A política de confiança da função de CodeCommit acesso na conta A permite que o perfil nomeado na conta B assuma a função de CodeCommit acesso.
4. A política de permissões do IAM do CodeCommit repositório na conta A permite que a função de CodeCommit acesso acesse o CodeCommit repositório.

Pilha de tecnologia

- CodeCommit
- Git
- IAM
- pip
- SageMaker

Ferramentas

- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O Git é um sistema distribuído de controle de versões para rastrear alterações no código-fonte durante o desenvolvimento do software.

- git-remote-codecommité um utilitário que ajuda você a enviar e extrair código de CodeCommit repositórios estendendo o Git.
- pip é o instalador de pacotes para Python. Você pode usar o pip para instalar pacotes do Python Package Index e outros índices.

Práticas recomendadas

Ao definir permissões com as políticas do IAM, certifique-se de conceder apenas as permissões necessárias para executar uma tarefa. Para obter mais informações, consulte Aplicar permissões de privilégios mínimos na documentação do IAM.

Ao implementar esse padrão, certifique-se de fazer o seguinte:

- Confirme se os princípios do IAM têm somente as permissões necessárias para realizar ações específicas e necessárias em cada repositório. Por exemplo, é recomendável permitir que os princípios aprovados do IAM enviem e mesclem alterações em ramificações específicas do repositório, mas somente solicitem mesclagens em ramificações protegidas.
- Confirme se os princípios do IAM recebem diferentes perfis do IAM com base em suas respectivas funções e responsabilidades em cada projeto. Por exemplo, um desenvolvedor terá permissões de acesso diferentes das de um gerente de lançamento ou administrador da AWS.

Épicos

Configurar o perfil do IAM

Tarefa	Descrição	Habilidades necessárias
Configure a função de CodeCommit acesso e a política de permissões.	**Note** Para automatiz ar o processo de configuração manual documentado neste épico, você pode usar um CloudFormation modelo da AWS.	AWS geral, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Na conta que contém o CodeCommit repositório (conta A), faça o seguinte: 1. Crie uma função do IAM que possa ser assumida pela função de instância do SageMaker notebook na conta B. 2. Crie uma política do IAM que conceda acesso ao repositório e anexe a política à função. Somente para fins de teste, escolha a política gerenciada pela AWSCodeCommitPowerUserAWS. Essa política concede todas CodeCommit as permissões, exceto a capacidade de excluir recursos. 3. Modifique a política de confiança da função para que a conta B seja listada como uma entidade confiável. **Important** Antes de mover essa configuração para seu ambiente de produção, é uma prática recomendada	

Tarefa	Descrição	Habilidades necessárias
	escrever sua própria política de IAM que aplique permissões de privilégios mínimos. Para obter mais informações, consulte a seção Informaçõ es adicionais desse padrão.	

Tarefa	Descrição	Habilidades necessárias
Conceda à função da instância do SageMaker notebook na conta B permissões para assumir a função de CodeCommit acesso na conta A.	Na conta que contém a função IAM da instância do SageMaker notebook (conta B), faça o seguinte: 1. Crie uma política do IAM que permita que uma função ou usuário do IAM assuma a função de CodeCommit acesso na conta A. Exemplo de política de permissões do IAM que permite que um perfil do IAM ou usuário assuma um perfil entre contas `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam:::accountA_ID:role/accountArole_ID" } }` 2. Anexe a política à função da instância do seu	AWS geral, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	SageMaker notebook na conta B. 3. Faça com que a função da instância do SageMaker notebook na conta B assuma a função de CodeCommit acesso na conta A. **Note** Para ver o Amazon Resource Name (ARN) do seu repositório, consulte CodeCommit Exibir detalhes do repositório no Guia do usuário da AWS CodeCommit .	

Configure sua instância do SageMaker notebook na conta B

Tarefa	Descrição	Habilidades necessárias
Configure um perfil de usuário na instância do SageMaker notebook da AWS para assumir a função na conta A.	**Important** Verifique se você tem a versão mais recente da AWS Command Line Interface (AWS CLI) instalada.	AWS geral, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	Na conta que contém a instância do SageMaker notebook (conta B), faça o seguinte:
	
	1. Faça login no Console de Gerenciamento da AWS e abra o console do SageMaker .
	2. Acesse sua instância de SageMaker notebook. A interface do Jupyter será aberta.
	3. Escolha Novo e, em seguida, escolha Terminal. Uma nova janela de terminal é aberta em seu ambiente Jupyter.
	4. Navegue até o arquivo ~/.aws/config da instância do SageMaker notebook. Em seguida, adicione um perfil de usuário ao arquivo inserindo a seguinte declaração:
	
	`------.aws/config-`
	`-------------`
	`[profile remoterep`
	`ouser]`
	`role_arn = arn:aws:i`
	`am::<ID of Account`
	`A>:role/<rolename>`
	`role_session_name =`
	`remoteaccesssession`	

Tarefa	Descrição	Habilidades necessárias

	`region = eu-west-1`
	`credential_source = Ec2InstanceMetadata`
	`----------`
	`----------`	

Instale o git-remote-codecommit utilitário.	Siga as instruções na Etapa 2: Instalação git-remote-codecommit no Guia do CodeCommit usuário da AWS.	Cientista de dados

Acesse o repositório

Tarefa	Descrição	Habilidades necessárias
Acesse o CodeCommit repositório usando os comandos Git ou. SageMaker	Para usar Git Os diretores do IAM que assumem a função da instância do SageMaker notebook na conta B agora podem executar comandos Git para acessar CodeCommit o repositório na conta A. Por exemplo, os usuários podem executar comandos `git clone` como `git pull`, e. `git push` Para obter instruções, consulte Conecte-se a um CodeCommit repositório da AWS no Guia do CodeCommit usuário da AWS.	Git, console bash

Tarefa	Descrição	Habilidades necessárias
	Para obter informaçõ es sobre como usar o Git com CodeCommit, consulte Introdução à AWS CodeCommit no Guia CodeCommit do usuário da AWS. Para usar SageMaker Para usar o Git a partir do SageMaker console, você deve permitir que o Git recupere as credenciais do seu repositório. CodeCommi t Para obter instruçõe s, consulte Associar um CodeCommit repositório em uma conta diferente da AWS a uma instância de notebook na SageMaker documentação.	

Recursos relacionados

- Configure o acesso entre contas a um CodeCommit repositório da AWS usando funções (documentação da AWS CodeCommit)
- Tutorial do IAM: delegue o acesso em todas as contas da AWS usando funções do IAM (documentação do IAM)

Mais informações

Restringindo CodeCommit permissões para ações específicas

Para restringir as ações que um diretor do IAM pode realizar no CodeCommit repositório, modifique as ações que são permitidas na política de CodeCommit acesso.

Para obter mais informações sobre operações de CodeCommit API, consulte a referência de CodeCommit permissões no Guia CodeCommit do usuário da AWS.

> **Note**
>
> Você também pode editar a política gerenciada AWSCodeCommitPowerUserda AWS de acordo com seu caso de uso.

Restringindo CodeCommit permissões para repositórios específicos

Para criar um ambiente multilocatário em que mais de um repositório de código possa ser acessado somente por usuários específicos, faça o seguinte:

1. Crie várias funções de CodeCommit acesso na conta A. Em seguida, configure a política de confiança de cada função de acesso para permitir que usuários específicos na conta B assumam a função.
2. Restrinja quais repositórios de código cada função pode assumir adicionando uma condição de “Recurso” à política de cada função de CodeCommit acesso.

Exemplo de condição de “Recurso” que restringe o acesso de um diretor do IAM a um repositório específico CodeCommit

```
"Resource" : [<REPOSITORY_ARN>,<REPOSITORY_ARN> ]
```

> **Note**
>
> Para ajudar a identificar e diferenciar vários repositórios de código na mesma conta da AWS, você pode atribuir prefixos diferentes aos nomes dos repositórios. Por exemplo, você pode nomear repositórios de código com prefixos que se alinham a diferentes grupos de desenvolvedores, como myproject-subproject1-repo1 e myproject-subproject2-repo1. Em seguida, você pode criar um perfil do IAM para cada grupo de desenvolvedores com base nos prefixos atribuídos. Por exemplo, você pode criar um perfil chamado myproject-subproject1-repoaccess e conceder a ele acesso a todos os repositórios de código que incluem o prefixo myproject-subproject1.

Exemplo de condição de “Recurso” que se refere a um ARN de repositório de código que inclui um prefixo específico

```
"Resource" : arn:aws:codecommit:<region>:<account-id>:myproject-subproject1-*
```

Implemente uma estratégia GitHub de ramificação do Flow para ambientes com várias contas DevOps

Criado por Mike Stephens (AWS) e Abhilash Vinod (AWS)

Resumo

Ao gerenciar um repositório de código-fonte, diferentes estratégias de ramificação afetam os processos de desenvolvimento e lançamento de software que as equipes de desenvolvimento usam. Exemplos de estratégias comuns de ramificação incluem Trunk, GitHub Flow e Gitflow. Essas estratégias usam ramificações diferentes e as atividades realizadas em cada ambiente são diferentes. As organizações que estão implementando DevOps processos se beneficiariam de um guia visual para ajudá-las a entender as diferenças entre essas estratégias de ramificação. Usar esse visual em sua organização ajuda as equipes de desenvolvimento a alinhar seu trabalho e seguir os padrões organizacionais. Esse padrão fornece esse visual e descreve o processo de implementação de uma estratégia de ramificação do GitHub Flow em sua organização.

Esse padrão faz parte de uma série de documentação sobre como escolher e implementar estratégias de DevOps ramificação para organizações com várias Contas da AWS. Esta série foi criada para ajudar você a aplicar a estratégia correta e as melhores práticas desde o início, a fim de otimizar sua experiência na nuvem. GitHub O fluxo é apenas uma estratégia de ramificação possível que sua organização pode usar. Esta série de documentação também aborda os modelos de ramificação Trunk e Gitflow. Se você ainda não fez isso, recomendamos que você analise Como escolher uma estratégia de ramificação do Git para DevOps ambientes com várias contas antes de implementar a orientação desse padrão. Use a devida diligência para escolher a estratégia de ramificação certa para sua organização.

Este guia fornece um diagrama que mostra como uma organização pode implementar a estratégia GitHub de fluxo. É recomendável que você revise o AWS DevOps Well-Architected Guidance para analisar as melhores práticas. Esse padrão inclui tarefas, etapas e restrições recomendadas para cada etapa do DevOps processo.

Pré-requisitos e limitações

Pré-requisitos

- Git, instalado. Isso é usado como uma ferramenta de repositório de código-fonte.
- Draw.io, instalado. Esse aplicativo é usado para visualizar e editar o diagrama.

Arquitetura

Arquitetura de destino

O diagrama a seguir pode ser usado como um quadrado de Punnett (Wikipedia). Você alinha as ramificações no eixo vertical com os AWS ambientes no eixo horizontal para determinar quais ações realizar em cada cenário. Os números indicam a sequência das ações no fluxo de trabalho. Este exemplo leva você de uma `feature` filial até a implantação na produção.

Para obter mais informações sobre ambientes e ramificações em uma abordagem de GitHub fluxo, consulte Escolhendo uma estratégia de ramificação do Git para ambientes com várias contas.
Contas da AWS DevOps

Automação e escala

A integração contínua e a entrega contínua (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDpipelines) também fornecem governança e barreiras para as equipes de desenvolvimento, impondo consistência, padrões, melhores práticas e níveis mínimos de aceitação para aceitação e implantação de recursos. Para obter mais informações, consulte Praticando a integração contínua e a entrega contínua em AWS.

AWS oferece um conjunto de serviços para desenvolvedores projetados para ajudá-lo a criar pipelines de CI/CD. Por exemplo, AWS CodePipelineé um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura. AWS CodeBuildcompila o código-fonte, executa testes e produz pacotes ready-to-deploy de software. Para obter mais informações, consulte Ferramentas do desenvolvedor em AWS.

Ferramentas

AWS serviços e ferramentas

AWS fornece um conjunto de serviços para desenvolvedores que você pode usar para implementar esse padrão:

- AWS CodeArtifacté um serviço de repositório de artefatos gerenciado e altamente escalável que ajuda você a armazenar e compartilhar pacotes de software para desenvolvimento de aplicativos.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeDeployautomatiza implantações no Amazon Elastic Compute Cloud (Amazon EC2) ou em instâncias AWS Lambda , funções ou serviços do Amazon Elastic Container Service (Amazon ECS) no local.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.

Outras ferramentas

- O Draw.io Desktop é um aplicativo para criar fluxogramas e diagramas. O repositório de código contém modelos no formato.drawio para Draw.io.
- Figma é uma ferramenta de design on-line projetada para colaboração. O repositório de código contém modelos no formato.fig para Figma.

Repositório de código

Esse arquivo fonte para o diagrama nesse padrão está disponível no repositório GitHub Git Branching Strategy for GitHub Flow. Ele inclui arquivos nos formatos PNG, draw.io e Figma. Você pode modificar esses diagramas para apoiar os processos da sua organização.

Práticas recomendadas

Siga as melhores práticas e recomendações em AWS DevOps Well-Architected Guidance e Choosing a Git branching strategy para ambientes com várias contas. DevOps Isso ajuda você a implementar com eficiência o desenvolvimento GitHub baseado em Flow, promover a colaboração, melhorar a qualidade do código e simplificar o processo de desenvolvimento.

Épicos

Analisando os fluxos de trabalho do GitHub Flow

Tarefa	Descrição	Habilidades necessárias
Revise o processo GitHub de fluxo padrão.	1. No ambiente sandbox, o desenvolvedor cria uma `feature` ramificação a partir da ramificação e usa o `main` padrão de nomenclatura. `feature/<ticket>_<initials>_<short description>` 2. O desenvolvedor adiciona um ou mais commits à `feature` ramificação, cada um representando uma alteração ou melhoria discreta. 3. O desenvolvedor abre uma solicitação de mesclagem (MR) para mesclar as alterações na `main` ramificação. Isso inicia um processo de revisão. 4. Durante o processo de revisão, os desenvolvedores discutem as mudanças no código e fornecem feedback. O objetivo é garantir que as mudanças sejam de alta qualidade e atendam aos padrões do projeto.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	5. Depois que o desenvolvedor cria a solicitação de mesclagem, um processo de criação automatizado é iniciado e implanta as alterações na `feature` ramificação no ambiente de desenvolvimento. 6. Testes automatizados verificam a integridade e a qualidade das alterações encapsuladas na solicitação de mesclagem. Uma construção bem-sucedida, uma implantação bem-sucedida e um teste bem-sucedidos são necessários para concluir a solicitação de mesclagem. 7. Quando o processo de revisão estiver concluído, as alterações serão mescladas na `main` ramificação. 8. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de teste. 9. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de teste.	

Tarefa	Descrição	Habilidades necessárias
	10. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de produção.	

Tarefa	Descrição	Habilidades necessárias
Revise o processo de correção de bugs do GitHub Flow.	1. O desenvolvedor cria uma `bugfix` ramificação a partir da `main` ramificação e usa o padrão `bugfix/<ticket number>_<developer initials>_<descriptor>` de nomenclatura. 2. O desenvolvedor corrige o problema, confirma a correção e cria a `bugfix` ramificação. 3. O desenvolvedor abre uma solicitação de mesclagem para mesclar a `bugfix` ramificação na `main` ramificação. Isso inicia um processo de revisão. 4. Durante o processo de revisão, os desenvolv edores discutem as mudanças no código e fornecem feedback. 5. Após a conclusão e aprovação da revisão, o desenvolvedor conclui a solicitação de mesclagem da `bugfix` filial na `main` filial. 6. Um aprovador aprova manualmente a implantaç ão dos artefatos de	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	lançamento em ambientes superiores.	

Tarefa	Descrição	Habilidades necessárias
Revise o processo de hotfix GitHub Flow.	GitHub O Flow foi projetado para permitir a entrega contínua, em que as alteraçõe s de código são implantad as com frequência e confiabil idade em ambientes superiore s. A chave é que cada `feature` filial possa ser implantada a qualquer momento. `Hotfix`ramificações, que são semelhantes a `feature` ou `bugfix` ramificações, podem seguir o mesmo processo de qualquer uma dessas outras ramificaç ões. No entanto, devido à sua urgência, os hotfixes geralmente têm uma prioridad e mais alta. Dependend o das políticas da equipe e da rapidez da situação, certas etapas do processo podem ser aceleradas. Por exemplo, as revisões de código para hotfixes podem ser aceleradas. Portanto, embora o processo de hotfix seja paralelo ao processo de recurso ou correção de bugs, a urgência em torno dos hotfixes pode justificar modificações na adesão aos procedimentos. É fundament	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	al estabelecer diretrizes sobre o gerenciamento de hotfixes para garantir que eles sejam tratados com eficiência e segurança.	

Solução de problemas

Problema	Solução
Conflitos filiais	Um problema comum que pode ocorrer com o modelo GitHub Flow é quando um hotfix precisa ocorrer na produção, mas uma alteração correspondente precisa ocorrer em uma `feature` `hotfix` ramificação ou ramificação em que os mesmos recursos estão sendo modificados. `bugfix` Recomendamos que você mescle frequentemente as alteraçõe s das `main` ramificações inferiores para evitar conflitos significativos ao mesclar com. `main`
maturidade da equipe	GitHub O Flow incentiva implantações diárias em ambientes superiores, adotando a verdadeira integração contínua e entrega contínua (CI/CD). É fundamental que a equipe tenha a maturidade de engenharia para criar recursos e criar testes de automação para eles. A equipe deve realizar uma análise exaustiva da solicitação de mesclagem antes que as alterações sejam aprovadas. Isso promove uma cultura de engenharia robusta que promove qualidade, responsabilidade e eficiência no processo de desenvolvimento.

Recursos relacionados

Este guia não inclui treinamento para Git; no entanto, há muitos recursos de alta qualidade disponíveis na Internet se você precisar desse treinamento. Recomendamos que você comece com o site de documentação do Git.

Os recursos a seguir podem ajudá-lo em sua jornada de ramificação do GitHub Flow no Nuvem AWS.

AWS DevOps orientação

- AWS DevOps Orientação
- AWS Arquitetura de referência do pipeline de implantação
- O que DevOps é
- DevOps recursos

GitHub Orientação de fluxo

- GitHub Tutorial de início rápido do Flow () GitHub
- Por que GitHub Flow?

Outros recursos

- Metodologia de aplicativo de doze fatores (12factor.net)

Implemente uma estratégia de ramificação do Gitflow para ambientes com várias contas DevOps

Criado por Mike Stephens (AWS), Stephen (DiCato AWS), Tim Wondergem (AWS) e Abhilash Vinod (AWS)

Resumo

Ao gerenciar um repositório de código-fonte, diferentes estratégias de ramificação afetam os processos de desenvolvimento e lançamento de software que as equipes de desenvolvimento usam. Exemplos de estratégias comuns de ramificação incluem Trunk, Gitflow e Flow. GitHub Essas estratégias usam ramificações diferentes e as atividades realizadas em cada ambiente são diferentes. As organizações que estão implementando DevOps processos se beneficiariam de um guia visual para ajudá-las a entender as diferenças entre essas estratégias de ramificação. Usar esse visual em sua organização ajuda as equipes de desenvolvimento a alinhar seu trabalho e seguir os padrões organizacionais. Esse padrão fornece esse visual e descreve o processo de implementação de uma estratégia de ramificação do Gitflow em sua organização.

Esse padrão faz parte de uma série de documentação sobre como escolher e implementar estratégias de DevOps ramificação para organizações com várias Contas da AWS. Esta série foi criada para ajudar você a aplicar a estratégia correta e as melhores práticas desde o início, a fim de otimizar sua experiência na nuvem. O Gitflow é apenas uma estratégia de ramificação possível que sua organização pode usar. Esta série de documentação também aborda os modelos de ramificação Trunk e GitHub Flow. Se você ainda não fez isso, recomendamos que você analise Como escolher uma estratégia de ramificação do Git para DevOps ambientes com várias contas antes de implementar a orientação desse padrão. Use a devida diligência para escolher a estratégia de ramificação certa para sua organização.

Este guia fornece um diagrama que mostra como uma organização pode implementar a estratégia do Gitflow. É recomendável que você revise o AWS DevOps Well-Architected Guidance para analisar as melhores práticas. Esse padrão inclui tarefas, etapas e restrições recomendadas para cada etapa do DevOps processo.

Pré-requisitos e limitações

Pré-requisitos

- Git, instalado. Isso é usado como uma ferramenta de repositório de código-fonte.
- Draw.io, instalado. Esse aplicativo é usado para visualizar e editar o diagrama.

- (Opcional) Plugin Gitflow, instalado.

Arquitetura

Arquitetura de destino

O diagrama a seguir pode ser usado como um quadrado de Punnett (Wikipedia). Você alinha as ramificações no eixo vertical com os AWS ambientes no eixo horizontal para determinar quais ações realizar em cada cenário. Os números indicam a sequência das ações no fluxo de trabalho. Este exemplo leva você de uma ramificação de recursos até a implantação na produção.

Para obter mais informações sobre ambientes e ramificações em uma abordagem do Contas da AWS Gitflow, consulte Escolhendo uma estratégia de ramificação do Git para ambientes com várias contas. DevOps

Automação e escala

A integração contínua e a entrega contínua (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDpipelines) também fornecem governança e barreiras para as equipes de desenvolvimento, impondo consistência, padrões, melhores práticas e níveis mínimos de aceitação para aceitação e implantação de recursos. Para obter mais informações, consulte Praticando a integração contínua e a entrega contínua em AWS.

AWS oferece um conjunto de serviços para desenvolvedores projetados para ajudá-lo a criar pipelines de CI/CD. Por exemplo, AWS CodePipelineé um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura. AWS CodeBuildcompila o código-fonte, executa testes e produz pacotes ready-to-deploy de software. Para obter mais informações, consulte Ferramentas do desenvolvedor em AWS.

Ferramentas

AWS serviços e ferramentas

AWS fornece um conjunto de serviços para desenvolvedores que você pode usar para implementar esse padrão:

- AWS CodeArtifacté um serviço de repositório de artefatos gerenciado e altamente escalável que ajuda você a armazenar e compartilhar pacotes de software para desenvolvimento de aplicativos.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeDeployautomatiza implantações no Amazon Elastic Compute Cloud (Amazon EC2) ou em instâncias AWS Lambda , funções ou serviços do Amazon Elastic Container Service (Amazon ECS) no local.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.

Outras ferramentas

- O Draw.io Desktop é um aplicativo para criar fluxogramas e diagramas. O repositório de código contém modelos no formato.drawio para Draw.io.
- Figma é uma ferramenta de design on-line projetada para colaboração. O repositório de código contém modelos no formato.fig para Figma.
- (Opcional) O plug-in Gitflow é uma coleção de extensões do Git que fornecem operações de repositório de alto nível para o modelo de ramificação do Gitflow.

Repositório de código

Esse arquivo fonte para o diagrama nesse padrão está disponível na Estratégia de ramificação do GitHub Git para repositório. GitFlow Inclui arquivos nos formatos PNG, draw.io e Figma. Você pode modificar esses diagramas para apoiar os processos da sua organização.

Práticas recomendadas

Siga as melhores práticas e recomendações em AWS DevOps Well-Architected Guidance e Choosing a Git branching strategy para ambientes com várias contas. DevOps Isso ajuda você a implementar com eficácia o desenvolvimento baseado em Gitflow, promover a colaboração, melhorar a qualidade do código e agilizar o processo de desenvolvimento.

Épicos

Analisando os fluxos de trabalho do Gitflow

Tarefa	Descrição	Habilidades necessárias
Revise o processo padrão do Gitflow.	1. No ambiente sandbox, o desenvolvedor cria uma `feature` ramificação a partir da ramificação e usa o `develop` padrão de nomenclatura. `feature/<ticket>_<initials>_<short description>` 2. O desenvolvedor desenvolve o código e implanta o código no ambiente sandbox de forma iterativa para concluir o tíquete. **Note** Opcionalmente, o desenvolvedor pode criar uma `sandbox` ramificação para executar um pipeline automatizado de compilação ou implantação no ambiente sandbox. 3. O desenvolvedor cria uma solicitação de mesclagem da `feature` ramificação para a `develop` ramificaç	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ão usando uma mesclagem de squash. 4. Um pipeline de integraçã o contínua e entrega contínua (CI/CD) cria e implanta automatic amente a `develop` filial no ambiente de desenvolv imento. 5. (Opcional) Um desenvolv edor integra `feature` ramificações adicionais à ramificação de desenvolv imento antes de continuar com as atividades de lançamento. 6. Quando você estiver pronto para lançar os recursos na `develop` ramificaç ão, o desenvolvedor cria uma `release` ramificação com o nome `release/v<number>` da `develop` ramificação. 7. O desenvolvedor cria a ramificação de lançament o, que publica artefatos para reutilização em outros ambientes. 8. Um aprovador aprova manualmente a implantaç ão dos artefatos de lançamento no ambiente de teste.	

Tarefa	Descrição	Habilidades necessárias
	9. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de teste. 10. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de produção. 11. O desenvolvedor mescla a `release` ramificação com a `main` ramificação. Idealmente, o desenvolvedor usa um script automatizado para realizar uma mesclagem rápida. Não use uma mesclagem de squash. 12. O desenvolvedor mescla a `release` ramificação com a `develop` ramificação. Idealmente, o desenvolvedor usa um script automatizado para realizar uma mesclagem rápida. Não use uma mesclagem de squash.	

Tarefa	Descrição	Habilidades necessárias
Revise o processo de hotfix do Gitflow.	1. O desenvolvedor cria uma `hotfix` ramificação a partir da `main` ramificação e usa o padrão `hotfix/<ticket>_<initials>_<short description>` de nomenclatura. 2. O desenvolvedor cria uma `release` ramificação a partir da `main` ramificação e a nomeia `release/v<number>` . 3. O desenvolvedor corrige o problema, confirma a correção e cria a `hotfix` ramificação. 4. O desenvolvedor cria uma solicitação de mesclagem da `hotfix` ramificação para a `release/v<number>` ramificação usando uma mesclagem de squash. 5. O desenvolvedor cria a `release` filial, que publica artefatos para reutilização em outros ambientes. 6. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de teste.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	7. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de teste. 8. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de produção. 9. O desenvolvedor mescla a `release` ramificação com a `main` ramificação. Idealmente, o desenvolvedor usa um script automatizado para realizar uma mesclagem rápida. Não use uma mesclagem de squash. 10. O desenvolvedor mescla a `release` ramificação com a `develop` ramificação. Idealmente, o desenvolvedor usa um script automatizado para realizar uma mesclagem rápida. Não use uma mesclagem de squash. 11. Se um conflito for detectado, os desenvolvedores recebem um alerta e resolvem o conflito com uma solicitação de mesclagem.	

Tarefa	Descrição	Habilidades necessárias
Revise o processo de correção de bugs do Gitflow.	1. O desenvolvedor cria uma `bugfix` ramificação a partir da `release/v<number>` ramificação atual e usa o padrão `bugfix/<ticket number>_<developer initials>_<descriptor>` de nomenclatura. 2. O desenvolvedor corrige o problema, confirma a correção e cria a `bugfix` ramificação. 3. O desenvolvedor cria uma solicitação de mesclagem da `bugfix` ramificação para a `release/v<number>` ramificação usando uma mesclagem de squash. 4. O desenvolvedor cria a `release` filial, que publica artefatos para reutilização em outros ambientes. 5. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de teste. 6. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente Stage.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	7. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de produção. 8. O desenvolvedor mescla a `release` ramificação com a `main` ramificação. Idealmente, o desenvolvedor usa um script automatizado para realizar uma mesclagem rápida. Não use uma mesclagem de squash. 9. O desenvolvedor mescla a `release` ramificação com a `develop` ramificação. Idealmente, o desenvolvedor usa um script automatizado para realizar uma mesclagem rápida. Não use uma mesclagem de squash. 10. Se um conflito for detectado, os desenvolvedores recebem um alerta e resolvem o conflito com uma solicitação de mesclagem.	

Solução de problemas

Problema	Solução
Conflitos filiais	Um problema comum que pode ocorrer com o modelo Gitflow é quando um hotfix precisa ocorrer na produção, mas uma alteração correspondente precisa ocorrer em um ambiente inferior, onde outra ramificaç ão está modificando os mesmos recursos. Recomendamos que você tenha apenas uma única ramificação de lançamento ativa por vez. Se você tiver mais de um ativo por vez, as mudanças nos ambientes podem colidir e talvez você não consiga levar uma filial para a produção.
Mesclar	As versões devem ser incorporadas novamente à principal e desenvolvidas o mais rápido possível para consolidar o trabalho nas ramificações principais.
Fusão de squash	Use uma mesclagem de squash somente quando estiver mesclando de uma `feature` ramificação para outra. `develop` Usar mesclagens de abóbora em galhos mais altos causa dificuldade ao mesclar mudanças de volta para galhos mais baixos.

Recursos relacionados

Este guia não inclui treinamento para Git; no entanto, há muitos recursos de alta qualidade disponíveis na Internet se você precisar desse treinamento. Recomendamos que você comece com o site de documentação do Git.

Os recursos a seguir podem ajudá-lo em sua jornada de ramificação do Gitflow no. Nuvem AWS

AWS DevOps orientação

- AWS DevOps Orientação
- AWS Arquitetura de referência do pipeline de implantação
- O que é DevOps?
- DevOps recursos

Orientação do Gitflow

- O blog original do Gitflow (postagem no blog de Vincent Driessen)
- Fluxo de trabalho do Gitflow (Atlassian)
- Gitflow ativado GitHub: Como usar fluxos de trabalho do Git Flow com GitHub repositórios baseados (vídeo) YouTube
- Exemplo de Git Flow Init (vídeo) YouTube
- A ramificação de lançamento do Gitflow do início ao fim (vídeo) YouTube

Outros recursos

Metodologia de aplicativo de doze fatores (12factor.net)

Implemente uma estratégia de ramificação de troncos para ambientes com várias contas DevOps

Criado por Mike Stephens (AWS) e Rayjan Wilson (AWS)

Resumo

Ao gerenciar um repositório de código-fonte, diferentes estratégias de ramificação afetam os processos de desenvolvimento e lançamento de software que as equipes de desenvolvimento usam. Exemplos de estratégias comuns de ramificação incluem Trunk, GitHub Flow e Gitflow. Essas estratégias usam ramificações diferentes e as atividades realizadas em cada ambiente são diferentes. As organizações que estão implementando DevOps processos se beneficiariam de um guia visual para ajudá-las a entender as diferenças entre essas estratégias de ramificação. Usar esse visual em sua organização ajuda as equipes de desenvolvimento a alinhar seu trabalho e seguir os padrões organizacionais. Esse padrão fornece esse visual e descreve o processo de implementação de uma estratégia de ramificação de troncos em sua organização.

Esse padrão faz parte de uma série de documentação sobre como escolher e implementar estratégias de DevOps ramificação para organizações com várias Contas da AWS. Esta série foi criada para ajudar você a aplicar a estratégia correta e as melhores práticas desde o início, a fim de otimizar sua experiência na nuvem. Trunk é apenas uma estratégia de ramificação possível que sua organização pode usar. Esta série de documentação também aborda os modelos de ramificação do GitHub Flow e do Gitflow. Se você ainda não fez isso, recomendamos que você revise Como escolher uma estratégia de ramificação do Git para DevOps ambientes com várias contas antes de implementar a orientação desse padrão. Use a devida diligência para escolher a estratégia de ramificação certa para sua organização.

Este guia fornece um diagrama que mostra como uma organização pode implementar a estratégia Trunk. É recomendável que você revise o AWS DevOps Well-Architected Guidance oficial para analisar as melhores práticas. Esse padrão inclui tarefas, etapas e restrições recomendadas para cada etapa do DevOps processo.

Pré-requisitos e limitações

Pré-requisitos

- Git, instalado. Isso é usado como uma ferramenta de repositório de código-fonte.
- Draw.io, instalado. Esse aplicativo é usado para visualizar e editar o diagrama.

Arquitetura

Arquitetura de destino

O diagrama a seguir pode ser usado como um quadrado de Punnett (Wikipedia). Você alinha as ramificações no eixo vertical com os AWS ambientes no eixo horizontal para determinar quais ações realizar em cada cenário. Os números indicam a sequência das ações no fluxo de trabalho. Este exemplo leva você de uma `feature` filial até a implantação na produção.

Para obter mais informações sobre ambientes e ramificações em uma abordagem de tronco, consulte Escolhendo uma estratégia de ramificação do Git para ambientes com várias contas. Contas da AWS DevOps

Automação e escala

A integração contínua e a entrega contínua (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDpipelines) também fornecem governança e barreiras para as equipes de desenvolvimento, impondo consistência, padrões, melhores práticas e níveis mínimos de aceitação para aceitação e implantação de recursos. Para obter mais informações, consulte Praticando a integração contínua e a entrega contínua em AWS.

AWS oferece um conjunto de serviços para desenvolvedores projetados para ajudá-lo a criar pipelines de CI/CD. Por exemplo, AWS CodePipelineé um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura. AWS CodeBuildcompila o código-fonte, executa testes e produz pacotes ready-to-deploy de software. Para obter mais informações, consulte Ferramentas do desenvolvedor em AWS.

Ferramentas

AWS serviços e ferramentas

AWS fornece um conjunto de serviços para desenvolvedores que você pode usar para implementar esse padrão:

- AWS CodeArtifacté um serviço de repositório de artefatos gerenciado e altamente escalável que ajuda você a armazenar e compartilhar pacotes de software para desenvolvimento de aplicativos.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeDeployautomatiza implantações no Amazon Elastic Compute Cloud (Amazon EC2) ou em instâncias AWS Lambda , funções ou serviços do Amazon Elastic Container Service (Amazon ECS) no local.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar as alterações de software continuamente.

Outras ferramentas

- Draw.io Desktop — Um aplicativo para criar fluxogramas e diagramas.
- Figma é uma ferramenta de design on-line projetada para colaboração. O repositório de código contém modelos no formato.fig para Figma.

Repositório de código

Esse arquivo fonte para o diagrama nesse padrão está disponível no repositório GitHub Git Branching Strategy for Trunk. Inclui arquivos nos formatos PNG, draw.io e Figma. Você pode modificar esses diagramas para apoiar os processos da sua organização.

Práticas recomendadas

Siga as melhores práticas e recomendações em AWS DevOps Well-Architected Guidance e Choosing a Git branching strategy para ambientes com várias contas. DevOps Isso ajuda você a implementar com eficiência o desenvolvimento baseado em troncos, promover a colaboração, melhorar a qualidade do código e agilizar o processo de desenvolvimento.

Épicos

Analisando o fluxo de trabalho do Trunk

Tarefa	Descrição	Habilidades necessárias
Revise o processo de tronco padrão.	1. No ambiente sandbox, o desenvolvedor cria uma `feature` ramificação a partir da ramificação e usa o `main` padrão de nomenclatura. `feature/<ticket>_<initials>_<short description>` 2. O desenvolvedor desenvolve o código e implanta o código no ambiente sandbox de forma iterativa para concluir o tíquete. **Note** Opcionalmente, o desenvolvedor pode criar uma `sandbox` ramificação para executar um pipeline automatizado de criação ou implantação no ambiente sandbox. 3. O desenvolvedor cria uma solicitação de mesclagem da `feature` ramificação para a `main` ramificação	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	usando uma mesclagem de squash. 4. Um pipeline de integração contínua e entrega contínua (CI/CD) cria e publica automaticamente os artefatos da `main` filial para o ambiente de desenvolvimento. 5. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de desenvolvimento. 6. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de teste. 7. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de teste. 8. Um aprovador aprova manualmente a implantação dos artefatos de lançamento no ambiente de produção.	

Solução de problemas

Problema	Solução
Conflitos filiais	Um problema comum que pode ocorrer com o modelo Trunk é quando um hotfix precisa ocorrer na produção, mas uma alteração correspondente precisa ocorrer em uma `feature` ramificação, onde os mesmos recursos estão sendo modificados. Recomendamos que você mescle frequente mente as alterações das `main` ramificações inferiores para evitar conflitos significativos na mesclagem com. `main`

Recursos relacionados

Este guia não inclui treinamento para Git; no entanto, há muitos recursos de alta qualidade disponíveis na Internet se você precisar desse treinamento. Recomendamos que você comece com o site de documentação do Git.

Os recursos a seguir podem ajudá-lo em sua jornada de ramificação de troncos no Nuvem AWS.

AWS DevOps orientação

- AWS DevOps Orientação
- Arquitetura de referência do pipeline de implantação da AWS
- O que é DevOps?
- DevOps recursos

Orientação do tronco

- Desenvolvimento baseado em troncos

Outros recursos

- Metodologia de aplicativo de doze fatores (12factor.net)

Implemente o escaneamento Checkov personalizado e centralizado para aplicar a política antes de implantar a infraestrutura AWS

Criado por Benjamin Morris (AWS)

Resumo

Esse padrão fornece uma estrutura de GitHub ações para escrever políticas personalizadas do Checkov em um repositório que pode ser reutilizada em toda a organização. GitHub Seguindo esse padrão, uma equipe de segurança da informação pode escrever, adicionar e manter políticas personalizadas com base nos requisitos da empresa. As políticas personalizadas podem ser inseridas automaticamente em todos os pipelines da GitHub organização. Essa abordagem pode ser usada para impor os padrões de recursos da empresa antes que os recursos sejam implantados.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Uma GitHub organização usando GitHub Ações
- AWS infraestrutura implantada com HashiCorp Terraform ou AWS CloudFormation

Limitações

- Esse padrão foi escrito para GitHub Ações. No entanto, ele pode ser adaptado a estruturas similares de integração contínua e entrega contínua (CI/CD), como. GitLab Nenhuma versão paga específica do GitHub é necessária.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para a disponibilidade da região, consulte Pontos de extremidade e cotas de serviço na AWS documentação e escolha o link para o serviço.

Arquitetura

Esse padrão foi projetado para ser implantado como um GitHub repositório que contém um fluxo de trabalho GitHub reutilizável e políticas personalizadas do Checkov. O fluxo de trabalho reutilizável pode escanear tanto o Terraform quanto os repositórios de CloudFormation infraestrutura como código (IaC).

O diagrama a seguir mostra o repositório de GitHub fluxos de trabalho reutilizáveis e o repositório de políticas do Custom Checkov como ícones separados. No entanto, você pode implementar esses repositórios como repositórios separados ou como um único repositório. O código de exemplo usa um único repositório, com arquivos para fluxos de trabalho (`.github/workflows`) e arquivos para políticas personalizadas (`custom_policies`pasta e arquivo de `.checkov.yml` configuração) no mesmo repositório.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário cria uma pull request em um GitHub repositório.
2. Os fluxos de trabalho do pipeline começam em GitHub Ações, incluindo uma referência a um fluxo de trabalho reutilizável do Checkov.
3. O fluxo de trabalho do pipeline baixa o fluxo de trabalho reutilizável Checkov referenciado de um repositório externo e executa esse fluxo de trabalho Checkov usando Ações. GitHub
4. O fluxo de trabalho reutilizável do Checkov baixa as políticas personalizadas de um repositório externo.
5. O fluxo de trabalho reutilizável do Checkov avalia o IaC no GitHub repositório em relação às políticas incorporadas e personalizadas do Checkov. O fluxo de trabalho reutilizável do Checkov passa ou falha com base na descoberta de problemas de segurança.

Automação e escala

Esse padrão permite o gerenciamento central da configuração do Checkov, para que as atualizações de políticas possam ser aplicadas em um único local. No entanto, esse padrão exige que cada repositório use um fluxo de trabalho que contenha uma referência ao fluxo de trabalho central reutilizável. Você pode adicionar essa referência manualmente ou usar scripts para enviar o arquivo para a `.github/workflows` pasta de cada repositório.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões. Checkov pode escanear CloudFormation.

Outras ferramentas

- O Checkov é uma ferramenta estática de análise de código que verifica o IaC em busca de configurações incorretas de segurança e conformidade.
- GitHub O Actions é integrado à GitHub plataforma para ajudar você a criar, compartilhar e executar fluxos de trabalho em seus GitHub repositórios. Você pode usar o GitHub Actions para automatizar tarefas como criar, testar e implantar seu código.
- O Terraform é uma ferramenta de IaC HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local. Checkov pode escanear o Terraform.

Repositório de código

O código desse padrão está disponível no GitHub centralized-custom-checkov-sastrepositório.

Práticas recomendadas

- Para manter uma postura de segurança consistente, alinhe as políticas de segurança da sua empresa com as políticas da Checkov.
- Nas fases iniciais da implementação das políticas personalizadas do Checkov, você pode usar a opção soft-fail em sua verificação do Checkov para permitir que o IaC com problemas de segurança seja mesclado. À medida que o processo amadurece, mude da opção de falha suave para a opção de falha definitiva.

Épicos

Crie um repositório central do Checkov para políticas personalizadas

Tarefa	Descrição	Habilidades necessárias
Crie um repositório central do Checkov.	Crie um repositório para armazenar políticas personalizadas do Checkov que serão usadas na organização. Para começar rapidamente, você pode copiar o conteúdo do repositório desse padrão	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	em seu GitHub centralized-custom-checkov-sast repositório central do Checkov.	
Crie um repositório para fluxos de trabalho reutilizáveis.	Se já existir um repositório para fluxos de trabalho reutilizáveis ou se você planeja incluir arquivos de fluxo de trabalho reutilizáveis no mesmo repositório das políticas personalizadas do Checkov, você pode pular esta etapa. Crie um GitHub repositório para armazenar fluxos de trabalho reutilizáveis. Os pipelines de outros repositórios farão referência a esse repositório.	DevOps engenheiro

Crie fluxos de trabalho Checkov reutilizáveis e de exemplo

Tarefa	Descrição	Habilidades necessárias
Adicione um fluxo de trabalho Checkov reutilizável.	Crie um fluxo de trabalho Checkov GitHub Actions reutilizável (arquivo YAML) no repositório de fluxos de trabalho reutilizáveis. Você pode adaptar esse fluxo de trabalho reutilizável a partir do arquivo de fluxo de trabalho fornecido nesse padrão.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Um exemplo de alteração que talvez você queira fazer é alterar o fluxo de trabalho reutilizável para usar a opção soft-fail. A configuração `soft-fail` para `true` permite que o trabalho seja concluído com êxito, mesmo se houver uma falha na verificação do Checkov. Para obter instruções, consulte Falha rígida e flexível na documentação do Checkov.	
Adicione um exemplo de fluxo de trabalho.	Adicione um exemplo de fluxo de trabalho Checkov que faça referência ao `reusable` fluxo de trabalho. Isso fornecerá um modelo de como reutilizar o `reusable` fluxo de trabalho. No repositório de exemplo, `checkov-source.yaml` é o fluxo de trabalho reutilizável e `checkov-scan.yaml` é o exemplo que consome. `checkov-source` Para obter mais detalhes sobre como escrever um exemplo de fluxo de trabalho do Checkov, consulte Informações adicionais.	DevOps engenheiro

Associe as políticas da empresa às políticas personalizadas da Checkov

Tarefa	Descrição	Habilidades necessárias
Determine as políticas que podem ser aplicadas com o Checkov.	1. Analise as políticas da empresa relacionadas à segurança da infraestrutura e quais requisitos devem estar em vigor. 2. Determine quais requisitos podem ser implementados usando as políticas personalizadas da Checkov. 3. Crie uma convenção de nomenclatura que mapeie o controle de política para a política personalizada do Checkov. Normalmente, as políticas personalizadas da Checkov têm um identificador com o nome da Checkov, a fonte da política (personalizada) e um número da política (por exemplo,`CKV2_CUSTOM_123`). Para obter mais detalhes sobre a criação de políticas personalizadas do Checkov, consulte Visão geral das políticas personalizadas na documentação do Checkov.	Segurança e conformidade

Tarefa	Descrição	Habilidades necessárias
Adicione políticas personalizadas do Checkov.	Converta as políticas identificadas da empresa em políticas personalizadas do Checkov no repositório central. Você pode escrever políticas simples de Checkov em Python ou YAML.	Segurança

Implemente políticas personalizadas centralizadas da Checkov

Tarefa	Descrição	Habilidades necessárias
Adicione o fluxo de trabalho reutilizável Checkov a todos os repositórios.	Nesse ponto, você deve ter um exemplo de fluxo de trabalho Checkov que faça referência ao fluxo de trabalho reutilizável. Copie o exemplo do fluxo de trabalho Checkov que faz referência ao fluxo de trabalho reutilizável para cada repositório que o requer.	DevOps engenheiro
Crie um mecanismo para garantir que o Checkov seja executado antes das fusões.	Para garantir que o fluxo de trabalho do Checkov seja executado para cada pull request, crie uma verificação de status que exija um fluxo de trabalho Checkov bem-sucedido antes que os pull requests possam ser mesclados. GitHub permite que você exija que fluxos de trabalho específicos sejam executados antes que as	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	pull requests possam ser mescladas.	
Crie um PAT para toda a organização e compartilhe-o em segredo.	Se sua GitHub organização estiver visível publicamente, você pode pular essa etapa. Esse padrão exige que o fluxo de trabalho do Checkov seja capaz de baixar políticas personalizadas do repositór io de políticas personalizadas em sua GitHub organização. Você deve fornecer permissõe s para que o fluxo de trabalho do Checkov possa acessar esses repositórios. Para fazer isso, crie um token de acesso pessoal (PAT) com permissões para ler os repositórios da organizaç ão. Compartilhe esse PAT com repositórios, seja como um segredo para toda a organização (se estiver em um plano pago) ou como um segredo em cada repositório (versão gratuita). No código de exemplo, o nome padrão do segredo é `ORG_PAT`.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
(Opcional) Proteja os arquivos do fluxo de trabalho do Checkov contra modificações.	Para proteger os arquivos do fluxo de trabalho do Checkov contra alterações indesejadas, você pode usar um `CODEOWNERS` arquivo. Normalmente, o `CODEOWNERS` arquivo é implantado na raiz do diretório. Por exemplo, para exigir aprovações do `secEng` grupo da sua GitHub organização quando o `checkov-scan.yaml` arquivo for modificado, acrescente o seguinte ao arquivo do repositório: `CODEOWNERS` `[Checkov] .github/workflows/checkov-scan.yaml @myOrg/secEng` Um `CODEOWNERS` arquivo é específico para o repositório em que ele reside. Para proteger o fluxo de trabalho do Checkov usado pelo repositório, você deve adicionar (ou atualizar) um `CODEOWNERS` arquivo em cada repositório. Para obter mais informações sobre a proteção dos arquivos de fluxo de trabalho do Checkov, consulte Informaçõ	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	es adicionais. Para obter mais informações sobre `CODEOWNERS` arquivos, consulte a documentação oficial do seu provedor de CI/CD (como GitHub).	

Recursos relacionados

- Visão geral das políticas personalizadas da Checkov
- CloudFormation Escaneamento de configuração
- GitHub Ações Fluxos de trabalho reutilizáveis

Mais informações

Escrevendo arquivos de fluxo de trabalho do Checkov

Ao escrever`checkov-scan.yaml`, considere quando você quer que ele seja executado. A `on` chave de nível superior determina quando o fluxo de trabalho é executado. No repositório de exemplo, o fluxo de trabalho será executado quando houver uma pull request direcionada à `main` ramificação (e sempre que a ramificação de origem da pull request for modificada). O fluxo de trabalho também pode ser executado conforme necessário devido à `workflow_dispatch` chave.

Você pode alterar as condições de acionamento do fluxo de trabalho com base na frequência com que deseja que o fluxo de trabalho seja executado. Por exemplo, você pode alterar o fluxo de trabalho para ser executado sempre que o código for enviado para qualquer ramificação `pull_request` substituindo `push` e removendo a `branches` chave.

Você pode modificar o arquivo de exemplo de fluxo de trabalho que você criou em um repositório individual. Por exemplo, você pode ajustar o nome da ramificação de destino de `main` para `production` se um repositório estiver estruturado em torno de uma `production` ramificação.

Protegendo arquivos de fluxo de trabalho do Chec

O escaneamento Checkov fornece informações úteis sobre possíveis erros de configuração de segurança. No entanto, alguns desenvolvedores podem perceber que isso é uma barreira para sua produtividade e tentar remover ou desativar o fluxo de trabalho de digitalização.

Há várias maneiras de resolver esse problema, incluindo melhores mensagens sobre o valor a longo prazo da verificação de segurança e documentação mais clara sobre como implantar uma infraestrutura segura. Essas são abordagens “leves” importantes de DevSecOps colaboração que podem ser vistas como a solução para a causa raiz desse problema. No entanto, você também pode usar controles técnicos, como um `CODEOWNERS` arquivo, como grades de proteção para ajudar a manter os desenvolvedores no caminho certo.

Padrão de teste em uma caixa de areia

Para testar esse padrão em um ambiente sandbox, siga estas etapas:

1. Crie uma nova GitHub organização. Crie um token com acesso somente de leitura a todos os repositórios da organização. Como esse token é para um ambiente sandbox, não para um ambiente pago, você não poderá armazená-lo em um segredo para toda a organização.
2. Crie um `checkov` repositório para manter a configuração do Checkov e um `github-workflows` repositório para manter a configuração do fluxo de trabalho reutilizável. Preencha os repositórios com o conteúdo do repositório de exemplo.
3. Crie um repositório de aplicativos e copie e cole o `checkov-scan.yaml` fluxo de trabalho em sua `.github/workflows` pasta. Adicione um segredo ao repositório que contém o PAT que você criou para acesso somente para leitura da organização. O segredo padrão é `ORG_PAT`.
4. Crie uma pull request que adicione um pouco de Terraform ou CloudFormation código ao repositório do aplicativo. Checkov deve digitalizar e retornar um resultado.

Detecte alterações automaticamente e inicie diferentes CodePipeline pipelines para um monorepo em CodeCommit

Criado por Helton Ribeiro (AWS), Petrus Batalha (AWS) e Ricardo Morais (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Aviso: não AWS Cloud9 está mais disponível para novos clientes. Os clientes existentes do AWS Cloud9 podem continuar usando o serviço normalmente. Saiba mais

Esse padrão ajuda você a detectar automaticamente alterações no código-fonte de um aplicativo baseado em monorepo AWS CodeCommit e, em seguida, iniciar um pipeline AWS CodePipeline que executa a integração contínua e a entrega contínua (CI/CD) automation for each microservice. This approach means that each microservice in your monorepo-based application can have a dedicated CI/CDpipeline), o que garante melhor visibilidade, compartilhamento mais fácil do código e melhor colaboração, padronização e capacidade de descoberta.

A solução descrita nesse padrão não realiza nenhuma análise de dependência entre os microsserviços dentro do monorepo. Ele só detecta alterações no código-fonte e inicia o pipeline de CI/CD correspondente.

O padrão é usado AWS Cloud9 como ambiente de desenvolvimento integrado (IDE) e AWS Cloud Development Kit (AWS CDK) para definir uma infraestrutura usando duas AWS CloudFormation pilhas: `MonoRepoStack` e. `PipelinesStack` A `MonoRepoStack` pilha cria o monorepo in AWS CodeCommit e a AWS Lambda função que inicia os pipelines de CI/CD. A pilha `PipelinesStack` define sua infraestrutura de pipeline.

> **Important**
>
> O fluxo de trabalho desse padrão é uma prova de conceito (PoC). Recomendamos que você o use somente em um ambiente de teste. Se você quiser usar a abordagem desse padrão em um ambiente de produção, consulte as melhores práticas de segurança no IAM na documentação AWS Identity and Access Management (IAM) e faça as alterações necessárias em suas funções do IAM Serviços da AWS e.

Pré-requisitos e limitações

Pré-requisitos

- Uma AWS conta ativa.
- AWS Command Line Interface (AWS CLI), instalado e configurado. Para obter mais informações, consulte Instalação, atualização e desinstalação do AWS CLI na AWS CLI documentação.
- Python 3 e `pip`, instalado na sua máquina local. Para obter mais informações, consulte a Documentação do Python.
- AWS CDK, instalado e configurado. Para obter mais informações, consulte Introdução ao AWS CDK na AWS CDK documentação.
- Um AWS Cloud9 IDE, instalado e configurado. Para obter mais informações, consulte Configuração AWS Cloud9 na AWS Cloud9 documentação.
- O GitHub AWS CodeCommit monorepo multi-pipeline aciona o repositório, clonado em sua máquina local.
- Um diretório existente contendo o código do aplicativo com o qual você deseja criar e implantar CodePipeline.
- Familiaridade e experiência com as DevOps melhores práticas no Nuvem AWS. Para aumentar sua familiaridade com DevOps, você pode usar o padrão Crie uma arquitetura fracamente acoplada com microsserviços usando DevOps práticas e AWS Cloud9 no site de orientação prescritiva. AWS

Arquitetura

O diagrama a seguir mostra como usar o AWS CDK para definir uma infraestrutura com duas AWS CloudFormation pilhas: `MonoRepoStack` e. `PipelinesStack`

O diagrama mostra o seguinte fluxo de trabalho:

1. O processo de bootstrap usa o AWS CDK para criar as AWS CloudFormation pilhas e. `MonoRepoStack` `PipelinesStack`
2. A `MonoRepoStack` pilha cria o CodeCommit repositório para seu aplicativo e a função `monorepo-event-handler` Lambda que é iniciada após cada confirmação.
3. A `PipelinesStack` pilha cria os pipelines CodePipeline que são iniciados pela função Lambda. Cada microsserviço deve ter um pipeline de infraestrutura definido.

4. O pipeline para `microservice-n` é iniciado pela função Lambda e inicia seus estágios isolados de CI/CD baseados no código-fonte em. CodeCommit
5. O pipeline para `microservice-1` é iniciado pela função Lambda e inicia seus estágios isolados de CI/CD baseados no código-fonte em. CodeCommit

O diagrama a seguir mostra a implantação das AWS CloudFormation pilhas `MonoRepoStack` e `PipelinesStack` em uma conta.

1. Um usuário altera o código em um dos microsserviços do aplicativo.
2. O usuário envia as alterações de um repositório local para um CodeCommit repositório.
3. A atividade push inicia a função Lambda que recebe todos os push no repositório. CodeCommit
4. A função Lambda lê um parâmetro no Parameter Store, um recurso do AWS Systems Manager, para recuperar o ID de confirmação mais recente. O parâmetro tem o formato de nomenclatura:`/MonoRepoTrigger/{repository}/{branch_name}/LastCommit`. Se o parâmetro não for encontrado, a função Lambda lê o último ID de confirmação do CodeCommit repositório e salva o valor retornado no Parameter Store.
5. Depois de identificar o ID do commit e os arquivos alterados, a função Lambda identifica os pipelines para cada diretório de microsserviços e inicia o pipeline necessário. CodePipeline

Ferramentas

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software para definir a infraestrutura de nuvem em código e provisioná-la por meio dela. AWS CloudFormation
- Python é uma linguagem de programação que permite trabalhar com rapidez e integrar sistemas com mais eficiência.

Código

O código-fonte e os modelos desse padrão estão disponíveis no repositório de gatilhos multipipeline GitHub AWS CodeCommit monorepo.

Práticas recomendadas

- Esse exemplo de arquitetura não inclui uma solução de monitoramento para a infraestrutura implantada. Se você quiser implantar essa solução em um ambiente de produção, recomendamos

que você habilite o monitoramento. Para obter mais informações, consulte Monitore seus aplicativos sem servidor com o CloudWatch Application Insights na documentação AWS Serverless Application Model (AWS SAM).

- Ao editar o código de amostra fornecido por esse padrão, siga as melhores práticas para desenvolver e implantar a infraestrutura de nuvem na AWS CDK documentação.
- Ao definir seus pipelines de microsserviços, revise as melhores práticas de segurança na AWS CodePipeline documentação.
- Você também pode verificar as melhores práticas em seu AWS CDK código usando o utilitário cdk-nag. Essa ferramenta usa um conjunto de regras, agrupadas por pacotes, para avaliar seu código. Os pacotes disponíveis são:
  - AWS Biblioteca de soluções
  - Segurança da Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA)
  - Instituto Nacional de Padrões e Tecnologia (NIST) 800-53 rev 4
  - NIST 800-53 rev 5
  - Payment Card Industry Data Security Standard (PCI DSS) 3.2.1

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Crie um ambiente virtual Python.	Em seu AWS Cloud9 IDE, crie um ambiente virtual em Python e instale as dependências necessárias executando o seguinte comando: `make install`	Desenvolvedor
Inicialize o Conta da AWS e Região da AWS para o. AWS CDK	Inicialize o necessário Conta da AWS e a região executando o seguinte comando: `make bootstrap account-id=<your-`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`AWS-account-ID> region=<required-region>`	

Adicione um novo pipeline para um microsserviço

Tarefa	Descrição	Habilidades necessárias
Adicione seu código de amostra ao diretório do aplicativo.	Adicione o diretório que contém o código do aplicativo de amostra ao `monorepo-sample` diretório no repositório clonado de gatilhos de vários GitHub AWS CodeCommit pipelines monorepo.	Desenvolvedor
Edite o arquivo `monorepo-main.json` .	Adicione o nome do diretório do código do seu aplicativo e o nome do pipeline ao `monorepo-main.json` arquivo no repositório clonado.	Desenvolvedor
Criar o pipeline.	No `Pipelines` diretório do repositório, adicione o pipeline `class` do seu aplicativo. O diretório contém dois arquivos de amostra `pipeline_hotsite.py` `pipeline_demo.py` e. Cada arquivo tem três estágios: origem, criação e implantação. Você pode copiar um dos arquivos e alterá-lo de acordo	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	com os requisitos do seu aplicativo.	

Tarefa	Descrição	Habilidades necessárias

Edite o arquivo `monorepo_config.py` .	Em `service_map` , adicione o nome do diretório do seu aplicativo e a classe que você criou para o pipeline.
	
	Por exemplo, o código a seguir mostra uma definição de pipeline no diretório `Pipelines` que usa um arquivo nomeado `pipeline_mysample.py` com uma classe `MySamplePipeline` :
	
	`...`
	`# Pipeline definition imports`
	`from pipelines.pipeline_demo import DemoPipeline`
	`from pipelines.pipeline_hotsite import HotsitePipeline`
	`from pipelines.pipeline_mysample import MySamplePipeline`
	
	`### Add your pipeline configuration here`
	`service_map: Dict[str, ServicePipeline] = {`
	`# folder-name -> pipeline-class`
	`'demo': DemoPipeline(),`
	`'hotsite': HotsitePipeline(),`
	`'mysample': MySamplePipeline()`
		Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`}`	

Implante a MonoRepoStack pilha

Tarefa	Descrição	Habilidades necessárias
Implante a AWS CloudFormation pilha.	Implante a AWS CloudFormation `MonoRepoStack` pilha com valores de parâmetros padrão no diretório raiz do repositório clonado executando o comando. `make deploy-core` Você pode alterar o nome do repositório executando o comando `make deploy-core monorepo-name=<repo_name>` . **Note** Você pode implantar simultaneamente os dois pipelines usando o `make deploy monorepo-name=<repo_name>` comando.	Desenvolvedor
Valide o CodeCommit repositório.	Valide se seus recursos foram criados executando o comando `aws codecommit get-repository`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`--repository-name <repo_name>` . **Important** Como a AWS CloudFormation pilha cria o CodeCommit repositório em que o monorepo é armazenado, não execute o `cdk destroy MonoRepoStack` comando se você tiver começado a fazer modificações nele.	
Valide os resultados da AWS CloudFormation pilha.	Valide se a AWS CloudFormation `MonoRepoStack` pilha foi criada e configurada corretamente executando o seguinte comando: `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE --query 'StackSummaries[?StackName == 'MonoRepoStack']'`	Desenvolvedor

Implante a PipelinesStack pilha

Tarefa	Descrição	Habilidades necessárias
Implante a AWS CloudFormation pilha.	A AWS CloudFormation `PipelinesStack` pilha deve ser implantada após a implantação da `MonoRepoStack` pilha. A pilha aumenta de tamanho quando novos microsserviços são adicionados à base de código do monorepo e é reimplantada quando um novo microsserviço é integrado. Implante a PipelinesStack pilha executando o `make deploy-pipelines` comando. **Note** Você também pode implantar simultaneamente os dois pipelines executando o `make deploy monorepo-name=<repo_name>` comando. O exemplo de saída a seguir mostra como a `Pipelines Stacks` implantação imprime	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	URLs os microsserviços no final da implementação: `Outputs: PipelinesStack.dem ourl = .cloudfront.net PipelinesStack.hotsi teurl = .cloudfro nt.net`	
Valide os resultados da AWS CloudFormation pilha.	Valide se a AWS CloudForm ation `PipelinesStacks` pilha foi criada e configurada corretamente executando o seguinte comando: `aws cloudformation list-stacks --stack-s tatus-filter CREATE_CO MPLETE UPDATE_COMPLETE --query 'StackSum maries[?StackName == 'PipelinesStack']'`	Desenvolvedor

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Exclua suas AWS CloudForm ation pilhas.	Execute o comando `make destroy`.	Desenvolvedor
Exclua os buckets do S3 dos pipelines.	1. Faça login no console do Amazon Simple Storage Service (Amazon S3) AWS Management Consolee abra o console do Amazon	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Simple Storage Service (Amazon S3). 2. Exclua os buckets do S3 associados aos seus pipelines e use o seguinte nome: `pipelines stack-codepipeline *`	

Solução de problemas

Problema	Solução
Eu encontrei AWS CDK problemas.	Consulte Solução de AWS CDK problemas comuns na documentação do AWS CDK.
Eu enviei meu código de microsserviço, mas o pipeline de microsserviços não funcionou.	Validação da configuração Verifique a configuração da filial: • Verifique se você está enviando seu código para a ramificação correta. Esse pipeline é configurado para ser executado somente quando alterações são feitas na `main` ramificação. Os envios para outras ramificaç ões não iniciam o pipeline, a menos que estejam configurados especificamente. • Depois de enviar seu código, verifique se o commit está visível AWS CodeCommit para garantir que o push tenha sido bem-suced ido e que a conexão entre seu ambiente local e o repositório esteja intacta. Atualize suas credenciais se houver problemas ao enviar o código.

Problema	Solução
	Valide os arquivos de configuração: • Confirme se a `service_map` variável in reflete `monorepo_config.py` com precisão a estrutura atual de diretórios de seus microsserviços. Essa variável desempenha um papel crucial no mapeamento do envio de código para o respectivo pipeline. • Certifique-se de que `monorepo-main.json` esteja atualizado para incluir o novo mapeamento para seu microsser viço. Esse arquivo é essencial para que o pipeline reconheça e gerencie corretamente as alterações em seu microsserviço. Solução de problemas no console AWS CodePipeline verificações: • No AWS Management Console, confirme se você está no Região da AWS local onde seu funil está hospedado. Abra o CodePipel ine console e verifique se o pipeline que corresponde ao seu microsserviço foi iniciado. Análise de erros: se o pipeline foi iniciado, mas falhou, revise todas as mensagens de erro ou registros fornecidos pelo CodePipel ine para entender o que deu errado. AWS Lambda solução de problemas: • No AWS Lambda console, abra a função `monorepo-event-handler` Lambda.

Problema	Solução
	Verifique se a função foi iniciada em resposta ao envio do código. Análise de registros: examine os registros da função Lambda em busca de problemas . Os registros podem fornecer informações detalhadas sobre o que aconteceu quando a função foi executada e ajudar a identificar se a função processou o evento conforme o esperado.

Problema	Solução
Preciso reimplantar todos os meus microsser viços.	Há duas abordagens para forçar a reimplant ação de todos os microsserviços. Escolha a opção que atenda às suas necessidades. Abordagem 1: Excluir um parâmetro no Parameter Store Esse método envolve a exclusão de um parâmetro específico no Systems Manager Parameter Store que rastreia o último ID de confirmação usado para implantação. Quando você remove esse parâmetro, o sistema é forçado a reimplantar todos os microsserviços no próximo acionador, pois o percebe como um estado novo. Etapas: 1. Localize a entrada específica do Parameter Store que contém o ID de confirmação ou um marcador de implantação relacionado para seu monorepo. O nome do parâmetro segue o formato: `"/MonoRepoTrigger/{repository}/{branch_name}/LastCommit"` 2. Considere fazer backup do valor do parâmetro se ele for crítico ou se você quiser manter um registro do estado da implantaç ão antes de redefini-lo. 3. Use o AWS Management Console AWS CLI, ou SDKs para excluir o parâmetro identific ado. Essa ação redefine o marcador de implantação. 4. Após a exclusão, o próximo envio para o repositório deve fazer com que o sistema

Problema	Solução
	implante todos os microsserviços, pois ele procura a confirmação mais recente a ser considerada para implantação. Prós: • Simples e rápido de implementar com etapas mínimas. • Não é necessário fazer alterações arbitrárias no código para iniciar as implantações. Contras: • Controle menos granular sobre o processo de implantação. • Potencialmente arriscado se o Parameter Store for usado para gerenciar outras configurações críticas. Abordagem 2: Envie um commit em cada subpasta monorepo Esse método envolve fazer uma pequena alteração e colocá-la em cada subpasta de microsserviços dentro do monorepo para iniciar seus pipelines individuais. Etapas: 1. Liste todos os microsserviços dentro do monorepo que precisam ser reimplantados. 2. Para cada microsserviço, faça uma alteração mínima e sem impacto em sua subpasta. Isso pode ser atualizar um `README` arquivo, adicionar um comentário em um arquivo de

Problema	Solução
	configuração ou qualquer alteração que não afete a funcionalidade do serviço. 3. Confirme essas alterações com uma mensagem clara (como “Iniciar a reimplant ação de microsserviços”) e envie-as para o repositório. Certifique-se de enviar as alterações para a ramificação que inicia a implantação. 4. Monitore os pipelines de cada microsser viço para confirmar se eles foram iniciados e concluídos com êxito. Prós: • Fornece controle granular sobre quais microsserviços são reimplantados. • Mais seguro porque não envolve a exclusão de parâmetros de configuração que possam ser usados para outros fins. Contras: • Mais demorado, especialmente com um grande número de microsserviços. • Requer fazer alterações desnecessárias no código que podem bagunçar o histórico de confirmações.

Recursos relacionados

- Integração e entrega contínuas (CI/CD) usando CDK Pipelines (documentação)AWS CDK
- módulo aws-cdk/pipelines (referência de API)AWS CDK

Integre um repositório Bitbucket com o AWS Amplify usando a AWS CloudFormation

Criado por Alwin Abraham (AWS)

Resumo

O AWS Amplify ajuda você a implantar e testar rapidamente sites estáticos sem precisar configurar a infraestrutura que normalmente é necessária. Você pode implantar a abordagem desse padrão se sua organização quiser usar o Bitbucket para controle de origem, seja para migrar o código do aplicativo existente ou para criar um novo aplicativo. Ao usar CloudFormation a AWS para configurar automaticamente o Amplify, você fornece visibilidade das configurações que você usa.

Esse padrão descreve como criar um pipeline e um ambiente de implantação de integração contínua e implantação contínuas (CI/CD) de front-end usando a AWS CloudFormation para integrar um repositório Bitbucket ao AWS Amplify. A abordagem do padrão significa que você pode criar um pipeline de frontend do Amplify para implantações repetíveis.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS)
- Uma conta ativa do Bitbucket com acesso de administrador
- Acesso a um terminal que usa cURL ou o aplicativo Postman
- Familiaridade com o Amplify
- Familiaridade com a AWS CloudFormation
- Familiaridade com arquivos formatados em YAML

Arquitetura

Pilha de tecnologia

- Amplify
- AWS CloudFormation
- Bitbucket

Ferramentas

- AWS Amplify: o Amplify ajuda os desenvolvedores a desenvolverem e implantarem aplicativos móveis e web baseados na nuvem.
- AWS CloudFormation — CloudFormation A AWS é um serviço que ajuda você a modelar e configurar seus recursos da AWS para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos que são executados na AWS.
- Bitbucket: o Bitbucket é uma solução de gerenciamento de repositórios Git projetada para equipes profissionais. Ele oferece um local central para gerenciar repositórios Git, colaborar em seu código-fonte e guiá-lo pelo fluxo de desenvolvimento.

Código

O `bitbucket-amplify.yml` arquivo (anexado) contém o CloudFormation modelo da AWS para esse padrão.

Épicos

Configurar o repositório Bitbucket

Tarefa	Descrição	Habilidades necessárias
(Opcional) Criar um repositório do Bitbucket.	1. Faça login na sua conta do Bitbucket e crie um novo repositório. Para obter mais informações, consulte Criar um repositório Git na documentação do Bitbucket . 2. Registre o nome do espaço de trabalho.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Note Você também pode usar um repositório Bitbucket existente.	
Abra as configurações do espaço de trabalho.	1. Abra o espaço de trabalho e escolha a guia Repositório. 2. Escolha o repositório que você deseja usar no Amplify. 3. Escolha o nome do espaço de trabalho que está acima do nome do repositório. 4. Na barra lateral, escolha Configurações.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Crie um OAuth consumidor.	1. Na seção Aplicativos e recursos, escolha OAuth consumidores e, em seguida, escolha Adicionar consumidor. 2. Insira um nome para o seu consumidor, como por exemplo, `Amplify Integration .` 3. Insira um URL de retorno de chamada. Embora esse campo seja uma entrada obrigatória, ele não é usado para concluir a integração, portanto, o valor pode ser `http://localhost:3000` 4. Marque a caixa Este é um consumidor privado. 5. Selecione as seguintes permissões: • Projeto – `Read` • Repositórios – `Admin` • Solicitações pull – `Read` • Webhooks – `Read` e `Write` 6. Deixe as opções padrão para todos os outros campos e escolha Enviar. 7. Registre a chave e o segredo que são gerados.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Obtenha o token de OAuth acesso.	1. Abra uma janela de terminal e execute o seguinte comando: `curl -X POST -u "KEY:SECRET" https://bitbucket.org/site/oauth2/access_token -d grant_type=client_credentials` **Important** Substitua `KEY` e `SECRET` pela chave e o segredo que você gravou anteriormente. 2. Grave o token de acesso sem usar as aspas. O token só é válido por um tempo limitado e o tempo padrão é de duas horas. Você deve executar o CloudFormation modelo da AWS nesse período.	DevOps engenheiro

Crie e implante o AWS CloudFormation stack

Tarefa	Descrição	Habilidades necessárias
Baixe o CloudFormation modelo da AWS.	Baixe o CloudFormation modelo `bitbucket-`	

Tarefa	Descrição	Habilidades necessárias
	`amplify.yml` da AWS (em anexo). Esse modelo cria o pipeline de CI/CD no Amplify, além do projeto e da ramificação do Amplify.	

Tarefa	Descrição	Habilidades necessárias
Crie e implante o AWS CloudFormation stack.	1. Faça login no Console de Gerenciamento da AWS na região da AWS em que você deseja implantar e abra o CloudFormation console da AWS. 2. Selecione Criar pilha (com novos recursos) e selecione Fazer upload de um arquivo de modelo. 3. Carregue o arquivo `bitbucket-amplify.yml` . 4. Escolha Próximo, insira o nome da pilha e, após, insira os seguintes parâmetros: • Token de acesso: cole o token de OAuth acesso que você criou anteriormente. • URL do repositório: adicione o URL do repositório do projeto Bitbucket. O URL tipicamente é no seguinte formato: `https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` • Nome da ramificação: deve corresponder ao nome de uma ramificaç	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ão no seu repositório do Bitbucket. Essa ramificaç ão não precisa existir quando você executa a CloudFormation pilha da AWS, mas é necessária para implantar código no ambiente. • Nome do projeto: Esse é o nome a ser associado ao projeto Amplify. 5. Escolha Próximo e, em seguida, Criar pilha.	

Testar o pipeline de CI/CD

Tarefa	Descrição	Habilidades necessárias
Implantar o código na ramificação do seu repositório.	1. Clone seu repositório Bitbucket executando o seguinte comando: `git clone https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` 2. Confira o nome da filial que foi usado ao executar o CloudFormation script da AWS. Para criar e verificar uma nova ramificaç ão, execute o comando `git checkout -b`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`<BRANCH_NAME>` . Para verificar uma ramificaç ão existente, execute o comando `git checkout <BRANCH_NAME>` 3. Confirme o código na ramificação e envie-o para a ramificação remota executando os comandos `git commit` e `git push`. 4. Em seguida, o Amplify cria e implanta o aplicativo. Para obter mais informações, consulte Comandos básicos do Git na documentação do Bitbucket.	

Recursos relacionados

Métodos de autenticação (documentação da Atlassian)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Lance um CodeBuild projeto em várias contas da AWS usando Step Functions e uma função de proxy Lambda

Criado por Richard Milner-Watts (AWS) e Amit Anjarlekar (AWS)

Resumo

Esse padrão demonstra como iniciar de forma assíncrona um projeto da AWS CodeBuild em várias contas da AWS usando o AWS Step Functions e uma função de proxy do AWS Lambda. Você pode usar a máquina de estado Step Functions de amostra do padrão para testar o sucesso do seu CodeBuild projeto.

CodeBuild ajuda você a iniciar tarefas operacionais usando a AWS Command Line Interface (AWS CLI) a partir de um ambiente de tempo de execução totalmente gerenciado. Você pode alterar o comportamento do seu CodeBuild projeto em tempo de execução substituindo as variáveis de ambiente. Além disso, você pode usar CodeBuild para gerenciar fluxos de trabalho. Para obter mais informações, consulte Service Catalog Tools no site do AWS Workshop e agende trabalhos no Amazon RDS for PostgreSQL usando a AWS e a EventBridge Amazon no blog do banco de dados CodeBuild da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Duas contas ativas da AWS: uma conta de origem para invocar uma função de proxy Lambda com Step Functions e uma conta de destino para criar um CodeBuild projeto de amostra remoto

Limitações

- Esse padrão não pode ser usado para copiar artefatos entre contas.

Arquitetura

O diagrama a seguir mostra a arquitetura que esse padrão cria.

O diagrama mostra o seguinte fluxo de trabalho:

1. A máquina de estado do Step Functions analisa o mapa de entrada fornecido e invoca a função de proxy do Lambda (`codebuild-proxy-lambda`) para cada conta, região e projeto que você definiu.
2. A função de proxy Lambda usa o AWS Security Token Service (AWS STS) para assumir uma função de proxy do IAM (`codebuild-proxy-role`), que está associada a uma política do IAM (`codebuild-proxy-policy`) na conta de destino.
3. Usando a função assumida, a função Lambda inicia o CodeBuild projeto e retorna o ID do CodeBuild trabalho. A máquina de estado do Step Functions faz um loop e pesquisa a CodeBuild tarefa até receber um status de sucesso ou falha.

A lógica da máquina de estados é mostrada na imagem a seguir.

Pilha de tecnologia

- AWS CloudFormation
- CodeBuild
- IAM
- Lambda
- Step Functions
- X-Ray

Ferramentas

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- O AWS CloudFormation Designer fornece um editor JSON e YAML integrado que ajuda você a visualizar e editar CloudFormation modelos.
- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando

necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

- O AWS Step Functions é um serviço de orquestração com tecnologia sem servidor que permite combinar funções do AWS Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios.
- O AWS X-Ray ajuda a coletar dados sobre solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informações sobre esses dados para identificar problemas e oportunidades de otimização.

Código

O código de amostra desse padrão está disponível no repositório GitHub Cross Account CodeBuild Proxy. Esse padrão usa a biblioteca AWS Lambda Powertools for Python para fornecer funcionalidade de registro e rastreamento. Para obter mais informações sobre essa biblioteca e seus utilitários, consulte Powertools para AWS Lambda (Python).

Práticas recomendadas

1. Ajuste os valores do tempo de espera na máquina de estado da Step Function para minimizar as solicitações de pesquisa sobre o status do trabalho. Use o tempo de execução esperado para o CodeBuild projeto.
2. Ajuste a `MaxConcurrency` propriedade do mapa em Step Functions para controlar quantos CodeBuild projetos podem ser executados em paralelo.
3. Se necessário, revise o código de amostra para verificar se a produção está pronta. Considere quais dados podem ser registrados pela solução e se a CloudWatch criptografia padrão da Amazon é suficiente.

Épicos

Crie a função de proxy Lambda e o perfil do IAM associada na conta de origem

Tarefa	Descrição	Habilidades necessárias
Registre a conta da AWS IDs.	A conta IDs da AWS é necessária para configurar o acesso entre contas.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Registre a ID da conta da AWS para suas contas de origem e destino. Para obter mais informações, consulte Como encontrar a ID da conta da AWS na documentação do IAM.	

Tarefa	Descrição	Habilidades necessárias
Baixe os CloudFormation modelos da AWS.	1. Faça o download do CloudFormation modelo da `sample_target_codebuild_template.yaml` AWS do GitHub repositório para esse padrão. 2. Faça o download do CloudFormation modelo da `codebuild_lambda_proxy_template.yaml` AWS do GitHub repositório para esse padrão. **Note** Nos CloudFormation modelos da AWS, `<SourceAccountId>` é o ID da conta da AWS para a conta de origem e `<TargetAccountId>` é o ID da conta da AWS para a conta de destino.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Crie e implante o AWS CloudFormation stack.	1. Faça login no Console de Gerenciamento da AWS para obter sua conta de origem, abra o CloudFormation console da AWS e escolha Stacks. 2. Selecione Create stack (Criar pilha) e With new resources (standard) (Com novos recursos, padrão). 3. Para Template source (Origem do template), escolha Upload a template file (Fazer upload de um arquivo de template). 4. Em Carregar um arquivo de modelo, escolha arquivo e, em seguida, escolha o arquivo `codebuild_lambda_proxy_template.yaml` baixado. Escolha Próximo. 5. Em Nome da pilha, insira um nome para a pilha (por exemplo, `codebuild-lambda-proxy`). 6. **Note** Substitua o parâmetro `crossAccountTargetRoleArn` por seu `<TargetAc`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`countId>` (por exemplo, `<arn:aws:iam::123456789012:role/proxy-lambda-codebuild-role>`). : você não precisa atualizar o valor padrão do **`targetCodeBuildProject`** parâmetro. 7. Escolha Avançar, aceite as opções padrão de criação de pilha e escolha Avançar. 8. Escolha a caixa de seleção Eu reconheço que a AWS CloudFormation pode criar recursos do IAM com nomes personalizados e, em seguida, escolha Criar pilha. **Note** Você deve criar a CloudFormation pilha da AWS para a função proxy Lambda antes de criar qualquer recurso nas contas	

Tarefa	Descrição	Habilidades necessárias
	de destino. Quando você cria uma política de confiança em uma conta de destino, o perfil do IAM é traduzida do nome da função para um identificador interno. É por isso que o perfil do IAM já deve existir.	
Confirme a criação da função proxy e da máquina de estado.	1. Aguarde até que a CloudFormation pilha da AWS alcance o status CREATE_COMPLETE. Isso deve levar menos de um minuto. 2. Abra o console do AWS Lambda, selecione sua Functions (Funções) e encontre `alambda-proxy-ProxyLambda-<GUID>` função. 3. Abra o console do AWS Step Functions, escolha as máquinas de estado e, em seguida, localize a máquina de estado `sample-crossaccount-codebuild-state-machine` .	AWS DevOps

Crie uma função do IAM na conta de destino e lance um CodeBuild projeto de amostra

Tarefa	Descrição	Habilidades necessárias
Crie e implante o AWS CloudFormation stack.	1. Faça login no AWS Management Console da sua conta de destino, abra o CloudFormation console da AWS e escolha Stacks. 2. Selecione Create stack (Criar pilha) e With new resources (standard) (Com novos recursos, padrão). 3. Para Template source (Origem do template), escolha Upload a template file (Fazer upload de um arquivo de template). 4. Em Carregar um arquivo de modelo, escolha Escolher arquivo e, em seguida, escolha o arquivo `sample_target_codebuild_template.yaml` . Escolha Próximo. 5. Em Nome da pilha, insira um nome para a pilha (por exemplo: `sample-codebuild-stack`). 6. Substitua o parâmetro `crossAccountSourceRoleArn` por seu `<SourceAccountId>` (por exemplo, `<arn:aws:iam::123456789012:role/code`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`build-proxy-lambda-role>`). 7. Escolha Avançar, aceite as opções padrão de criação de pilha e escolha Avançar. 8. Escolha a caixa de seleção Eu reconheço que a AWS CloudFormation pode criar recursos do IAM com nomes personalizados e, em seguida, escolha Criar pilha.	
Verifique a criação do CodeBuild projeto de amostra.	1. Aguarde até que a CloudFormation pilha da AWS alcance o status CREATE_COMPLETE. Isso deve levar menos de um minuto. 2. Abra o CodeBuild console da AWS e encontre o `sample-codebuild-project` projeto.	AWS DevOps

Teste a função de proxy do Lambda entre contas do Lambda

Tarefa	Descrição	Habilidades necessárias
Inicie a máquina de estado.	1. Faça login no Console de Gerenciamento da AWS para obter sua conta de origem, abra o console do AWS Step Functions	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	e escolha Máquinas de estado. 2. Escolha a máquina de estado `sample-crossaccount-codebuild-state-machine` e, em seguida, escolha Iniciar execução. 3. No editor de entrada, insira o seguinte JSON e substitua `<TargetAccountID>` pelo ID da conta da AWS da conta que contém o CodeBuild projeto. `{ "crossAccountTargetRoleArns": [ { "arn": "arn:aws:iam::<TargetAccountID>:role/proxy-lambda-codebuild-role", "region": "eu-west-1", "codeBuildProject": "sample-codebuild-project", "SampleValue1": "Value1", "SampleValue2": "Value2" } ] }`	

Tarefa	Descrição	Habilidades necessárias
	Note Os pares de valores-chave são passados como variáveis de ambiente da função na conta de origem para o CodeBuild projeto na conta de destino. 4. Selecione Iniciar execução. 5. Na guia Detalhes da página da máquina de estado, verifique se o Status de execução está definido como Bem-sucedido. Isso confirma que sua máquina de estado está em execução. Nota: pode levar cerca de 30 segundos para que a máquina de estado alcance o status Bem-sucedido. 6. Para ver a saída e a entrada de uma etapa na máquina de estado, expanda essa etapa na seção Histórico de eventos de execução. Por exemplo, expanda a etapa Lambda - CodeBuild Proxy — Start. A saída inclui detalhes	

Tarefa	Descrição	Habilidades necessárias
	sobre as variáveis de ambiente substituídas, a carga original e o ID do CodeBuild trabalho.	
Valide as variáveis de ambiente.	1. Faça login no Console de Gerenciamento da AWS para sua conta de destino. 2. Abra o CodeBuild console da AWS, expanda Build e escolha Build projects. 3. Escolha o `sample-codebuild-project` projeto e, em seguida, escolha Exibir detalhes. 4. Na guia Histórico de compilação, escolha a compilação mais recente do projeto e, em seguida, escolha Exibir registros. 5. Na saída de logs, verifique se as variáveis de ambiente impressas em STDOUT correspondem às variáveis de ambiente da máquina de estado de amostra do Step Functions.	AWS DevOps

Solução de problemas

Problema	Solução
A execução do Step Functions está demorando mais do que o esperado.	Ajuste a `MaxConcurrency` propriedade do mapa na máquina de estado da Step Function

Problema	Solução
	para controlar quantos CodeBuild projetos podem ser executados paralelamente.
A execução dos CodeBuild trabalhos está demorando mais do que o esperado.	1. Ajuste os valores do tempo de espera na máquina de estado Step Functions para minimizar as solicitações de pesquisa sobre o status do trabalho. Use o tempo de execução esperado para o CodeBuild projeto. 2. Considere se CodeBuild é a ferrament a apropriada a ser usada. Por exemplo, o tempo necessário para inicializar um CodeBuild trabalho pode ser significa tivamente maior do que o AWS Lambda. Se for necessário um alto rendimento e tempos de conclusão rápidos, considere migrar a lógica de negócios para o AWS Lambda e usar uma arquitetura fan-out.

Gerencie o failover Multi-AZ para clusters do EMR usando o Application Recovery Controller

Criado por Aarti Rajput (AWS), Ashish Bhatt (AWS), Neeti Mishra (AWS) e Nidhi Sharma (AWS)

Resumo

Esse padrão oferece uma estratégia eficiente de recuperação de desastres para cargas de trabalho do Amazon EMR para ajudar a garantir a alta disponibilidade e a consistência dos dados em várias zonas de disponibilidade em uma única. Região da AWS O design usa o Amazon Application Recovery Controller e um Application Load Balancer para gerenciar operações de failover e distribuição de tráfego para um cluster EMR baseado em Apache Spark.

Sob condições padrão, a zona de disponibilidade principal hospeda um cluster e um aplicativo EMR ativos com funcionalidade completa de leitura/gravação. Se uma zona de disponibilidade falhar inesperadamente, o tráfego será redirecionado automaticamente para a zona de disponibilidade secundária, onde um novo cluster do EMR será lançado. Ambas as zonas de disponibilidade acessam um bucket compartilhado do Amazon Simple Storage Service (Amazon S3) por meio de endpoints de gateway dedicados, que garantem o gerenciamento consistente dos dados. Essa abordagem minimiza o tempo de inatividade e permite a recuperação rápida de cargas de trabalho críticas de big data durante falhas na zona de disponibilidade. A solução é útil em setores como finanças ou varejo, onde análises em tempo real são cruciais.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Amazon EMR na Amazon Elastic Compute Cloud (Amazon) EC2
- Acesso do nó principal do cluster do EMR ao Amazon S3.
- AWS Infraestrutura Multi-AZ

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Versões do produto

- Amazon EMR 6.x e versões posteriores

Arquitetura

Pilha de tecnologias de destino

- Cluster Amazon EMR
- Amazon Application Recovery Controller
- Application Load Balancer
- Bucket do Amazon S3
- Endpoints de gateway para o Amazon S3

Arquitetura de destino

Essa arquitetura fornece resiliência ao aplicativo usando várias zonas de disponibilidade e implementando um mecanismo de recuperação automatizado por meio do Controlador de Recuperação de Aplicativos.

1. O Application Load Balancer roteia o tráfego para o ambiente ativo do Amazon EMR, que normalmente é o cluster principal do EMR na zona de disponibilidade primária.
2. O cluster ativo do EMR processa as solicitações do aplicativo e se conecta ao Amazon S3 por meio de seu endpoint de gateway Amazon S3 dedicado para operações de leitura e gravação.
3. O Amazon S3 serve como um repositório central de dados e é potencialmente usado como um ponto de verificação ou como armazenamento compartilhado entre clusters do EMR. Os clusters do EMR mantêm a consistência dos dados quando gravam diretamente no Amazon S3 por meio `s3://` do protocolo e do EMR File System (EMRFS).
4. O Application Recovery Controller monitora continuamente a integridade da zona de disponibilidade principal e gerencia automaticamente as operações de failover quando necessário.
5. Se o Application Recovery Controller detectar uma falha no cluster primário do EMR, ele executará as seguintes ações:
   - Inicia o processo de failover para o cluster EMR secundário na Zona de Disponibilidade 2.
   - Atualiza as configurações de roteamento para direcionar o tráfego para o cluster secundário.

Ferramentas

Serviços da AWS

- O Amazon Application Recovery Controller ajuda você a gerenciar e coordenar a recuperação de seus aplicativos em todas Regiões da AWS as zonas de disponibilidade. Esse serviço simplifica o processo e melhora a confiabilidade da recuperação de aplicativos ao reduzir as etapas manuais exigidas pelas ferramentas e processos tradicionais.
- O Application Load Balancer opera na camada do aplicativo, que é a sétima camada do modelo Open Systems Interconnection (OSI). Ele distribui o tráfego de entrada do aplicativo em vários destinos, como EC2 instâncias, em várias zonas de disponibilidade. Isso aumenta a disponibilidade do seu aplicativo.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- O Amazon EMR é uma plataforma de big data que fornece processamento de dados, análise interativa e aprendizado de máquina para estruturas de código aberto, como Apache Spark, Apache Hive e Presto.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon S3 fornece uma interface de serviço web simples que você pode usar para armazenar e recuperar qualquer quantidade de dados, a qualquer momento, de qualquer lugar. Usando esse serviço, você pode criar facilmente aplicativos que usam armazenamento nativo em nuvem.
- Os endpoints de gateway para o Amazon S3 são gateways que você especifica em sua tabela de rotas para acessar o Amazon S3 a partir da sua nuvem privada virtual (VPC) pela rede. AWS

Práticas recomendadas

- Siga as AWS melhores práticas de segurança, identidade e conformidade para garantir uma arquitetura robusta e segura.
- Alinhe a arquitetura com o AWS Well-Architected Framework.
- Use o Amazon S3 Access Grants para gerenciar o acesso do seu cluster EMR baseado em Spark ao Amazon S3. Para obter detalhes, consulte a postagem do blog Use o Amazon EMR com concessões de acesso do S3 para escalar o acesso do Spark ao Amazon S3.
- Melhore o desempenho do Spark com o Amazon S3.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Faça login no AWS Management Console.	Faça login no AWS Management Consolecomo usuário do IAM. Para obter instruções, consulte a AWS documentação.	AWS DevOps
Configure AWS CLI o.	Instale o AWS CLI ou atualize-o para a versão mais recente para que você possa interagir com Serviços da AWS AWS Management Console o. Para obter instruções, consulte a AWS CLI documentação.	AWS DevOps

Implante um aplicativo Spark em seu cluster EMR

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	1. Crie um bucket S3 para armazenar o conjunto de dados de entrada, os registros, o aplicativo e os dados de saída. Para obter instruções, consulte a documentação do Amazon S3. 2. Organize o bucket em pastas separadas para dados de entrada (`dataset`), logs (`logs`),	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	aplicativo Spark (`spark-app `) e dados de saída (`output`).	

Tarefa	Descrição	Habilidades necessárias

Crie um cluster EMR.	1. Use os AWS CLI comandos a seguir para criar um cluster do EMR (por exemplo, versão 6.12 ou posterior) com instâncias que abrangem duas zonas de disponibilidade (como `us-east-1a` e `us-east-1b`) para alta disponibilidade. O comando especifica o tipo de `m4.large` instância como exemplo.
	
	`aws emr create-cluster \ --ec2-attributes AvailabilityZone=<AZ-name-1> \ --release-label emr-6.12.0 \ --instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE,InstanceCount=2,InstanceType=m4.large`
	
	`aws emr create-cluster \ --ec2-attributes AvailabilityZone=<AZ-name-2> \ --release-label emr-6.12.0 \`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`--instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE,InstanceCount=2,InstanceType=m4.large` Para obter mais informações, consulte o comando create-cluster e a documentação do Amazon EMR. 2. Forneça ao par de chaves, à função de serviço e ao perfil da instância as permissões necessárias, conforme necessário.	

Tarefa	Descrição	Habilidades necessárias
Defina as configurações de segurança para o cluster do EMR.	1. Identifique o grupo de segurança associado ao nó principal do cluster do EMR usando o comando AWS CLI describe-cluster: `aws emr describe-cluster --cluster-id j-XXXXXXXX` 2. Para aumentar a segurança, modifique as configurações do grupo de segurança para permitir o acesso SSH (porta TCP 22) ao nó principal, mas restrinja-o ao seu endereço IP específico. Para obter mais informações, consulte a documentação do Amazon EMR.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Conecte-se ao cluster do EMR.	Conecte-se ao nó principal do cluster EMR por meio de SSH usando o par de chaves fornecido.
	
	Certifique-se de que o arquivo de key pair esteja presente no mesmo diretório do seu aplicativo.
	
	Execute os comandos a seguir para definir as permissões corretas para o key pair e estabelecer a conexão SSH:
	
	`chmod 400 <key-pair-name>`
	`ssh -i ./<key-pair-name> hadoop@<master-node-public-dns>`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Implante o aplicativo Spark.	Depois de estabelecer a conexão SSH, você estará no console do Hadoop.
	
	1. Crie ou edite o arquivo do aplicativo Spark (`main.py`) usando um editor de texto como o vim:
	
	`vim main.py`
	
	Para obter mais informaçõ es sobre como criar e modificar o aplicativo Spark, consulte a documentação do Amazon EMR.
	2. Envie o aplicativo Spark para o cluster do EMR, especificando os dados de entrada e os locais dos dados de saída no bucket do S3:
	
	`spark-submit main.py –data_source <input-data-folder-in-s3> –output_uri <output-folder-in-s3>`
	
	Aqui está um exemplo baseado nas pastas que você configurou anteriorm ente:
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`spark-submit main.py –data_source dataset –output_uri output`
	3. Monitore o progresso do aplicativo verificando os registros do aplicativo:
	`yarn logs -applicationId <application-id>`	

Monitore o aplicativo Spark.	1. Abra outra janela de terminal e estabeleça um túnel SSH para a interface web do gerenciador de recursos do cluster EMR: `ssh -i <key-pair-name> -N -L 8157:<resource-manager-public-dns>:8088 hadoop@<resource-manager-public-dns>` 2. Para monitorar o aplicativo, acesse a interface do usuário da web do gerenciador de recursos navegando até `http://localhost:8157` seu navegador da web.	AWS DevOps

Transferir o tráfego para outra zona de disponibilidade

Tarefa	Descrição	Habilidades necessárias
Criar um Application Load Balancer.	Configure o grupo-alvo que roteia o tráfego entre os nós principais do Amazon EMR que são implantados em duas zonas de disponibilidade em uma. Região da AWS Para obter instruções, consulte Criar um grupo-alvo para seu Application Load Balancer na documentação do Elastic Load Balancing.	AWS DevOps
Configure a mudança zonal no Application Recovery Controller.	Nesta etapa, você usará o recurso de mudança de zona no Application Recovery Controller para transferir o tráfego para outra zona de disponibilidade. 1. Abra o console do Application Recovery Controller. 2. Em Introdução, escolha Mudança zonal, Iniciar mudança zonal. 3. Selecione a zona de disponibilidade da qual você deseja afastar o tráfego. 4. Selecione um recurso compatível (por exemplo, Application Load Balancer)	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	para a mudança de zona na tabela Resources. 5. Em Definir expiração da mudança de zona, escolha ou insira uma expiração para a mudança de zona. Você pode definir uma duração entre 1 minuto e três dias (72 horas). Todas as mudanças de zona são temporárias. Você deve definir uma expiração , mas pode atualizar as mudanças ativas posterior mente para definir um novo período de expiração de até três dias. 6. Insira um comentário sobre essa mudança de zona. 7. Marque a caixa de seleção para reconhecer que iniciar uma mudança de zona reduzirá a capacidad e disponível para seu aplicativo ao afastar o tráfego da zona de disponibilidade. 8. Escolha Iniciar. Para usar o AWS CLI, consulte Exemplos de uso do AWS CLI com mudança zonal	

Tarefa	Descrição	Habilidades necessárias
	na documentação do Application Recovery Controller.	

Tarefa	Descrição	Habilidades necessárias

Verifique a configuração e o progresso do turno zonal.	1. Verifique os recursos que estão registrados com o deslocamento zonal:
	`aws arc-zonal-shift list-managed-resources --region <AWS-region-name>`
	Por exemplo, a saída a seguir confirma que os recursos estão funcionando em ambas as zonas de disponibilidade.
	`"appliedWeights": { "use1-az1": 1.0, "use1-az2": 1.0 },`
	2. Para visualizar o deslocamento zonal, use o AWS CLI comando a seguir para iniciar o deslocamento zonal:
	`aws arc-zonal-shift start-zonal-shift \ --resource-identifier <application-load-balancer-arn> \ --away-from <source-AZ> \ --expires-in 10m --comment "testing" \`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>--region <AWS-regi
	on-name></pre>
	onde <source-AZ> é o identificador da zona de disponibilidade da qual você deseja afastar o tráfego e <application-load-balancer-arn> é o Amazon Resource Name (ARN) do seu Application Load Balancer.
	3. Verifique se o tráfego foi transferido para outra zona de disponibilidade.
	<pre>aws arc-zonal-shift
	get-managed-resour
	ce \
	--resource-identif
	ier <application-
	load-balancer-arn> \
	--region <AWS-regi
	on-name></pre>
	Você pode ver a mudança zonal confirmada por esses pesos:
	<pre>"appliedWeights": {
	"use1-az1":
	0.0,
	"use1-az2":
	1.0
	},</pre>	

Recursos relacionados

- AWS CLI comandos:
  - create-cluster
  - describe-cluster
  - arc-zonal-shift
- Configurando os tipos de instância de cluster do Amazon EMR e as melhores práticas para instâncias spot (documentação do Amazon EMR)
- Práticas recomendadas de segurança no IAM (documentação do IAM)
- Use perfis de instância (documentação do IAM)
- Use o deslocamento zonal e o deslocamento automático zonal para recuperar aplicativos no ARC (documentação do Application Recovery Controller)

Gerencie implantações azul/verdes de microsserviços em várias contas e regiões usando os serviços de código da AWS e as chaves multirregionais do AWS KMS

Criado por Balaji Vedagiri (AWS), Ashish Kumar (AWS), Faisal Shahdad (AWS), Anand Krishna Varanasi (AWS), Vanitha Dontireddy (AWS) e Vivek Thangamuthu (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão descreve como implantar um aplicativo global de microsserviços de uma conta central da AWS para várias contas de workload e regiões, de acordo com uma estratégia de implantação azul/verde. O padrão suporta o seguinte:

- O software é desenvolvido em uma conta central, enquanto as workloads e os aplicativos estão espalhados por várias contas e regiões da AWS.
- Uma única chave multirregional do AWS Key Management System (AWS KMS) é usada para criptografia e descriptografia para abranger a recuperação de desastres.
- A chave KMS é específica da região e precisa ser mantida ou criada em três regiões diferentes para artefatos do pipeline. Uma chave multirregional do KMS ajuda a manter a mesma ID de chave em todas as regiões.
- O modelo de ramificação do fluxo de trabalho do Git é implementado com duas ramificações (desenvolvimento e principal) e o código é mesclado usando pull requests (). PRs A função do AWS Lambda que é implantada a partir dessa pilha cria um PR da ramificação de desenvolvimento para a ramificação principal. A fusão de relações públicas com a filial principal inicia um CodePipeline pipeline da AWS, que orquestra o fluxo de integração contínua e entrega contínua (CI/CD) e implanta as pilhas em todas as contas.

Esse padrão fornece um exemplo de configuração de infraestrutura como código (IaC) por meio de CloudFormation pilhas da AWS para demonstrar esse caso de uso. A implantação azul/verde de microsserviços é implementada usando a AWS. CodeDeploy

Pré-requisitos e limitações

Pré-requisitos

- Quatro contas ativas da AWS:
  - Uma conta de ferramentas para gerenciar o pipeline de código e manter o CodeCommit repositório da AWS.
  - Três contas de workload (teste) para implantar a workload de microsserviços.
- Esse padrão usa as seguintes regiões. Se quiser usar outras regiões, você deve fazer as modificações apropriadas nas pilhas multirregionais da AWS CodeDeploy e do AWS KMS.
  - Conta de ferramentas (AWS CodeCommit): `ap-south-1`
  - Conta de workload (teste) 1: `ap-south-1`
  - Conta de workload (teste) 2: `eu-central-1`
  - Conta de workload (teste) 3: `us-east-1`
- Três buckets do Amazon Simple Storage Service (Amazon S3) para as regiões de implantação em cada conta de workload. (Eles são chamados `S3BUCKETNAMETESTACCOUNT1`, `S3BUCKETNAMETESTACCOUNT2` e `S3BUCKETNAMETESTACCOUNT3` posteriormente, nesse padrão.)

  Por exemplo, você pode criar esses buckets em contas e regiões específicas com nomes de bucket exclusivos da seguinte forma (substitua xxxx por um número aleatório):

```
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-xxxx-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-xxxx-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-xxxx-us-east-1 --region us-east-1

#Example
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-18903-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-18903-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-18903-us-east-1 --region us-east-1
```

Limitações

O padrão usa a AWS CodeBuild e outros arquivos de configuração para implantar um microsserviço de amostra. Se você tiver um tipo de workload diferente (por exemplo, tecnologia sem servidor), deverá atualizar todas as configurações relevantes.

Arquitetura

Pilha de tecnologias de destino

- AWS CloudFormation
- AWS CodeCommit
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline

Arquitetura de destino

Automação e escala

A configuração é automatizada usando modelos de CloudFormation pilha da AWS (IaC). Ele pode ser facilmente escalado para vários ambientes e contas.

Ferramentas

Serviços da AWS

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- A AWS CodeDeploy automatiza implantações no Amazon Elastic Compute Cloud (Amazon EC2) ou em instâncias locais, funções do AWS Lambda ou serviços Amazon Elastic Container Service (Amazon ECS).

- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Ferramentas adicionais

- O Git é um sistema de controle de versão distribuído e de código aberto que funciona com o repositório da AWS. CodeCommit
- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres. Esse padrão usa o Docker para compilar e testar imagens de contêiner localmente.
- cfn-lint e cfn-nag são ferramentas de código aberto que ajudam você a analisar as CloudFormation pilhas em busca de erros e problemas de segurança.

Repositório de código

O código desse padrão está disponível nas implantações GitHub globais azul/verde em várias regiões e no repositório de contas.

Épicos

Definição de variáveis de ambiente

Tarefa	Descrição	Habilidades necessárias

Exporte variáveis de ambiente para implantação CloudFormation de pilha.	Defina as variáveis de ambiente que serão usadas como entrada para as CloudFormation pilhas posteriormente nesse padrão.
	1. Atualize os nomes dos buckets que você criou nas três contas e regiões, conforme explicado anteriormente na seção Pré-requisitos:
	`export S3BUCKETNAMETESTACCOUNT1=<S3BUCKETACCOUNT1>`
	`export S3BUCKETNAMETESTACCOUNT2=<S3BUCKETACCOUNT2>`
	`export S3BUCKETNAMETESTACCOUNT3=<S3BUCKETACCOUNT3>`
	2. Defina uma string aleatória para criar buckets de artefatos, pois os nomes dos buckets devem ser exclusivos globalmente:
	`export BUCKETSTARTNAME=ecs-codepipeline-artifacts-19992`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	3. Defina e exporte a conta IDs e as regiões:
	
	`export TOOLSACCOUNT=<TOOLSACCOUNT>`
	`export CODECOMMITACCOUNT=<CODECOMMITACCOUNT>`
	`export CODECOMMITREGION=ap-south-1`
	`export CODECOMMITREPONAME=Poc`
	`export TESTACCOUNT1=<TESTACCOUNT1>`
	`export TESTACCOUNT2=<TESTACCOUNT2>`
	`export TESTACCOUNT3=<TESTACCOUNT3>`
	`export TESTACCOUNT1REGION=ap-south-1`
	`export TESTACCOUNT2REGION=eu-central-1`
	`export TESTACCOUNT3REGION=us-east-1`
	`export TOOLSACCOUNTREGION=ap-south-1`
	`export ECRREPOSITORYNAME=web`	

Package e implemente as CloudFormation pilhas para a infraestrutura

Tarefa	Descrição	Habilidades necessárias

Clonar o repositório.	Clone o repositório de amostra em um novo repositório em seu local de trabalho:
	`##In work location`
	`git clone https://github.com/aws-samples/ecs-blue-green-global-deployment-with-multiregion-cmk-codepipeline.git`
		AWS DevOps

Empacote os recursos do Cloudformation.	Nesta etapa, você empacota os artefatos locais aos quais os CloudFormation modelos fazem referência para criar os recursos de infraestrutura necessários para serviços como Amazon Virtual Private Cloud (Amazon VPC) e Application Load Balancer.
	Os modelos estão disponíveis na pasta `Infra` do repositório de código.
	`##In TestAccount1##`
	`aws cloudformation package \`
	`--template-file mainInfraStack.yaml \`
	`--s3-bucket $S3BUCKETNAMETESTACCOUNT1 \`
	`--s3-prefix infraStack \`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	--region $TESTACCO UNT1REGION \ --output-template- file infrastructure_ ${TESTACCOUNT1}.templ ate ##In TestAccount2## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTA CCOUNT2 \ --s3-prefix infraStack \ --region $TESTACCO UNT2REGION \ --output-template- file infrastructure_ ${TESTACCOUNT2}.templ ate ##In TestAccount3## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTA CCOUNT3 \ --s3-prefix infraStack \ --region $TESTACCO UNT3REGION \ --output-template- file infrastructure_	

Tarefa	Descrição	Habilidades necessárias
	`${TESTACCOUNT3}.templ ate`	

Valide os modelos de pacote.	Valide os modelos de pacote:
	`aws cloudformation validate-template \ --template-body file://infrastruct ure_${TESTACCOUNT1 }.template`
	
	`aws cloudformation validate-template \ --template-body file://infrastruct ure_${TESTACCOUNT2 }.template`
	
	`aws cloudformation validate-template \ --template-body file://infrastruct ure_${TESTACCOUNT3 }.template`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Implante os arquivos do pacote nas contas de workload,	1. Atualize os valores dos espaços reservados e os nomes das contas no script `infraParameters.json` com base na sua configuração.
	2. Implante os modelos de pacote em suas três contas de workload.
	
	`##In TestAccount1##`
	`aws cloudformation deploy \`
	`--template-file infrastructure_${TESTACCOUNT1}.template \`
	`--stack-name mainInfrastack \`
	`--parameter-overrides file://infraParameters.json \`
	`--region $TESTACCOUNT1REGION \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`
	
	`##In TestAccount2##`
	`aws cloudformation deploy \`
	`--template-file infrastructure_${TESTACCOUNT2}.template \`
	`--stack-name mainInfrastack \`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`--parameter-overrides file://infraParameters.json \ --region $TESTACCOUNT2REGION \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`
	
	`##In TestAccount3## aws cloudformation deploy \ --template-file infrastructure_${TESTACCOUNT3}.template \ --stack-name mainInfrastack \ --parameter-overrides file://infraParameters.json \ --region $TESTACCOUNT3REGION \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`	

Envie uma imagem de amostra e escale o Amazon ECS

Tarefa	Descrição	Habilidades necessárias
Envia uma imagem de amostra para o repositório do Amazon ECR.	Envia uma imagem de amostra (NGINX) para o repositório do Amazon Elastic Container Registry (Amazon ECR) chamado `web` (conforme	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	definido nos parâmetros). Você pode personalizar a imagem conforme necessário.
	
	Para fazer login e definir as credenciais para enviar uma imagem para o Amazon ECR, siga as instruções na documentação do Amazon ECR.
	
	Os comandos são:
	
	`docker pull nginx`
	`docker images`
	`docker tag <imageid> aws_account_id.dkr.ecr.region.amazonaws.com/<web>:latest`
	`docker push <aws_account_id>.dkr.ecr.<region>.amazonaws.com/<web>:tag`	

Tarefa	Descrição	Habilidades necessárias
Escale o Amazon ECS e verifique o acesso.	1. Dimensione o Amazon ECS para criar duas réplicas: `aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 2` onde `Poc-Service` se refere à sua aplicação de exemplo. 2. Verifique se os serviços estão acessíveis a partir do Application Load Balancer usando um nome de domínio totalmente qualificado (FQDN) ou DNS de um navegador ou usando o comando curl.	AWS DevOps

Configurar serviços e recursos de código

Tarefa	Descrição	Habilidades necessárias
Crie um CodeCommit repositório na conta de ferramentas.	Crie um CodeCommit repositório na conta de ferramentas usando o `codecommit.yaml` modelo, que está na `code` pasta do GitHub repositório. Você deve criar este repositório somente na única região em	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	que planeja desenvolver o código. `aws cloudformation deploy --stack-name codecommitrepoStack --parameter-overrides CodeCommitReponame=$CODECOMMITREPONAME \ ToolsAccount=$TOOLSACCOUNT --template-file codecommit.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`	

Tarefa	Descrição	Habilidades necessárias
Crie um bucket do S3 para gerenciar artefatos gerados pelo. CodePipeline	Crie um bucket do S3 para gerenciar artefatos gerados CodePipeline usando o `pre-reqs-bucket.yaml` modelo, que está na `code` pasta do GitHub repositório. As pilhas devem ser implantadas em todas as três contas e regiões de workload (teste) e ferramentas. `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM`  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketSta`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts	

Tarefa	Descrição	Habilidades necessárias
	-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM	

Tarefa	Descrição	Habilidades necessárias
Configure uma chave KMS multirregional.	1. Crie uma chave KMS multirregional com chaves primárias e de réplica que CodePipeline serão usadas. Em nosso exemplo, `ToolsAccount1region - ap-south-1` será a região principal. `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Defina as variáveis CMKARN a serem passadas para os projetos. CodeBuild Os valores estão disponíveis na saída da pilha de modelos ecs-codepipeline-pre-reqs -KMS (o ID da chave será o mesmo em todas as regiões e começará com). `mrk-` Ou	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	você pode obter os valores CMKARN na conta de ferramentas. Exporte-os em todas as sessões da conta:
	
	`export CMKARN1=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMKARN2=arn:aws:kms:eu-central-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMKARN3=arn:aws:kms:us-east-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMARNTOOLS=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`	

Tarefa	Descrição	Habilidades necessárias

Configure o CodeBuild projeto na conta de ferramentas.	1. Use o `codebuild_IAM.yaml` modelo da `code` pasta do GitHub repositório para configurar o AWS Identity and Access Management (IAM) para a AWS CodeBuild em uma única região na conta de ferramentas:
	`#In ToolsAccount`
	`aws cloudformation deploy --stack-name ecs-codebuild-iam \`
	`--template-file codebuild_IAM.yaml --region $TOOLSACCOUNTREGION \`
	`--capabilities CAPABILITY_NAMED_IAM`
	2. Use o `codebuild.yaml` modelo CodeBuild para configurar seu projeto de compilação. Implante esse modelo em todas as três regiões da seguinte forma:
	`aws cloudformation deploy --stack-name ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \`
	`CodeCommitRepoName=$CODECOMMITREPONAME ECRRepositoryName=`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`$ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT1 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN1 \ --template-file codebuild.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM` `aws cloudformation deploy --stack-name ecscodebuildstack -- parameter-overrides ToolsAccount=$TOOL SACCOUNT \ CodeCommitRepoName= $CODECOMMITREPONAME ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN2 \ --template-file codebuild.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM`  `aws cloudformation deploy --stack-name ecscodebuildstack --`	

Tarefa	Descrição	Habilidades necessárias
	parameter-overrides ToolsAccount=$TOOL SACCOUNT \ CodeCommitRepoName= $CODECOMMITREPONAME ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT3 \ CodeCommitRegion= $CODECOMMITREGION CMKARN=$CMKARN3 \ --template-file codebuild.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM	

Tarefa	Descrição	Habilidades necessárias

Configure CodeDeploy em contas de carga de trabalho.	Use o `codedeploy.yaml` modelo na `code` pasta do GitHub repositório para configurar CodeDeploy em todas as três contas de carga de trabalho. A saída de `mainInfraStack` inclui os Amazon Resource Names (ARNs) do cluster Amazon ECS e o ouvinte do Application Load Balancer.
	
	Note
	Os valores das pilhas de infraestrutura já foram exportados e, portanto, são importados pelos modelos de CodeDeploy pilha.
	
	`##WorkloadAccount1##`
	`aws cloudformation deploy --stack-name ecscodedeploystack \`
	`--parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \`
	`--template-file codedeploy.yaml --region $TESTACCOUNT1REGION --capabil`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	ities CAPABILIT Y_NAMED_IAM ##WorkloadAccount2## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM ##WorkloadAccount3## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM	

Configurar CodePipeline na conta de ferramentas

Tarefa	Descrição	Habilidades necessárias
Crie um pipeline de código na conta de ferramentas.	Na conta de ferramentas, execute o comando: `aws cloudformation deploy --stack-name ecscodepipelinestack --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount1Region=$TESTACCOUNT1REGION \ TestAccount2=$TESTACCOUNT2 TestAccount2Region=$TESTACCOUNT2REGION \ TestAccount3=$TESTACCOUNT3 TestAccount3Region=$TESTACCOUNT3REGION \ CMKARNTools=$CMKTROOLSARN CMKARN1=$CMKARN1 CMKARN2=$CMKARN2 CMKARN3=$CMKARN3 \ CodeCommitRepoName=$CODECOMMITREPONAME BucketStartName=$BUCKETSTARTNAME \ --template-file codepipeline.yaml --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps
Forneça acesso CodePipeline e CodeBuild funções na política de chaves do AWS	1. Forneça acesso CodePipeline e CodeBuild funções na	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
KMS e na política de bucket do S3.	política de chaves do AWS KMS: `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ CodeBuildCondition=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION`  2. Atualize a política de bucket do S3 para permitir acesso CodePipeline e CodeDeploy funções:  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1`	

Tarefa	Descrição	Habilidades necessárias
	TestAccount2=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ PutS3BucketPolic y=true TestAccou nt1=$TESTACCOUNT1 TestAccount2=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter-	

Tarefa	Descrição	Habilidades necessárias
	overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabil	

Tarefa	Descrição	Habilidades necessárias
	`ities CAPABILIT Y_NAMED_IAM`	

Ligue e teste o pipeline

Tarefa	Descrição	Habilidades necessárias
Envie as alterações para o CodeCommit repositório.	1. Clone o CodeCommit repositório que foi criado no `codecommitrepoStac k` usando o `git clone` comando, conforme descrito na documentação da AWS CodeCommit . 2. Atualize os artefatos de entrada com os detalhes necessários: • Arquivo JSON: atualize `AccountID` no arquivo em três locais desse arquivo. Renomeie os três arquivos para incluir a conta IDs. • Arquivos YAML: atualize o ARN e a versão da definição de tarefa. Renomeie os três arquivos para incluir a conta IDs. 3. Modifique o arquivo `index.html` para fazer algumas pequenas alterações na página inicial.	

Tarefa	Descrição	Habilidades necessárias

	4. Copie os seguintes arquivos para o repositório e confirme:
	
	`index.html`
	`Dockerfile`
	`buildspec.yaml`
	`appspec_<accountid>.yaml (3 files - one per account )`
	`taskdef<accountid>.json (3 files - one per account)`
	
	5. Inicie ou reinicie o pipeline e verifique os resultados.
	6. Acesse o serviço a partir do Application Load Balancer usando um FQDN ou DNS e verifique se as atualizações foram implantadas.	

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpe todos os recursos implantados.	1. Reduza a escala verticalmente do Amazon ECS para zero instâncias: `aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 0`	

Tarefa	Descrição	Habilidades necessárias

	2. Exclua as CloudFormation pilhas em cada conta e região:
	
	`##In Tools Account##`
	`aws cloudformation delete-stack --stack-name ecscodepipelinestack --region $TOOLSACCOUNTREGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT1REGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT2REGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT3REGION`
	`aws cloudformation delete-stack --stack-name ecs-codepipeline-pre-reqs-KMS --region $TOOLSACCOUNTREGION`
	`aws cloudformation delete-stack --stack-name codecommitrepoStack --region $TOOLSACCOUNTREGION`
	`aws cloudformation delete-stack --stack-name pre-reqs-artifacts-bucket`	

Tarefa	Descrição	Habilidades necessárias
	--region $TESTACCOUNT1REGION aws cloudformation delete-stack --stack-name pre-reqs-artifacts-bucket --region $TESTACCOUNT2REGION aws cloudformation delete-stack --stack-name pre-reqs-artifacts-bucket --region $TESTACCOUNT3REGION aws cloudformation delete-stack --stack-name pre-reqs-artifacts-bucket --region $TOOLSACCOUNTREGION aws cloudformation delete-stack --stack-name ecs-codebuild-iam --region $TOOLSACCOUNTREGION ##NOTE: Artifact buckets will not get deleted if there are artifacts so it has to be emptied manually before deleting.## ##In Workload / Test Accounts## ##Account:1## aws cloudformation delete-stack --stack-name ecscodede	

Tarefa	Descrição	Habilidades necessárias

	`ploystack --region $TESTACCOUNT1REGION`
	`aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT1REGION`
	`##Account:2##`
	`aws cloudformation delete-stack --stack-name ecscodedeployst ack --region $TESTACCOUNT2REGION`
	`aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT2REGION`
	`##Account:3##`
	`aws cloudformation delete-stack --stack-name ecscodedeployst ack --region $TESTACCOUNT3REGION`
	`aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT3REGION`
	`##NOTE: Amazon ECR (web) will not get deleted if the registry still includes images. It can be manually cleaned up if not required.`	

Solução de problemas

Problema	Solução
As alterações que você confirmou no repositór io não estão sendo implantadas.	• Verifique se há erros nos CodeBuild registros na ação de compilação do Docker. Para obter mais informações, consulte a documentação do CodeBuild . • Verifique se há problemas de CodeDeploy implantação do Amazon ECS na implantaç ão.

Recursos relacionados

- Enviando uma imagem do Docker (documentação do Amazon ECR)
- Conecte-se a um CodeCommit repositório da AWS (CodeCommit documentação da AWS)
- Solução de problemas da AWS CodeBuild (CodeBuild documentação da AWS)

Monitore os repositórios do Amazon ECR para obter permissões curinga usando o AWS e o AWS Config CloudFormation

Criado por Vikrant Telkar (AWS), Sajid Momin (AWS) e Wassim Benhallam (AWS)

Resumo

O, Amazon Web Services (AWS) Nuvem, Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado pelo registro de imagens de contêiner compatível com repositórios privados com permissões baseadas em recursos usando o AWS Identity and Access Management (IAM).

O IAM suporta o caractere curinga "`*`" tanto nos recursos quanto nos atributos de ação, o que facilita a escolha automática de vários itens correspondentes. Em seu ambiente de teste, você pode permitir que todos os usuários autenticados da AWS acessem um repositório Amazon ECR usando a permissão curinga `ecr:*` em um elemento principal da declaração de política do seu repositório. A permissão curinga `ecr:*` pode ser útil ao desenvolver e testar em contas de desenvolvimento que não conseguem acessar seus dados de produção.

No entanto, você deve garantir que a permissão curinga `ecr:*` não seja usada em seus ambientes de produção, pois ela pode causar sérias vulnerabilidades de segurança. A abordagem desse padrão ajuda você a identificar repositórios do Amazon ECR que contêm a permissão curinga `ecr:*` nas declarações de política do repositório. O padrão fornece etapas e um CloudFormation modelo da AWS para criar uma regra personalizada no AWS Config. Em seguida, uma função do AWS Lambda monitora suas declarações de política do repositório Amazon ECR em busca de permissões curinga `ecr:*`. Se encontrar declarações de política de repositório não compatíveis, o Lambda notifica o AWS Config para enviar um evento para a Amazon EventBridge e, em seguida, inicia um tópico do EventBridge Amazon Simple Notification Service (Amazon SNS). O tópico do SNS notifica você por e-mail sobre as declarações de política de repositório não compatíveis.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI), instalada e configurada. Para obter mais informações, consulte Instalação, atualização e desinstalação da AWS CLI na documentação da AWS CLI.
- Um repositório Amazon ECR existente com uma declaração de política anexada, instalado e configurado em seu ambiente de teste. Para obter mais informações sobre isso, consulte

Criação de um repositório privado e Definição de uma declaração de política de repositório na documentação do Amazon ECR.

- AWS Config, configurado em sua região preferida da AWS. Para obter mais informações sobre isso, consulte Conceitos básicos do AWS Config na documentação do AWS Config.
- O arquivo `aws-config-cloudformation.template` (anexado), baixado na sua máquina local.

Limitações

- A solução desse padrão é regional e seus recursos devem ser criados na mesma região.

Arquitetura

O diagrama a seguir mostra como o AWS Config avalia as declarações de política do repositório Amazon ECR.

O diagrama mostra o seguinte fluxo de trabalho:

1. O AWS Config inicia uma regra personalizada.
2. A regra personalizada invoca uma função do Lambda para avaliar a conformidade das declarações de política do repositório Amazon ECR. A função do Lambda então identifica declarações de política de repositório não compatíveis.
3. A função do Lambda envia o estado de não conformidade atualizado para o AWS Config.
4. O AWS Config envia um evento para. EventBridge
5. EventBridge publica as notificações de não conformidade em um tópico do SNS.
6. O Amazon SNS envia um alerta por e-mail para você ou para um usuário autorizado.

Automação e escala

A solução desse padrão pode monitorar qualquer número de declarações de política do repositório Amazon ECR, mas todos os recursos que você deseja avaliar devem ser criados na mesma região.

Ferramentas

- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em várias contas e regiões da AWS.
- AWS Config: o AWS Config oferece uma exibição detalhada da configuração dos recursos da AWS em sua conta da AWS. Isso inclui como os recursos estão relacionados um com o outro e como eles foram configurados no passado, de modo que você possa ver como os relacionamentos e as configurações foram alterados ao longo do tempo.
- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagem de contêiner, seguro, escalável e confiável. O Amazon ECR oferece suporte a repositórios privados com permissões baseadas em recursos usando o IAM.
- Amazon EventBridge — EventBridge A Amazon é um serviço de ônibus de eventos sem servidor que você pode usar para conectar seus aplicativos a dados de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus aplicativos, aplicativos de software como serviço (SaaS) e serviços da AWS para destinos como funções do AWS Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras contas.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

O código desse padrão está disponível no arquivo `aws-config-cloudformation.template` (anexado).

Épicos

Crie a CloudFormation pilha da AWS

Tarefa	Descrição	Habilidades necessárias
Crie a CloudFormation pilha da AWS.	Crie uma CloudFormation pilha da AWS executando o seguinte comando na AWS CLI: `$ aws cloudformation create-stack --stack-name=AWSConfigECR \ --template-body file://aws-config-cloudformation.template \ --parameters ParameterKey=<email>,ParameterValue=<myemail@example.com> \ --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps

Teste a regra personalizada do AWS Config

Tarefa	Descrição	Habilidades necessárias
Teste a regra personalizada do AWS Config.	1. Faça login no Console de Gerenciamento da AWS, abra o console do AWS Config e escolha Recursos. 2. Na página Inventário de recursos, você pode filtrar por categoria de recurso,	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	tipo de recurso e status de conformidade. 3. Um repositório Amazon ECR que contém `ecr:*` is `NON-COMPLIANT?` e um repositório Amazon ECR que não contém`ecr:*` is `COMPLIANT` . 4. O endereço de e-mail inscrito no tópico do SNS recebe notificações se um repositório do Amazon ECR contiver declarações de política não compatíveis.	

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Otimize implantações sem servidor de várias contas usando os fluxos de trabalho e Actions AWS CDK GitHub

Criado por Sarat Chandra Pothula (AWS) e VAMSI KRISHNA SUNKAVALLI (AWS)

Resumo

Organizações que implantam infraestrutura sem servidor em vários ambientes de rede geralmente enfrentam desafios como duplicação de código, processos manuais Contas da AWS e práticas inconsistentes. A solução desse padrão mostra como usar os fluxos de trabalho reutilizáveis AWS Cloud Development Kit (AWS CDK) in Go and GitHub Actions para agilizar o gerenciamento da infraestrutura sem servidor de várias contas. Essa solução demonstra como você pode definir recursos de nuvem como código, implementar processos padronizados integration/continuous deployment (CI/CD (contínuos) e criar componentes modulares e reutilizáveis.

Ao usar essas ferramentas, as organizações podem gerenciar com eficiência os recursos entre contas, implementar pipelines de implantação consistentes e simplificar arquiteturas complexas sem servidor. A abordagem também aprimora a segurança e a conformidade ao impor práticas padronizadas para uso com Contas da AWS, em última análise, melhorando a produtividade e reduzindo os erros no desenvolvimento e na implantação de aplicativos sem servidor.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Identity and Access Management As funções e permissões (IAM) estão em vigor para o processo de implantação. Isso inclui permissões para acessar repositórios do Amazon Elastic Container Registry (Amazon ECR), AWS Lambda criar funções e quaisquer outros recursos necessários em todo o destino. Contas da AWS
- AWS Command Line Interface (AWS CLI) versão 2.9.11 ou posterior, instalada e configurada.
- AWS Cloud Development Kit (AWS CDK) versão 2.114.1 ou posterior, instalada e inicializada.
- Go 1.22 ou posterior, instalado.
- Docker 24.0.6 ou posterior, instalado.

Limitações

- Compatibilidade de idiomas — Go é uma linguagem popular para aplicativos sem servidor. No entanto, além do Go, ele AWS CDK suporta outras linguagens de programação, incluindo C#, Java, Python e. TypeScript Se sua organização já tem bases de código ou experiência em outras linguagens, talvez seja necessário adaptar ou aprender Go para usar totalmente a solução descrita no padrão.
- Curva de aprendizado — A adoção do AWS CDK, Go (se for novo na organização) e fluxos de trabalho GitHub reutilizáveis pode envolver uma curva de aprendizado para desenvolvedores e equipes. DevOps Treinamento e documentação podem ser necessários para garantir a adoção tranquila e o uso eficaz dessas tecnologias.

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

Essa solução executa as seguintes etapas:

1. O desenvolvedor clona o repositório, cria uma nova ramificação e faz alterações no código do aplicativo em seu ambiente local.
2. O desenvolvedor confirma essas alterações e envia a nova ramificação para o GitHub repositório.
3. O desenvolvedor cria uma pull request no GitHub repositório, propondo mesclar seu recurso ou nova ramificação de recurso na ramificação principal.
4. Essa pull request aciona o fluxo de trabalho de GitHub ações de integração contínua (CI). Os fluxos de trabalho de CI e implantação contínua (CD) nesse padrão usam fluxos de trabalho reutilizáveis, que são modelos modulares predefinidos que podem ser compartilhados e executados em diferentes projetos ou repositórios. Fluxos de trabalho reutilizáveis promovem padronização e eficiência nos processos de CI/CD.
5. O fluxo de trabalho de CI configura o ambiente necessário, gera uma tag Docker para a imagem e cria a imagem Docker usando o código do aplicativo.
6. O fluxo de trabalho de CI é AWS autenticado usando a função central do Conta da AWS GitHub OIDC. Para fluxos de trabalho de CI, a função central do Conta da AWS GitHub OIDC usa AWS Security Token Service (AWS STS) para obter credenciais temporárias. Essas credenciais permitem que a função crie e envie imagens do Docker para o repositório Amazon ECR da central. Conta da AWS
7. O fluxo de trabalho de CI envia a imagem do Docker criada para o Amazon ECR.

8. O fluxo de trabalho de CI armazena a tag de imagem no Systems Manager Parameter Store.
9. Depois que o fluxo de trabalho de CI for concluído com êxito, a tag de imagem do Docker será gerada.
10. Ao acionar o fluxo de trabalho do CD, o desenvolvedor insere manualmente a tag de imagem da imagem do Docker que deseja implantar. Essa tag de imagem corresponde à tag que foi gerada e enviada para o Amazon ECR durante o fluxo de trabalho de CI.
11. O desenvolvedor aciona manualmente o fluxo de trabalho do CD, que usa o fluxo de trabalho reutilizável do CD.
12. O fluxo de trabalho do CD é autenticado AWS usando a função central do Conta da AWS GitHub OIDC. Para o fluxo de trabalho do CD, AWS STS é usado primeiro para assumir a função central do Conta da AWS GitHub OIDC. Em seguida, essa função assume as funções de bootstrap do CDK para implantações de contas de destino.
13. O fluxo de trabalho do CD usa o AWS CDK para sintetizar modelos AWS CloudFormation .
14. O fluxo de trabalho do CD implanta o aplicativo no destino Conta da AWS usando o CDK deploy, usando a tag de imagem especificada manualmente para a função Lambda.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS CloudFormation é parte integrante do processo AWS CDK de implantação. O CDK sintetiza CloudFormation modelos e depois usa CloudFormation para criar ou atualizar os recursos no ambiente. AWS
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

- AWS Systems Manager O Parameter Store fornece armazenamento seguro e hierárquico para gerenciamento de dados de configuração e gerenciamento de segredos.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- GitHub O Actions é uma plataforma de integração contínua e entrega contínua (CI/CD) totalmente integrada aos GitHub repositórios. Você pode usar o GitHub Actions para automatizar seu pipeline de criação, teste e implantação.
- Go é uma linguagem de programação de código aberto compatível com o Google.

Repositório de código

O código desse padrão está disponível no cicd-github-actions repositório GitHub aws-cdk-golang-serverless-.

Práticas recomendadas

- Design modular — Organize seu AWS CDK código em construções ou pilhas modulares e reutilizáveis, promovendo a reutilização e a manutenção do código em várias contas e projetos.
- Separação de preocupações — Separe o código da infraestrutura do código do aplicativo, permitindo a implantação e o gerenciamento independentes de cada componente.
- Controle de versão e imutabilidade — Trate sua infraestrutura como código (IaC) e use o Git para controle de versão. Adote princípios de infraestrutura imutáveis criando novos recursos em vez de modificar os existentes.
- Teste e validação — Implemente estratégias de teste abrangentes, incluindo testes unitários, testes de integração e end-to-end testes, para ajudar a apoiar a exatidão e a confiabilidade de seu AWS CDK código e implantações.
- Segurança e conformidade — siga as melhores práticas de AWS segurança, como acesso com privilégios mínimos, comunicação segura e criptografia de dados. Implemente verificações de conformidade e mecanismos de auditoria para garantir a adesão às políticas organizacionais e aos requisitos regulatórios. Implemente as melhores práticas de segurança para imagens de contêineres, como verificar vulnerabilidades, impor a assinatura de imagens e cumprir os requisitos de conformidade de sua organização.

- Monitoramento e registro — Configure mecanismos de monitoramento e registro para rastrear a integridade e o desempenho de seus aplicativos e infraestrutura sem servidor. Use Serviços da AWS como Amazon CloudWatch, AWS CloudTrail, e AWS X-Ray para fins de monitoramento e auditoria.
- Automação e CI/CD — Use fluxos de trabalho GitHub reutilizáveis e outras ferramentas de CI/CD para automatizar os processos de criação, teste e implantação, o que pode ajudar a suportar implantações consistentes e repetíveis em várias contas.
- Gerenciamento do ambiente — mantenha ambientes separados (por exemplo, desenvolvimento, preparação e produção). Implemente estratégias para promover mudanças entre ambientes, garantindo testes e validação adequados antes das implantações de produção.
- Documentação e colaboração — Documente seu código de infraestrutura, processos de implantação e melhores práticas para facilitar o compartilhamento de conhecimento e a colaboração em sua equipe.
- Otimização de custos — implemente estratégias de monitoramento e otimização de custos, como o dimensionamento correto dos recursos, o uso do auto-scaling e o aproveitamento de serviços de otimização de AWS custos, como e. AWS Budgets AWS Cost Explorer
- Recuperação de desastres e backup — Planeje cenários de recuperação de desastres implementando mecanismos de backup e restauração para seus aplicativos sem servidor e recursos de infraestrutura.
- Melhoria contínua — revise regularmente e atualize suas práticas, ferramentas e processos para se alinhar às melhores práticas, recomendações de segurança e avanços tecnológicos mais recentes no ecossistema sem servidor.
- Melhore a postura de segurança — Use AWS PrivateLinkpara melhorar a postura de segurança de sua nuvem privada virtual (VPC) configurando endpoints de VPC de interface para Amazon ECR e Parameter Store. AWS Lambda AWS Systems Manager

Épicos

Configure os ambientes

Tarefa	Descrição	Habilidades necessárias
Crie um repositório Amazon ECR na central. Conta da AWS	Para compartilhar imagens de contêineres entre várias Contas da AWS, você deve	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	configurar o acesso entre contas para o Amazon ECR. Primeiro, crie um repositór io Amazon ECR na central. Conta da AWS Para criar um repositório Amazon ECR, execute o seguinte comando: `aws ecr create-re pository --repository- name sample-repo` Em uma tarefa posterior, conceda acesso de pull à outra pessoa Contas da AWS que precisa usar a imagem do contêiner.	

Tarefa	Descrição	Habilidades necessárias
Adicione permissões entre contas ao repositório Amazon ECR.	Para adicionar permissões entre contas ao repositório Amazon ECR na central Conta da AWS, execute o seguinte código: `{ "Version": "2008-10-17", "Statement": [{ "Sid": "LambdaECRImageRetrievalPolicy", "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": ["ecr:BatchGetImage", "ecr:GetDownloadUrlForLayer",], "Condition": { "StringLike": { "aws:sourceArn": "arn:aws:lambda:<Target_Region>:<Target_Account_ID>:function:*" } } }, { "Sid": "new statement", "Effect": "Allow",`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	"Principal": {
	"AWS": "arn:aws:iam::<Target_Account_ID>:root"
	},
	"Action": [
	"ecr:BatchGetImage",
	"ecr:GetDownloadUrlForLayer",
	],
	}
	]
	}	

Tarefa	Descrição	Habilidades necessárias
Configure uma função para a função GitHub OIDC na central. Conta da AWS	1. Configure AWS para confiar no GitHub OIDC como uma identidade federada, o que inclui adicionar o provedor GitHub OIDC AWS e configurar a função e a política de confiança no IAM. Para fazer isso, siga as instruções em Configuração do OpenID Connect na Amazon Web Services GitHub na documentação. 2. Depois que a função for criada, adicione as permissões necessárias à função. Por exemplo, adicione permissões para o Amazon ECR e o AWS Systems Manager Parameter Store. Para obter mais informações, consulte Configuração de uma função para o provedor de identidade GitHub OIDC na documentação do IAM.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Inicialize o AWS ambiente no destino. Contas da AWS	Configure um ambiente CDK em um ambiente específico Conta da AWS e Região da AWS que permita implantaç ões entre contas a partir de uma conta central e aplique princípios de privilégi os mínimos à função de execução. CloudFormation Para inicializar um AWS ambiente, execute o seguinte comando: `cdk bootstrap aws://<Target_Account_ID>/<Target_Region> --trust <Central_Account_ID> --cloudformation-execution-policies arn:aws:iam::aws:policy/<Least_Privilege_Policy>`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Conceda acesso à função central do Conta da AWS OIDC às funções de Conta da AWS bootstrap de destino.	O bootstrap do CDK cria as seguintes funções do IAM, projetadas para serem assumidas pela central Conta da AWS durante vários estágios do processo de implantação do CDK: • Perfil de publicação de arquivos • Perfil de publicação de imagens • Perfil de pesquisa • Função de implantação Cada função tem permissões específicas adaptadas à sua finalidade, seguindo o princípio do menor privilégio. O `Target_Account_ID` e `Target_Region` em cada nome de função ajuda a indicar que essas funções são exclusivas em diferentes Contas da AWS regiões. Essa abordagem oferece suporte à identificação e ao gerenciamento claros em configurações de várias contas e várias regiões. `Target Account CDK Bootstrap Roles`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`arn:aws:iam::<Target_Account_ID>:role/cdk-deploy-role-<Target_Account_ID>-<Target_Region>`
	`arn:aws:iam::<Target_Account_ID>:role/cdk-file-publishing-role-<Target_Account_ID>-<Target_Region>`
	`arn:aws:iam::<Target_Account_ID>:role/cdk-image-publishing-role-<Target_Account_ID>-<Target_Region>`
	`arn:aws:iam::<Target_Account_ID>:role/cdk-lookup-role-<Target_Account_ID>-<Target_Region>`
	• Atualize a política de permissões para a função do OIDC na conta central para permitir que ela assuma funções na conta de destino. Essa configuração permite a implantação de pilhas de CDK em diferentes. Contas da AWS Ao permitir que a função OIDC da conta central adote as permissões necessárias da conta de destino, você cria uma ponte segura para implantações de CDK entre contas. Essa abordagem mantém o controle de	

Tarefa	Descrição	Habilidades necessárias
	acesso adequado e, ao mesmo tempo, facilita o gerenciamento contínuo da infraestrutura de várias contas. Para atualizar a política de permissões para a função do OIDC na central Conta da AWS, use o código a seguir: `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": ["arn:aws:iam::<Target_Account_ID>:role/cdk-deploy-role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-file-publishing-role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-image-publishing-`	

Tarefa	Descrição	Habilidades necessárias
	role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-lookup-role-<Target_Account_ID>-<Target_Region>”] }] }	

Crie a imagem do Docker

Tarefa	Descrição	Habilidades necessárias
Clone o repositório do projeto.	Para clonar o GitHub repositório desse padrão, execute o seguinte comando: `git clone https://github.com/aws-samples/aws-cdk-golang-serverless-cicd-github-actions.git`	AWS DevOps
Vá para o caminho do Dockerfile.	Para navegar até o caminho do Dockerfile, execute o seguinte comando: `cd lambda`	AWS DevOps
Autentique o Docker com o Amazon ECR.	O Amazon ECR exige acesso seguro aos seus repositórios de contêineres privados. Ao	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	assinar dessa forma, você está permitindo que o Docker em sua máquina local ou ambiente de CI/CD interaja com o Amazon ECR de forma segura. Para autenticar o Docker com o Amazon ECR, execute o seguinte comando: `aws ecr get-login -password --region <AWS_REGION> | docker login --username AWS --password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com` Revise os espaços reservados `AWS_REGION` e `AWS_Account_ID` com suas informações.	
Crie a imagem do Docker.	Para criar a imagem do Docker, execute o seguinte comando: `docker build --platform linux/arm64 -t sample-app .`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Marque e envie a imagem do Docker.	Para marcar e enviar a imagem do Docker para o repositório Amazon ECR, execute os seguintes comandos:
	`docker tag sample-ap p:latest <AWS_ACCO UNT_ID>.dkr.ecr.<A WS_REGION>.amazona ws.com/<ECR_REPOSI TORY>:<DOCKER_TAG>`
	`docker push <AWS_ACCO UNT_ID>.dkr.ecr.<A WS_REGION>.amazona ws.com/<ECR_REPOSI TORY>:<DOCKER_TAG>`
	Revise os espaços reservado s`AWS_Account_ID` ,, `AWS_REGION` `ECR_REPOS ITORY` , e `DOCKER_TAG` com suas informações.
		AWS DevOps

Implemente o AWS CDK aplicativo

Tarefa	Descrição	Habilidades necessárias
Sintetize a pilha CDK com variáveis específicas do ambiente.	Para gerar o CloudFormation modelo para sua infraestr utura conforme definido no seu código CDK, execute o seguinte comando:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`ENV=<environment> IMAGETAG=<image_tag> ECR_ARN=<ecr_repo_arn> cdk synth` Revise os seguintes espaços reservados com suas informações: • `environment` — Substituído por um nome de ambiente específico`dev`, como`staging`, ou`prod`. • `image_tag` — Substitua por uma tag específica para uma imagem do Docker, como `v1.0.0` ou`latest`. • `ecr_repo_arn` — Substitua pelo Amazon Resource Name (ARN) de um repositório Amazon ECR.	

Tarefa	Descrição	Habilidades necessárias
Implante a pilha CDK.	Para implantar a pilha CDK na sua Conta da AWS, execute o comando a seguir. A `--require-approval never` bandeira significa que o CDK aprovará e executará automaticamente todas as alterações. Isso inclui mudanças que o CDK normalmente sinalizaria como necessitando de revisão manual (como mudanças na política do IAM ou remoção de recursos). Certifique-se de que seu código CDK e seu pipeline de CI/CD estejam bem testados e seguros antes de usar a `--require-approval never` bandeira em ambientes de produção. `ENV=<environment> IMAGETAG=<image_tag> ECR_ARN=<ecr_repo_arn> cdk deploy --require-approval never`	AWS DevOps

Automatize CI/CD usando fluxos de trabalho de ações GitHub

Tarefa	Descrição	Habilidades necessárias
Crie uma ramificação de recursos e adicione suas alterações.	Use o repositório clonado que você criou anteriormente, crie uma ramificação de recursos	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	e adicione suas alterações ao código do aplicativo. Use os seguintes comandos:
	
	`git checkout -b <feature_branch>`
	`git add .`
	`git commit -m “add your changes”`
	`git push origin <feature_branch>`
	
	Veja a seguir exemplos de mudanças:
	
	• Alterações na lógica da função Lambda
	• Adicionar novos recursos ou funcionalidades ao código Lambda
	• Corrigindo bugs ou otimizando o código existente na função Lambda
	
	GitHub As ações usarão os fluxos de trabalho reutilizáveis e acionarão os pipelines de CI/CD.	

Mescle suas alterações.	Crie uma pull request e mescle suas alterações com a principal.	AWS DevOps

Solução de problemas

Problema	Solução
`AccessDenied` erros ao implantar recursos em Contas da AWS, por exemplo,`AccessDenied: User not authorized to perform: “sts:AssumeRole"` .	Para ajudar a resolver esse problema, faça o seguinte para verificar as permissões entre contas: • Certifique-se de que as funções e políticas necessárias do IAM estejam em vigor para implantações em várias contas. • Verifique se as permissões da `assume` função estão configuradas corretamente.
Problemas de compatibilidade devido a incompatibilidades de versão, por exemplo, `undefined: awscdkStack` erro com uma versão desatualizada do CDK.	Para ajudar a resolver esse problema, faça o seguinte para verificar se você está usando as versões necessárias do AWS CDK e do Go: • Verifique se você está usando versões compatíveis do AWS CDK e do Go. • Verifique se há problemas conhecidos ou alterações significativas nas versões recentes.
Falhas no pipeline de CI/CD, por exemplo, `Error: No such file or directory` devido à configuração incorreta do YAML ou `Permission denied` a filiais protegidas.	Para ajudar a resolver problemas com a configuração GitHub das Ações, verifique se os fluxos de trabalho reutilizáveis estão devidamente referenciados e configurados.

Recursos relacionados

Recursos da AWS

- AWS Práticas recomendadas de segurança, identidade e conformidade
- AWS CDK Workshop
- AWS Biblioteca do Cloud Development Kit
- Criar uma função do Lambda usando uma imagem de contêiner

- Identity and Access Management para Amazon Elastic Container Registry
- Trabalhando com o AWS CDK em Go

Outros recursos

- Configurando o OpenID Connect na Amazon Web GitHub Services (documentação)
- Documentação Golang
- Início rápido para GitHub ações (GitHub documentação)
- Reutilização de fluxos de trabalho (documentação) GitHub

Execute ações personalizadas a partir de CodeCommit eventos da AWS

Criado por Abdullahi Olaoye (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Ao usar um CodeCommit repositório da AWS para armazenar código, talvez você queira monitorar o repositório e iniciar um fluxo de trabalho de ações quando eventos específicos ocorrerem. Por exemplo, talvez você queira enviar uma notificação por e-mail quando um usuário comentar sobre uma linha de código em uma confirmação ou iniciar uma função do AWS Lambda para realizar verificações de segurança no conteúdo do repositório após uma confirmação. Esse padrão descreve as etapas para configurar um CodeCommit repositório para ações personalizadas. O padrão usa as regras de CodeCommit notificação da AWS para capturar os eventos de interesse e, em seguida, envia esses eventos para um destino configurado.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Familiaridade com os comandos do Git.
- AWS CodeCommit, configure. Para obter instruções, consulte Configuração para a AWS CodeCommit.
- (Recomendado) AWS Command Line Interface (AWS CLI), instalada e configurada. Para obter instruções, consulte Conceitos básicos da AWS CLI.

Arquitetura

Ferramentas

Serviços da AWS

- CodeCommitA AWS é um serviço de controle de origem totalmente gerenciado que hospeda repositórios seguros baseados em Git. Isso facilita a colaboração das equipes no código em

um ecossistema seguro e altamente escalável. CodeCommit elimina a necessidade de operar seu próprio sistema de controle de origem ou a preocupação com a escalabilidade de sua infraestrutura

- O Amazon Simple Notification Service (Amazon SNS) é um serviço web que permite que aplicativos, usuários finais e dispositivos enviem e recebam notificações da nuvem instantaneamente. O Amazon SNS fornece tópicos (canais de comunicação) para mensagens de alta taxa de transferência, baseadas em push. many-to-many Usando tópicos do Amazon SNS, os publicadores podem distribuir mensagens para um grande número de assinantes para processamento paralelo, incluindo filas do Amazon Simple Queue Service (Amazon SQS), funções do AWS Lambda e webhooks HTTP/S. Também é possível usar o Amazon SNS para enviar notificações para usuários finais usando push móvel, SMS e e-mail.

Épicos

Configurar um CodeCommit repositório

Tarefa	Descrição	Habilidades necessárias
Crie um CodeCommit repositório.	Use o CodeCommit console ou o AWS CLI para criar um CodeCommit repositór io. Para obter instruções, consulte Criar um CodeCommi t repositório.	DevOps engenheiro
Envie conteúdo para o CodeCommit repositório.	Depois de criar um repositór io, adicione conteúdo a ele usando os comandos do Git. Você pode migrar o conteúdo de um repositór io Git existente ou conteúdo local não versionado do seu computador. Para obter instruções, consulte Adicionar arquivos ao seu repositór	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	io ou Migrar para a AWS. CodeCommit	

Configuração do Amazon SNS

Tarefa	Descrição	Habilidades necessárias
Criar um tópico do SNS.	Este tópico do SNS recebe os eventos de CodeCommit. Para obter instruções consulte Como criar um tópico do Amazon SNS.	Arquiteto de nuvem, DevOps engenheiro
Crie um recurso para uma ação personalizada.	Para que a ação personalizada seja executada, você deve criar o recurso correspondente. Por exemplo, se sua ação personalizada for executar o código Lambda e enviar mensagens para uma fila SQS, você deverá criar a função do Lambda e a fila SQS. Ações como notificações por e-mail e SMS não exigem recursos. Para obter mais informações, consulte a documentação da AWS para o tipo de recurso que você está criando.	Arquiteto de nuvem, DevOps engenheiro
Assinar o recurso de ação personalizada no tópico do SNS.	Dependendo da ação personalizada, você cria uma assinatura para o protocolo apropriado. Por exemplo, você assina um endereço de e-mail	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	para notificação por e-mail, uma função do Lambda para executar código personalizado ou uma fila SQS para enviar eventos para o Amazon SQS. Para protocolos de assinatura como e-mail e SMS, você precisa confirmar a assinatura usando o link enviado para o e-mail ou número de telefone, respectivamente. Para obter instruções, consulte Assinatura de um tópico do Amazon SNS.	

Configurar regras de notificação

Tarefa	Descrição	Habilidades necessárias
Crie a regra de notificação para o CodeCommit repositório.	Ao criar a regra de notificação, você seleciona os eventos do Git que devem iniciar a notificação, seleciona o tópico do SNS como o tipo de destino e, em seguida, seleciona o tópico do SNS que você criou anteriormente. Você também pode configurar vários destinos para o repositório. Para obter instruções, consulte Criar uma regra de notificação.	DevOps engenheiro
Teste ações personalizadas.	Execute um dos eventos que foram configurados para	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	iniciar a notificação. Por exemplo, crie uma solicitação pull se você selecionou esse evento como acionador. É necessário ver sua ação personalizada sendo executada. Por exemplo, se você inscreveu um endereço de e-mail para o tópico do SNS, deve receber uma notificação por e-mail.	

Recursos relacionados

- CodeCommit Documentação da AWS
- Documentação do Amazon SNS
- Documentação do Git

Provisione AWS Service Catalog produtos com base em AWS CloudFormation modelos usando GitHub Ações

Criado por Ashish Bhatt (AWS) e Ruchika Modi (AWS)

Resumo

Esse padrão fornece às organizações uma abordagem simplificada usando AWS Service Catalogprodutos e portfólios para provisionar de forma padronizada e compatível Serviços da AWS entre as equipes. AWS CloudFormationajuda a combinar componentes essenciais nos produtos e portfólios do Service Catalog para provisionar a infraestrutura de rede básica em. Nuvem AWSEsse padrão também promove DevOps práticas ao integrar a infraestrutura como código (IaC) em fluxos de trabalho de desenvolvimento automatizados usando ações. GitHub

AWS Service Catalog permite que as organizações criem e gerenciem serviços de TI aprovados AWS, oferecendo benefícios como padronização, controle centralizado, provisionamento de autoatendimento e gerenciamento de custos. Ao automatizar a implantação de portfólios e produtos do Service Catalog por meio do GitHub Actions, as empresas podem fazer o seguinte:

- Obtenha implantações consistentes e reproduzíveis.
- Use o controle de versão para IaC.
- Integre o gerenciamento de recursos de nuvem aos fluxos de trabalho de desenvolvimento existentes.

Essa combinação simplifica as operações na nuvem, reforça a conformidade e acelera a entrega de serviços aprovados, ao mesmo tempo em que reduz os erros manuais e melhora a eficiência geral.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Acesso ao GitHub repositório
- Compreensão básica de AWS CloudFormation e AWS Service Catalog
- Um bucket do Amazon Simple Storage Service (Amazon S3) para hospedar modelos CloudFormation

- Uma função AWS Identity and Access Management (IAM) chamada `github-actions` que é usada para conectividade entre GitHub e AWS

Limitações

- O código reutilizável desse padrão foi testado somente com GitHub Actions.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

A solução desse padrão foi criada usando as seguintes ações do GitHub Marketplace e suas respectivas versões:

- `actions/checkout@v4`
- `aws-actions/configure-aws-credentials@v2`
- `aws-actions/aws-cloudformation-github-deploy@v1.2.0`

Arquitetura

O diagrama a seguir mostra a arquitetura dessa solução.

1. Administradores ou engenheiros de plataforma enviam CloudFormation modelos padronizados para um GitHub repositório, onde os modelos são mantidos. O GitHub repositório também contém fluxos de trabalho que automatizam o provisionamento do uso de ações. AWS Service Catalog GitHub
2. GitHub As ações acionam um fluxo de trabalho que se conecta ao Nuvem AWS uso de um provedor OpenID Connect (OIDC) para provisionar o Service Catalog.
3. O Service Catalog contém o portfólio e os produtos que os desenvolvedores podem usar diretamente para provisionar AWS recursos padronizados. Esse padrão agrupa AWS recursos como nuvens privadas virtuais (VPCs), sub-redes, gateways NAT e de internet e tabelas de rotas.
4. Depois que o desenvolvedor cria um produto do Service Catalog, o Service Catalog o converte em recursos pré-configurados e padronizados AWS . Como resultado, os desenvolvedores

economizam tempo porque não precisam provisionar recursos individuais e configurá-los manualmente.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWSÉ um serviço de infraestrutura como código (IaC) que pode ser facilmente usado como um dos tipos de produto com AWS Service Catalog.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Service Catalogajuda você a gerenciar centralmente o catálogo de serviços de TI aprovados AWS. Os usuários finais podem implantar rapidamente somente os serviços de TI aprovados de que precisam, seguindo as restrições definidas pela organização.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outros

- GitHub O Actions é uma plataforma de integração contínua e entrega contínua (CI/CD) totalmente integrada aos GitHub repositórios. Você pode usar o GitHub Actions para automatizar seu pipeline de criação, teste e implantação.

Repositório de código

O código desse padrão está disponível no repositório GitHub service-catalog-with-github-actions. O repositório contém os seguintes arquivos de interesse:

- `github/workflows`:
  - `e2e-test.yaml`— Esse arquivo chama`workflow.yaml`, que é o fluxo de trabalho reutilizável. Esse fluxo de trabalho é acionado assim que há uma confirmação e um push em uma ramificação.

  - `workflow.yaml`— Esse arquivo contém o fluxo de trabalho reutilizável dessa solução e é configurado `workflow_call` como acionador. Como um fluxo de trabalho reutilizável, `workflow.yaml` pode ser chamado de qualquer outro fluxo de trabalho.
- `templates`:
  - `servicecatalog-portfolio.yaml`— Esse CloudFormation modelo inclui recursos que provisionam o portfólio do Service Catalog e o produto Service Catalog. O modelo contém um conjunto de parâmetros que são usados durante o provisionamento do portfólio e dos produtos do Service Catalog. Um parâmetro aceita uma URL de arquivo do Amazon S3 na qual o modelo `vpc.yaml` é carregado. Embora esse padrão inclua o `vpc.yaml` arquivo para provisionar AWS recursos, você também pode usar o parâmetro URL do arquivo S3 para configuração.
  - `vpc.yaml`— Esse CloudFormation modelo contém AWS recursos a serem adicionados ao produto Service Catalog. AWS os recursos incluem sub-redes VPCs, gateways de internet, gateways NAT e tabelas de rotas. O `vpc.yaml` modelo é um exemplo de como você pode usar qualquer CloudFormation modelo com um modelo de portfólio e produto do Service Catalog.

Práticas recomendadas

- Consulte as melhores práticas de segurança AWS Service Catalog na AWS Service Catalog documentação.
- Consulte Fortalecimento de segurança para GitHub ações na GitHub documentação.

Épicos

Configurar a estação de trabalho local

Tarefa	Descrição	Habilidades necessárias
Configure o Git na sua estação de trabalho local.	Para instalar e configurar o Git em sua estação de trabalho local, use as instruções de Introdução — Instalação do Git na documentação do Git.	Desenvolvedor de aplicativos
Clone o repositório do GitHub projeto.	Para clonar o repositório GitHub do projeto, faça o seguinte:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	1. Abra o GitHub repositório para esse padrão
	2. Escolha Código para ver as opções de clonagem e copie o URL fornecido na guia HTTPS.
	3. Crie uma pasta para seu projeto na sua estação de trabalho.
	4. Abra um terminal e navegue até essa pasta
	5. Para clonar o GitHub repositório, execute o comando a seguir usando a URL que você copiou na etapa 2:
	`git clone https://github.com/aws-samples/service-catalog-with-github-actions.git`
	6. Quando a clonagem estiver concluída, para mudar para o repositório clonado na pasta do projeto, execute o seguinte comando:
	`cd <folder-name>/service-catalog-with-github-actions`
	7. Abra o projeto em um ambiente de desenvolv	

Tarefa	Descrição	Habilidades necessárias
	imento integrado (IDE) de sua escolha.	

Configurar o provedor OIDC

Tarefa	Descrição	Habilidades necessárias
Configure um provedor OIDC.	Crie um provedor OpenID Connect (OIDC) que permita que os fluxos de trabalho do GitHub Actions acessem recursos sem precisar armazenar as AWS credencia is como segredos duradouro s. AWS GitHub Para obter instruções, consulte Configura ção do OpenID Connect na Amazon Web Services GitHub na documentação. Depois que um provedor OIDC for configurado, a política de confiança da função do IAM`github-actions` , mencionada anteriormente nos Pré-requi sitos, será atualizada.	Administrador da AWS, AWS DevOps, AWS geral

Pipeline Trigger GitHub Actions para implantar o portfólio e os produtos do Service Catalog

Tarefa	Descrição	Habilidades necessárias
Atualizar `e2e-test.yaml` .	O `e2e-test.yaml` arquivo aciona o fluxo de trabalho	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	reutilizável em. `workflow.yaml` Atualize e valide os valores dos seguintes parâmetros de entrada `eme2e-test.yaml` :
	• `aws_account_id` — Especifique o correto Conta da AWS.
	• `aws_region` — Especifiq ue o correto Região da AWS.
	• `s3BucketName` — Especifique o bucket do Amazon S3 para armazenar os CloudForm ation modelos.
	• O arquivo do fluxo de trabalho exige duas funções do IAM como entrada:
	  • `LaunchConstraintRo le` - A função do IAM que AWS Service Catalog assume quando um usuário final lança, atualiza ou encerra um produto.
	  • `PrincipalArn` - O Amazon Resource Name (ARN) do principal (usuário, função ou grupo do IAM) que será associado ao portfólio do Service Catalog.	

Tarefa	Descrição	Habilidades necessárias
	Se `PrincipalType` for`IAM`, o valor suportado é um Amazon Resource Name (ARN) do IAM totalmente definido. Se `PrincipalType` for`IAM_PATTERN` , o valor suportado é um ARN do IAM sem um `AccountID` no seguinte formato: `arn:partition:iam::::resource-type/resource-id`	

Valide a implantação

Tarefa	Descrição	Habilidades necessárias
Valide os recursos do Service Catalog.	Para validar os recursos do Service Catalog, faça o seguinte: 1. Faça login no AWS Management Console do Conta da AWS e verifique se o Região da AWS está correto. 2. Navegue até AWS Service Cataloge valide se um portfólio está presente em Administração, Portfólios. 3. Escolha o portfólio e valide as informações nas guias	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Produtos, Restrições e Acesso.	

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Exclua a CloudFormation pilha.	Para excluir a CloudFormation pilha, faça o seguinte: 1. Abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation. 2. Na barra de navegação na parte superior da tela, escolha Região da AWS onde a pilha está localizada. 3. Na página Pilhas, escolha a pilha que deseja excluir. A pilha deve estar em execução no momento. 4. No painel de detalhes da pilha, escolha Excluir. 5. Selecione Excluir pilha quando solicitado. Para obter mais informações, consulte Excluir uma pilha do CloudFormation console na documentação CloudFormation	DevOps engenheiro, administrador da AWS

Solução de problemas

Problema	Solução

`e2e-test`
 	
`Can't find 'action.yml', 'action.yaml' or 'Dockerfile' under '*/home/runner/work/service-catalog-with-github-actions/service-catalog-with-github-actions`
 	
`Did you forget to run actions/checkout before running your local action?`
	Para garantir que você tenha as configurações corretas do repositório habilitadas, faça o seguinte:
	
	1. Navegue até o repositório Github, guia Configurações.
	2. Escolha Ações, Geral no menu do lado esquerdo
	3. Vá para a seção Acesso e selecione a opção Acessível a partir de repositórios na organização 'XXX'.

Recursos relacionados

AWS documentação

- Visão geral do Service Catalog

Outros recursos

- Sobre eventos que acionam fluxos de trabalho (GitHub documentação)
- Reutilização de fluxos de trabalho (documentação) GitHub

Mais informações

Para ver capturas de tela relacionadas aos Epics, acesse a pasta Images no repositório desse padrão. GitHub As seguintes capturas de tela estão disponíveis:

- AWS Service Catalog portfólio, seção de administração
- AWS Service Catalog produto, seção de administração
- AWS Service Catalog produto, seção Usuário/Provisionamento

Provisione funções do IAM com privilégios mínimos implantando uma solução de máquina de venda automática de funções

Criado por Benjamin Morris (AWS), Aman Kaur Gandhi (AWS), Chade Moon (AWS) e Nima Fotouhi (AWS)

Resumo

Permissões de função com escopo excessivo AWS Identity and Access Management (IAM) para pipelines podem introduzir riscos desnecessários para uma organização. Às vezes, os desenvolvedores concedem permissões amplas durante o desenvolvimento, mas se esquecem de reduzir o escopo das permissões após a solução de problemas do código. Isso causa um problema em que funções poderosas estão presentes sem a necessidade comercial e podem nunca ter sido revisadas por um engenheiro de segurança.

Esse padrão oferece uma solução para esse problema: a máquina de venda automática de papéis (RVM). Usando um modelo de implantação seguro e centralizado, o RVM demonstra como provisionar funções do IAM com privilégios mínimos para pipelines de repositórios individuais GitHub com o mínimo esforço dos desenvolvedores. Como o RVM é uma solução central, você pode configurar suas equipes de segurança como revisores necessários para aprovar as alterações. Essa abordagem permite que a segurança rejeite solicitações de função de pipeline com permissão excessiva.

O RVM usa o código do Terraform como entrada e gera funções do IAM prontas para o pipeline como saída. As entradas necessárias são o Conta da AWS ID, o nome do GitHub repositório e a política de permissões. O RVM usa essas entradas para criar a política de confiança e a política de permissões da função. A política de confiança resultante permite que o GitHub repositório especificado assuma a função e a use para operações de pipeline.

O RVM usa uma função do IAM (configurada durante o bootstrap). Essa função tem permissões para assumir uma role-provisioning-role em cada conta na organização. A função é configurada por meio do AWS Control Tower Account Factory for Terraform (AFT) ou AWS CloudFormation StackSets. Essas role-provisioning-roles são as funções que realmente criam as funções do pipeline para desenvolvedores.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Uma GitHub organização usada para implantar infraestrutura como código (IaC) por meio de GitHub ações. (não GitHub Enterprise/Premium/Ultimate são obrigatórios.)
- Um AWS ambiente com várias contas. Esse ambiente não precisa fazer parte dele AWS Organizations.
- Um mecanismo para implantar uma função do IAM em todos Contas da AWS (por exemplo, AFT ou CloudFormation StackSets).
- Terraform versão 1.3 ou posterior instalado e configurado.
- Terraform AWS Provider versão 4 ou posterior instalado e configurado.

Limitações

- O código desse padrão é específico para GitHub Actions e Terraform. No entanto, os conceitos gerais do padrão podem ser reutilizados em outras estruturas de integração e entrega contínuas (CI/CD).
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir ilustra o fluxo de trabalho deste padrão.

O fluxo de trabalho para o uso típico da máquina de venda automática de papéis consiste nas seguintes etapas:

1. Um desenvolvedor envia o código que contém o código do Terraform para uma função IAM recém-solicitada no repositório GitHub RVM. Essa ação aciona o pipeline de ações do RVM GitHub .
2. O pipeline usa uma política de confiança do OpenID Connect (OIDC) para assumir a função de assumir a função de RVM.
3. À medida que o pipeline do RVM é executado, ele assume a função do fluxo de trabalho do RVM na conta na qual está provisionando a nova função do IAM do desenvolvedor. (A função do fluxo de trabalho do RVM foi provisionada usando AFT ou.) CloudFormation StackSets

4. O RVM cria a função IAM do desenvolvedor com permissões e confiança apropriadas, para que a função possa ser assumida por outros pipelines de aplicativos.
5. Os desenvolvedores de aplicativos podem configurar seus pipelines de aplicativos para assumir essa função provisionada por RVM.

A função criada inclui as permissões solicitadas pelo desenvolvedor e uma `ReadOnlyAccess` política. A função só pode ser assumida por pipelines executados na `main` ramificação do repositório especificado pelo desenvolvedor. Essa abordagem ajuda a garantir que a proteção e as revisões da filial possam ser necessárias para usar a função.

Automação e escala

As permissões com privilégios mínimos exigem atenção aos detalhes de cada função que está sendo provisionada. Esse modelo reduz a complexidade necessária para criar essas funções, permitindo que os desenvolvedores criem as funções de que precisam sem muito aprendizado ou esforço adicional.

Ferramentas

Serviços da AWS

- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.

Outras ferramentas

- O Git é um sistema de controle de versão distribuído e de código aberto. Inclui a capacidade de criar uma conta organizacional.
- GitHub O Actions é uma plataforma de integração contínua e entrega contínua (CI/CD) totalmente integrada aos GitHub repositórios. Você pode usar o GitHub Actions para automatizar seu pipeline de criação, teste e implantação.
- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Repositório de código

O código desse padrão está disponível no GitHub role-vending-machinerepositório.

Práticas recomendadas

- Torne fácil o certo e difícil o errado — Torne mais fácil fazer a coisa certa. Se os desenvolvedores tiverem dificuldades com o processo de provisionamento do RVM, eles podem tentar criar funções por outros meios, o que prejudica a natureza central do RVM. Certifique-se de que sua equipe de segurança forneça orientações claras sobre como usar o RVM de forma segura e eficaz.

  Você também deve dificultar que os desenvolvedores façam a coisa errada. Use políticas de controle de serviço (SCPs) ou limites de permissão para restringir quais funções podem criar outras funções. Essa abordagem pode ajudar a limitar a criação de funções apenas ao RVM e a outras fontes confiáveis.
- Forneça bons exemplos — Inevitavelmente, alguns desenvolvedores adaptarão as funções existentes no repositório RVM como modelos informais para conceder permissões para suas novas funções. Se você tiver exemplos de permissões mínimas dos quais eles possam copiar, isso pode reduzir o risco de os desenvolvedores solicitarem permissões amplas e cheias de caracteres curinga. Se você começar com funções altamente autorizadas com muitos curingas, esse problema pode se multiplicar com o passar do tempo.
- Use convenções e condições de nomenclatura — Mesmo que um desenvolvedor não saiba todos os nomes de recursos que seu aplicativo criará, ele ainda deve limitar as permissões de função usando uma convenção de nomenclatura. Por exemplo, se eles estiverem criando buckets do Amazon S3, o valor da chave de recurso pode parecer `arn:aws:s3:::myorg-myapp-dev-*` que sua função não tenha permissões além dos buckets correspondentes a esse nome. Aplicar a convenção de nomenclatura por meio de uma política do IAM tem o benefício adicional de melhorar a conformidade com a convenção de nomenclatura. Essa melhoria ocorre porque não será permitida a criação de recursos não correspondentes.
- Exigir revisões de pull request (PR) — O valor da solução RVM é que ela cria um local central onde novas funções do pipeline podem ser revisadas. No entanto, esse design só é útil se houver grades de proteção que ajudem a garantir que um código seguro e de alta qualidade seja comprometido com o RVM. Proteja as ramificações usadas para implantar código (por exemplo,`main`) de envios diretos e exija aprovações para qualquer solicitação de mesclagem direcionada a elas.
- Configurar funções somente para leitura — Por padrão, o RVM provisiona uma `readonly` versão de cada função solicitada. Essa função pode ser usada em pipelines de CI/CD que não gravam dados, como um `terraform plan` fluxo de trabalho de pipeline. Essa abordagem ajuda a evitar alterações indesejadas se um fluxo de trabalho somente para leitura se comportar mal.

Por padrão, a `ReadOnlyAccess` política AWS gerenciada é anexada às funções somente leitura e às funções de leitura e gravação. Essa política reduz a necessidade de iteração ao determinar as permissões necessárias, mas pode ser excessivamente permissiva para algumas organizações. Se quiser, você pode remover a política do código do Terraform.

- Conceda permissões mínimas — siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Prepare o ambiente

Tarefa	Descrição	Habilidades necessárias
Copie o repositório de amostras para sua GitHub organização.	Clone o repositório desse padrão ou bifurque esse repositório para sua GitHub organização para que você possa adaptá-lo às suas necessidades. • Se você optar por clonar esse repositório, poderá usar o seguinte comando: `git clone https://github.com/aws-samples/role-vending-machine` • Se você optar por bifurcar o repositório para sua GitHub organização, poderá usar o seguinte comando: `gh repo fork aws-samples/role-vending-machine`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`--org YOUR_ORGANIZATION_NAME`	
Determine o Conta da AWS para o RVM.	Determine qual implantação de infraestrutura usar Conta da AWS para o RVM. Não use a conta raiz ou de gerenciamento.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
(Opcional) Permita que os pipelines da organização sejam criados PRs.	**Note** Essa etapa só é necessária se você quiser permitir que o `generate_providers_and_account_vars` fluxo de trabalho seja criado PRs. Para permitir que os pipelines da sua organização sejam criados PRs, use as seguintes etapas: 1. Acesse `https://github.com/organizations/YOUR_ORG/settings/actions` . 2. Selecione Permitir GitHub ações para criar e aprovar pull requests. Para obter mais informações, consulte Gerenciando configurações de GitHub ações para um repositório na GitHub documentação.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Conceda permissões somente de leitura à conta RVM.	Crie uma política de delegação em sua conta de gerenciamento que conceda permissões somente de leitura à sua conta RVM. Isso permite que seus GitHub fluxos de trabalho do RVM obtenham dinamicamente uma lista das contas da sua AWS organização quando o script é executado. `generate_providers_and_account_vars.py` Use o código a seguir e `<YOUR RVM Account ID>` substitua pelo Conta da AWS ID que você selecionou na Etapa 2: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Statement", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<YOUR RVM Account ID>:root" }, "Action": [ "organizations:ListAccounts",`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	"organizations:DescribeOrganization", "organizations:DescribeOrganizationalUnit", "organizations:ListRoots", "organizations:ListAWSServiceAccessForOrganization", "organizations:ListDelegatedAdministrators"], "Resource": "*" }] }	

Tarefa	Descrição	Habilidades necessárias
Atualize os valores padrão do repositório de amostra.	Para configurar o RVM para operar em seu ambiente específico Região da AWS, faça o seguinte: 1. Atualize `scripts/generate_providers_and_account_vars.py` e outros arquivos (como a `bootstrap` pasta) com a região apropriada em que você opera. 2. Atualize o `.github/workflows/.env` arquivo com o Conta da AWS ID, a região e quaisquer outras variáveis que você deseja especificar.	DevOps engenheiro

Inicializar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Inicialize o repositório RVM.	Essa etapa é necessária para criar a confiança do OIDC e as funções do IAM usadas pelo próprio pipeline do RVM, para que ele possa começar a operar e vender outras funções. No contexto da sua conta RVM, execute manualmen	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	te um `terraform apply` comando do `scripts/bootstrap` diretório. Forneça todos os valores necessários com base na documentação da variável.	

Configurar operações

Tarefa	Descrição	Habilidades necessárias
Implante as `github-workflow-rvm-readonly` funções `github-workflow-rvm` e em todas as contas.	Escolha um método de implantação que se alinhe às práticas da sua organização, como AFT ou StackSets. Use esse método para implantar as duas funções do IAM no `scripts/assumed_role/main.tf` arquivo (nomes padrão `github-workflow-rvm` e `github-workflow-rvm-readonly`) em cada conta em que você deseja que o RVM possa criar funções de pipeline. Essas funções do IAM têm políticas de confiança que permitem que a função de assunção de função da conta RVM (ou `readonly` equivalente) a assuma. As funções também têm políticas de permissão do IAM que	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	permitem ler e escrever (a menos que usem a `readonly` função) funções correspon dentes`github-workflow-role-*` .	
Execute o `generate_providers_and_account_vars` fluxo de trabalho.	Para configurar seu RVM para que ele esteja pronto para criar funções de pipeline, faça o seguinte: 1. Execute o `generate_providers_and_account_vars` fluxo de trabalho usando workflow_dispatch. 2. Mescle o PR que o fluxo de trabalho cria. Depois que o fluxo de trabalho for concluído, o RVM estará pronto para: • Aceite solicitações de novas funções no pipeline. • Crie funções de somente leitura ou de leitura e gravação conforme solicitado. • Implante funções de acordo com o especificado Contas da AWS.	DevOps engenheiro

Solução de problemas

Problema	Solução
Eu criei uma função usando o RVM, mas GitHub não consigo assumi-la.	Verifique se o nome do GitHub repositório corresponde ao nome fornecido ao `github_workflow_roles` módulo. As funções são definidas de forma que somente um repositório possa assumi-las. Da mesma forma, verifique se a ramificação usada no GitHub pipeline corresponde ao nome da ramificação fornecida ao `github_workflow_roles` módulo. Normalmente, as funções criadas pelo RVM com permissões de gravação só podem ser usadas por fluxos de trabalho com escopo na `main` ramificação (ou seja, implantações provenientes de). `main`
Minha função de somente leitura está falhando ao executar seu pipeline porque não tem permissões para ler um recurso específico.	Embora a `ReadOnlyAccess` política forneça amplas permissões somente para leitura, ela não tem algumas ações de leitura (por exemplo, determinadas AWS Security Hub ações). Você pode adicionar permissões de ação específicas usando o `inline_policy_readonly` parâmetro do `github-workflow-roles` módulo.

Recursos relacionados

- Práticas recomendadas de uso AWS CloudFormation StackSets
- Organizando seu AWS ambiente usando várias contas
- Visão geral do AWS Control Tower Account Factory for Terraform (AFT)
- Melhores práticas políticas

Mais informações

Usando GitHub ambientes

GitHub ambientes são uma abordagem alternativa às restrições baseadas em filiais para acesso a funções. Se você preferir usar um GitHub ambiente, veja a seguir um exemplo da sintaxe de uma condição adicional na política de confiança do IAM. Essa sintaxe especifica que a função só pode ser usada quando a GitHub ação está sendo executada no `Production` ambiente.

```
"StringLike": {
    "token.actions.githubusercontent.com:sub": "repo:octo-org/octo-
repo:environment:Production"
}
```

O exemplo de sintaxe usa os seguintes valores de espaço reservado:

- `octo-org`é o nome GitHub da organização.
- `octo-repo`é o nome do repositório.
- `Production`é o nome específico do GitHub ambiente.

Publique CloudWatch métricas da Amazon em um arquivo CSV

Criado por Abdullahi Olaoye (AWS)

Resumo

Esse padrão usa um script Python para recuperar as métricas da CloudWatch Amazon e converter as informações métricas em um arquivo de valores separados por vírgula (CSV) para melhorar a legibilidade. O script usa o serviço da AWS cujas métricas devem ser recuperadas como um argumento obrigatório. Você pode especificar a região da AWS e o perfil de credencial da AWS como argumentos opcionais. Se você não especificar esses argumentos, o script usará a região e o perfil padrão configurados para a estação de trabalho em que o script é executado. Depois que o script é executado, ele gera e armazena um arquivo CSV no mesmo diretório.

Consulte a seção Anexos para ver o script e os arquivos associados fornecidos com esse padrão.

Pré-requisitos e limitações

Pré-requisitos

- Python 3.x
- AWS Command Line Interface (AWS CLI)

Limitações

O script atualmente é compatível com os seguintes serviços AWS:

- AWS Lambda
- Nuvem de computação elástica da Amazon (Amazon EC2)
  - Por padrão, o script não coleta métricas de volume do Amazon Elastic Block Store (Amazon EBS) Para coletar métricas do Amazon EBS, você deve modificar o `metrics.yaml` arquivo anexado.
- Amazon Relational Database Service (Amazon RDS)
  - No entanto, o script não é compatível com o Amazon Aurora.
- Application Load Balancer
- Network Load Balancer
- Amazon API Gateway

Ferramentas

- CloudWatchA Amazon é um serviço de monitoramento criado para DevOps engenheiros, desenvolvedores, engenheiros de confiabilidade de sites (SREs) e gerentes de TI. CloudWatch fornece dados e insights acionáveis para ajudá-lo a monitorar seus aplicativos, responder às mudanças de desempenho em todo o sistema, otimizar a utilização de recursos e obter uma visão unificada da integridade operacional. CloudWatch coleta dados operacionais e de monitoramento na forma de registros, métricas e eventos e fornece uma visão unificada dos recursos, aplicativos e serviços da AWS que são executados na AWS e em servidores locais.

Épicos

Instalar e configurar os pré-requisitos

Tarefa	Descrição	Habilidades necessárias
Instalar os pré-requisitos.	Execute o seguinte comando: `$ pip3 install -r requirements.txt`	Desenvolvedor
Configure a AWS CLI.	Execute o seguinte comando: `$ aws configure`	Desenvolvedor

Configure o script do Python

Tarefa	Descrição	Habilidades necessárias
Abra o script.	Para alterar a configuração padrão do script, abra `metrics.yaml` .	Desenvolvedor
Defina o período para o script.	Esse é o período de tempo para buscar. O período padrão é 5 minutos (300 segundos).	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Você pode alterar o período, mas observe as seguintes limitações: • Se o valor de horas especificado estiver entre 3 horas e 15 dias atrás, use um múltiplo de 60 segundos (1 minuto) para o período. • Se o valor de horas especificado estiver entre 15 horas e 63 dias atrás, use um múltiplo de 300 segundos (5 minutos) para o período. • Se o valor de horas especificado for maior que 63 dias atrás, use um múltiplo de 3.600 segundos (1 hora) para o período. Caso contrário, a operação da API não retornará nenhum ponto de dados.	
Defina as horas para o script.	Esse valor especifica quantas horas de métricas você deseja buscar. O valor padrão é 1 hora. Para recuperar vários dias de métricas, forneça o valor em horas. Por exemplo, por 2 dias, especifique 48.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Altere os valores das estatísticas do script.	(Opcional) O valor das estatísticas globais é `Average`, usado ao buscar métricas que não têm um valor estatístico específico atribuído. O script suporta os valores estatísticos `MaximumSampleCount` , `Sum` e.	Desenvolvedor

Execute o script do Python

Tarefa	Descrição	Habilidades necessárias

Executar o script.	Use o seguinte comando:
	`$ python3 cwreport.py <service>`
	Para ver uma lista de valores de serviço e os parâmetros opcionais `region` e `profile` , execute o seguinte comando:
	`$ python3 cwreport.py -h`
	Para obter mais informações sobre os parâmetros opcionais, consulte a seção Informações adicionais.
		Desenvolvedor

Recursos relacionados

- Como configurar a AWS CLI
- Usando CloudWatch métricas da Amazon
- CloudWatch Documentação da Amazon
- EC2 CloudWatch Métricas
- Métricas do AWS Lambda
- Métricas do Amazon RDS
- Métricas do Application Load Balancer
- Métricas do Network Load Balancer
- Métricas para Amazon API Gateway

Mais informações

Uso do script

```
$ python3 cwreport.py -h
```

Exemplo de sintaxe

```
python3 cwreport.py <service> <--region=Optional Region> <--profile=Optional credential
 profile>
```

Parâmetros

- service (obrigatório) – O serviço no qual você deseja executar o script. Atualmente, o script oferece suporte aos seguintes serviços: AWS Lambda, Amazon, EC2 Amazon RDS, Application Load Balancer, Network Load Balancer e API Gateway.
- region (opcional) – A região da AWS da qual buscar métricas. A região padrão é `ap-southeast-1`.
- profile (opcional) – O perfil nomeado pela AWS CLI a ser usado. Se esse parâmetro não for especificado, o perfil de credencial configurado padrão será usado.

Exemplos

- Para usar a região padrão `ap-southeast-1` e as credenciais configuradas padrão para obter métricas da Amazon EC2 : `$ python3 cwreport.py ec2`
- Para especificar uma região e buscar métricas do API Gateway: `$ python3 cwreport.py apigateway --region us-east-1`
- Para especificar um perfil da AWS e obter EC2 métricas da Amazon: `$ python3 cwreport.py ec2 --profile testprofile`
- Para especificar a região e o perfil para obter EC2 métricas da Amazon: `$ python3 cwreport.py ec2 --region us-east-1 --profile testprofile`

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Remova EC2 as entradas Contas da AWS da Amazon em frente AWS Managed Microsoft AD usando a AWS Lambda automação

Criado pelo Dr. Rahul Sharad Gaikwad (AWS) e Tamilselvan P (AWS)

Resumo

O Active Directory (AD) é uma ferramenta de script da Microsoft que gerencia as informações do domínio e as interações do usuário com os serviços de rede. É amplamente usado entre provedores de serviços gerenciados (MSPs) para gerenciar credenciais de funcionários e permissões de acesso. Como os atacantes do AD podem usar contas inativas para tentar invadir uma organização, é importante encontrar contas inativas e desativá-las em um cronograma de manutenção de rotina. Com AWS Directory Service for Microsoft Active Directory, você pode executar o Microsoft Active Directory como um serviço gerenciado. Esse padrão pode ajudar você a configurar a AWS Lambda automação para encontrar e remover rapidamente contas inativas.

Se os cenários a seguir se aplicarem à sua organização, esse padrão poderá ajudá-lo:

- Gerenciamento centralizado do AD — Se sua organização tiver várias Contas da AWS, cada uma com sua própria implantação do AD, pode ser difícil gerenciar contas de usuário e permissões de acesso de forma consistente em todas as contas. Com uma solução de limpeza do AD entre contas, você pode desativar ou remover contas inativas de todas as instâncias do AD de forma centralizada.
- Reestruturação ou migração do AD — Se sua organização planeja reestruturar ou migrar sua implantação do AD, uma solução de limpeza do AD entre contas pode ajudá-lo a preparar o ambiente. A solução pode ajudá-lo a remover contas desnecessárias ou inativas, simplificar o processo de migração e reduzir possíveis conflitos ou problemas.

Ao usar esse padrão, você pode obter os seguintes benefícios:

- Melhore o desempenho do banco de dados e do servidor e corrija vulnerabilidades em sua segurança a partir de contas inativas.
- Se o seu servidor AD estiver hospedado na nuvem, a remoção de contas inativas também pode reduzir os custos de armazenamento e melhorar o desempenho. Suas contas mensais podem diminuir porque as tarifas de largura de banda e os recursos de computação podem diminuir.
- Mantenha possíveis invasores afastados com um Active Directory limpo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa para pais Conta da AWS e uma ou várias contas para crianças. Nesse padrão, uma conta principal é onde o Active Directory é criado. As contas secundárias hospedam servidores Windows e são ingressadas por meio da conta principal do Active Directory.
- Git instalado e configurado em uma estação de trabalho local.
- Terraform instalado e configurado em uma estação de trabalho local.
- AWS Managed Microsoft AD diretório configurado na conta principal e compartilhado com todas as contas secundárias. Para obter mais detalhes, consulte Tutorial: Compartilhando seu AWS Managed Microsoft AD diretório para uma EC2 associação perfeita ao domínio no Guia de Administração.AWS Directory Service
- Uma conexão de emparelhamento de nuvem privada virtual (VPC) ou AWS Transit Gateway conexão disponível entre a VPC da AWS Directory Service (conta principal) e a VPC das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) (contas secundárias). Para obter mais detalhes, consulte Configurar uma conexão de emparelhamento de VPC entre o proprietário do diretório e a conta do consumidor do diretório no AWS Directory Service Guia de Administração.
- Uma máquina Windows configurada com o `EC2WindowsUserdata` script em todas as contas principal e secundária. O arquivo de script está disponível na raiz do repositório de código desse padrão.
- Uma função entre contas AWS Identity and Access Management (IAM) disponível em cada conta secundária configurada com uma política de confiança para permitir o uso de uma AWS Lambda função da conta principal. Para obter mais informações, consulte Enviar e receber eventos entre a Amazon Contas da AWS EventBridge no Guia do EventBridge usuário da Amazon.
- Os seguintes valores secretos estão disponíveis no AWS Systems Manager Parameter Store da conta principal:
  - `domainJoinUser`— Nome de usuário do serviço de diretório
  - `domainJoinPassword`— Senha do serviço de diretório

  Para obter mais informações sobre segredos, consulte Criar um AWS Secrets Manager segredo no Guia do AWS Secrets Manager usuário.

Limitações

- A criação de um recurso em uma conta infantil não é automatizada com o Terraform. Você deve criar os seguintes recursos manualmente usando o AWS Management Console:
  - EventBridge Regra da Amazon para enviar os eventos de EC2 rescisão da Amazon para a conta principal
  - Criação de função EC2 entre contas da Amazon na conta infantil com política de confiança
  - Emparelhamento de VPC ou conexão Transit Gateway
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- Terraform versão 1.1.9 ou posterior
- Terraform AWS Provider versão 3.0 ou superior

Arquitetura

O diagrama a seguir mostra a arquitetura de alto nível da solução.

O diagrama da arquitetura ilustra o seguinte processo:

1. Em contas infantis, a EventBridge regra coleta todos os eventos de EC2 rescisão da Amazon. A regra envia os eventos EventBridge que estão presentes na conta principal.
2. Da conta principal, EventBridge coleta todos os eventos e contém a regra para acionar a função `ADcleanup-Lambda` Lambda.
3. A conta principal recebe todos os eventos de encerramento da conta principal ou secundária e aciona a função Lambda.
4. A função Lambda faz a chamada para grupos do Amazon Auto EC2 Scaling usando o módulo boto do Python e obtém o ID aleatório da instância. O ID da instância é usado para executar comandos do Systems Manager.
5. A função Lambda faz outra chamada para a Amazon EC2 usando o módulo boto. A função Lambda obtém os endereços IP privados dos servidores Windows em execução e armazena os endereços em uma variável temporária. Nas etapas 5.1 e 5.2, as EC2 instâncias do Windows em execução são coletadas de contas secundárias.

6. A função Lambda faz outra chamada para o Systems Manager para obter as informações do computador ao qual está conectado. AWS Directory Service
7. Um AWS Systems Manager documento ajuda a executar o PowerShell comando nos servidores Amazon EC2 Windows para obter os endereços IP privados dos computadores conectados ao AD. (O documento Systems Manager usa o ID da instância obtido na etapa 4.)
8. O nome de usuário e as senhas do domínio AD são armazenados no AWS Systems Manager Parameter Store. AWS Lambda e o Systems Manager fazem uma chamada para o Parameter Store e obtêm os valores de nome de usuário e senha a serem usados para se conectar ao AD.
9. Usando o documento Systems Manager, o PowerShell script é executado no servidor Amazon EC2 Windows usando o ID da instância obtido anteriormente na etapa 4.
10. A Amazon EC2 se conecta AWS Directory Service usando PowerShell comandos e remove os computadores que não estão em uso ou inativos.

Ferramentas

AWS serviços

- AWS Directory Servicefornece várias maneiras de usar o Microsoft Active Directory (AD) com outros Serviços da AWS , como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) para SQL Server e FSx Amazon para Windows File Server.
- AWS Directory Service for Microsoft Active Directorypermite que suas cargas de trabalho e AWS recursos com reconhecimento de diretório usem o Microsoft Active Directory no. Nuvem AWS
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los. Com o IAM, você pode especificar em quem ou o que pode acessar serviços e recursos AWS, gerenciar centralmente permissões refinadas e analisar o acesso para refinar as permissões. AWS

- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala.
- AWS Systems Manager os documentos definem as ações que o Systems Manager executa em suas instâncias gerenciadas. O Systems Manager inclui mais de 100 documentos pré-configurados, que você pode usar especificando parâmetros no runtime.
- AWS Systems Manager O Parameter Store é um recurso AWS Systems Manager e fornece armazenamento seguro e hierárquico para gerenciamento de dados de configuração e gerenciamento de segredos.

Outras ferramentas

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.
- PowerShellé um programa de gerenciamento de automação e configuração da Microsoft executado em Windows, Linux e macOS.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub aws-lambda-ad-cleanup-terraform-samples.

Práticas recomendadas

- Ingresse automaticamente em domínios.Ao iniciar uma instância do Windows que fará parte de um AWS Directory Service domínio, entre no domínio durante o processo de criação da instância, em vez de adicioná-la manualmente posteriormente. Para ingressar automaticamente em um domínio, selecione o diretório correto na lista suspensa Diretório de ingresso no domínio ao iniciar uma nova instância. Para obter mais detalhes, consulte Unir perfeitamente uma instância EC2 do Amazon

Windows ao seu AWS Managed Microsoft AD Active Directory no Guia de AWS Directory Service Administração.

- Exclua contas não utilizadas.É comum encontrar contas no AD que nunca foram usadas. Assim como contas desativadas ou inativas que permanecem no sistema, contas não utilizadas negligenciadas podem desacelerar seu sistema AD ou tornar sua organização vulnerável a violações de dados.
- Automatize as limpezas do Active Directory.Para ajudar a mitigar os riscos de segurança e evitar que contas obsoletas afetem o desempenho do AD, é necessário realizar limpezas do AD em intervalos regulares. Você pode realizar a maioria das tarefas de gerenciamento e limpeza do AD escrevendo scripts. Exemplos de tarefas incluem remover contas desativadas e inativas, excluir grupos vazios e inativos e localizar contas de usuário e senhas expiradas.

Épicos

Configurar contas infantis

Tarefa	Descrição	Habilidades necessárias
Crie uma função entre contas na conta da criança.	Para criar uma função entre contas em uma conta secundária, faça o seguinte: 1. Para cada conta secundária, crie uma função nomeada `ec2crossaccountrole` usando a política gerenciada chamada `AmazonEC2ReadOnlyAccess` . (Para obter mais informações, consulte Criar uma função usando políticas de confiança personalizadas na documentação do IAM.)	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	2. Na seção Política de confiança personalizada, adicione o seguinte código: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "ec2.amazonaws.com" }, "Action": "sts:AssumeRole" }, { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::${Parentaccountid}:role/ADcleanuprole" }, "Action": "sts:AssumeRole" } ] }`	

Tarefa	Descrição	Habilidades necessárias
Crie uma regra de evento na conta da criança.	Para criar uma EventBridge regra para cada conta infantil, faça o seguinte: 1. Faça login na criança e Conta da AWS, em seguida, abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/. 2. No painel de navegação, escolha Regras. 3. Escolha Create rule. 4. Insira um Nome e, opcionalmente, uma descrição para a regra. 5. Para Barramento de eventos, selecione Barramento de eventos padrão da AWS. 6. Em Tipo de regra, escolha Regra com um padrão de evento. 7. Escolha Próximo. 8. Para Padrão de evento, cole o seguinte código: `{ "source": ["aws.ec2"], "detail-type": ["EC2 Instance State-change Notification"], "detail": {`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre>"state": ["terminated"]
	}
	}</pre>
	9. Escolha Próximo.
	10. Para Tipo de destino, escolha Barramento de eventos em uma conta ou região diferente.Para Barramento de eventos como destino, insira o Amazon Resource Name (ARN) do barramento de eventos para a conta principal.
	11. Em Função de execução, escolha Criar uma nova função para esse recurso específico.
	12. Escolha Avançar para revisar os detalhes da nova regra e, em seguida, escolha Criar.
	
	Para obter mais detalhes, consulte Criação de regras que reagem a eventos na Amazon EventBridge no Guia EventBridge do usuário da Amazon.	

Tarefa	Descrição	Habilidades necessárias
Crie uma EC2 instância e participe do AD.	Para criar uma EC2 instância para o Windows, faça o seguinte: 1. Use o `EC2Windows sUserdata` script que está disponível no repositório de código desse padrão. 2. No script de dados do usuário, revise o código a seguir para usar seus `Directory service addresses` valores da conta principal: `set-DnsClientServerAddress -InterfaceIndex 6 -ServerAddresses $(Directory service addresses)`	DevOps engenheiro

Configurar a estação de trabalho local

Tarefa	Descrição	Habilidades necessárias
Crie uma pasta de projeto e adicione os arquivos.	Para clonar o repositório e criar uma pasta de projeto, faça o seguinte: 1. Abra o GitHub repositório desse padrão. 2. Escolha o botão Código para ver as opções de	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	clonagem no menu suspenso Clonar.
	3. Na guia HTTPS, copie o URL fornecido em Clone usando o URL da web.
	4. Crie uma pasta na sua máquina e nomeie-a com o nome do seu projeto.
	5. Abra um terminal em sua máquina local e navegue até essa pasta.
	6. Para clonar o repositório git, use o comando a seguir.
	`git clone <repository-URL>.git`
	7. Depois que o repositório for clonado, use o comando a seguir para acessar o diretório clonado.
	`cd <directory name>/terraform-aws-lambda-ad-cleanup/multiple-account-cleanup`
	8. No repositório clonado, abra esse projeto em um ambiente de desenvolvimento integrado (IDE) de sua escolha.	

Tarefa	Descrição	Habilidades necessárias
Crie o `adcleanup.zip` arquivo.	Para compactar o `lambda_function.py` arquivo, execute o seguinte comando: `zip -r adcleanup.zip lambda_function.py`	DevOps engenheiro

Provisione a arquitetura de destino usando a configuração do Terraform

Tarefa	Descrição	Habilidades necessárias
Forneça valores para as variáveis do Terraform.	Para a conta secundária, forneça valores para as seguintes `arn` variáveis como tipos de string no `terraform.tfvars` arquivo: • `lambda_env_cross_role_arn` • `child_account_cross_role_arn`	DevOps engenheiro
Inicialize a configuração do Terraform.	Para inicializar seu diretório de trabalho que contém os arquivos do Terraform, execute o seguinte comando: `terraform init`	DevOps engenheiro
Pré-visualize as alterações.	Você pode visualizar as alterações que o Terraform fará na infraestrutura antes que sua infraestrutura seja implantada. Para validar se o Terraform fará as alterações	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	conforme necessário, execute o seguinte comando: `terraform plan –– var-file=examples/ terraform.tfvars`	
Execute as ações propostas.	Para verificar se os resultados do `terraform plan` comando são os esperados, faça o seguinte: 1. Execute o seguinte comando: `terraform apply` 2. Faça login no AWS Management Console e verifique se os recursos estão presentes.	DevOps engenheiro

Verificar a implantação

Tarefa	Descrição	Habilidades necessárias
Execute e teste a função Lambda.	Para verificar se a implantação ocorreu com êxito, faça o seguinte: 1. Faça login no AWS Management Console e abra o console Lambda. Abra a página Funções e selecione o nome da função que começa com ADcleanup-Lambda-*.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	2. Na página de visão geral da função, escolha Testar na guia Código na seção Fonte do código. 3. Para salvar o evento de teste, forneça um nome para o evento e escolha Salvar. Para testar o evento, escolha Testar novamente. Os resultados da execução mostram a saída da função.	

Tarefa	Descrição	Habilidades necessárias
Veja os resultados da execução da EventBridge regra na conta principal.	Para ver os resultados da EventBridge regra baseada nos eventos de EC2 rescisão da Amazon na conta principal, faça o seguinte: 1. Encerre EC2 instâncias da conta principal. 2. Abra o console Lambda da conta principal. Abra a página Funções e selecione o nome da função que começa com ADcleanup-Lambda-*. 3. Escolha a guia Monitor e escolha Exibir CloudWatch registros. No CloudWatch console, a página Grupos de registros mostra os resultados da função Lambda.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Veja os resultados da execução da EventBridge regra na conta secundária.	Para ver os resultados da EventBridge regra baseada nos eventos de EC2 rescisão da Amazon da conta da criança, faça o seguinte: 1. Encerre EC2 instâncias da conta da criança. 2. Abra o console Lambda da conta principal. Abra a página Funções e selecione o nome da função que começa com ADcleanup-Lambda-*. 3. Escolha a guia Monitor e escolha Exibir CloudWatch registros. No CloudWatch console, a página Grupos de registros mostra os resultados da função Lambda.	DevOps engenheiro

Limpe a infraestrutura após o uso

Tarefa	Descrição	Habilidades necessárias
Limpe a infraestrutura.	Para limpar a infraestrutura que você criou, use o seguinte comando: `terraform destroy`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para confirmar o `destroy` comando, digite`yes`.	
Verifique após a limpeza.	Verifique se os recursos foram removidos com sucesso.	DevOps engenheiro

Solução de problemas

Problema	Solução
Problema de conexão entre AWS Directory Service (conta principal) e EC2 instância da Amazon (conta secundária) — Você não consegue associar os computadores da conta secundária ao AD, mesmo que o emparelhamento de VPC esteja disponível.	Adicione roteamento no VPCs. Para obter instruções, consulte Configurar uma conexão de emparelhamento de VPC entre o proprietário do diretório e a conta do consumidor do diretório na documentação. AWS Directory Service

Recursos relacionados

AWS documentação

- Amazon EventBridge e AWS Identity and Access Management
- Configurar permissões de instância obrigatórias para o Systems Manager
- Gerenciamento de identidade e acesso para AWS Directory Service
- Políticas de IAM baseadas em identidade para Lambda
- Associe manualmente uma instância EC2 do Amazon Windows ao seu AWS Managed Microsoft AD Active Directory
- Remova EC2 as entradas da Amazon na mesma forma Conta da AWSAWS Managed Microsoft AD usando a AWS Lambda automação

Outros recursos

- AWS Provedor (documentação do Terraform)

- Configuração de back-end (documentação do Terraform)
- Instale o Terraform (documentação do Terraform)
- Módulo de inicialização do Python (repositório Python Package Index)
- Download do binário do Terraform (documentação do Terraform)

Remova EC2 as entradas da Amazon na mesma forma Conta da AWSAWS Managed Microsoft AD usando a AWS Lambda automação

Criado pelo Dr. Rahul Sharad Gaikwad (AWS) e Tamilselvan P (AWS)

Resumo

O Active Directory (AD) é uma ferramenta de script da Microsoft que gerencia as informações do domínio e as interações do usuário com os serviços de rede. É amplamente usado entre provedores de serviços gerenciados (MSPs) para gerenciar credenciais de funcionários e permissões de acesso. Como os atacantes do AD podem usar contas inativas para tentar invadir uma organização, é importante encontrar contas inativas e desativá-las em um cronograma de manutenção de rotina. Com AWS Directory Service for Microsoft Active Directory, você pode executar o Microsoft Active Directory como um serviço gerenciado.

Esse padrão pode ajudar você a configurar a AWS Lambda automação para encontrar e remover rapidamente contas inativas. Ao usar esse padrão, você pode obter os seguintes benefícios:

- Melhore o desempenho do banco de dados e do servidor e corrija vulnerabilidades em sua segurança a partir de contas inativas.
- Se o seu servidor AD estiver hospedado na nuvem, a remoção de contas inativas também pode reduzir os custos de armazenamento e melhorar o desempenho. Suas contas mensais podem diminuir porque as tarifas de largura de banda e os recursos de computação podem diminuir.
- Mantenha possíveis invasores afastados com um Active Directory limpo.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Git instalado e configurado em uma estação de trabalho local.
- Terraform instalado e configurado em uma estação de trabalho local.
- Computador Windows com módulos do Active Directory (`ActiveDirectory`).
- Um diretório AWS Managed Microsoft AD e credenciais armazenadas em um AWS Systems Manager parâmetro no Parameter Store.

- AWS Identity and Access Management Função (IAM) com permissões para a Serviços da AWS listada em Ferramentas. Para obter mais informações sobre o IAM, consulte Recursos relacionados.

Limitações

- Esse padrão não é compatível com a configuração de várias contas.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- Terraform versão 1.1.9 ou posterior
- Terraform AWS Provider versão 3.0 ou superior

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. A Amazon EventBridge aciona a AWS Lambda função com base em uma expressão cron. (Para esse padrão, a programação da expressão cron é uma vez por dia.)
2. A função e a política necessárias do IAM são criadas e anexadas AWS Lambda por meio do Terraform.
3. A AWS Lambda função é executada e chama os grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Groups usando o módulo de inicialização do Python. A função Lambda obtém o ID da instância aleatória. O ID da instância é usado para executar AWS Systems Manager comandos.
4. AWS Lambda faz outra chamada para a Amazon EC2 usando o módulo boto e obtém os endereços IP privados dos servidores Windows em execução e armazena os endereços em uma variável temporária.
5. AWS Lambda faz outra chamada para o Systems Manager para obter as informações do computador ao qual está conectado AWS Directory Service.

6. Um AWS Systems Manager documento ajuda a executar o PowerShell script nos servidores Amazon EC2 Windows para obter os endereços IP privados dos computadores conectados ao AD.
7. O nome de usuário e as senhas do domínio AD são armazenados no AWS Systems Manager Parameter Store. AWS Lambda e o Systems Manager fazem uma chamada para o Parameter Store e obtêm os valores de nome de usuário e senha a serem usados para conectar o AD.
8. Usando o documento Systems Manager, o PowerShell script é executado no servidor Amazon EC2 Windows usando o ID da instância obtido anteriormente na etapa 3.
9. A Amazon EC2 se conecta AWS Directory Service usando PowerShell comandos e remove os computadores que não estão em uso ou inativos.

Ferramentas

Serviços da AWS

- AWS Directory Servicefornece várias maneiras de usar o Microsoft Active Directory (AD) com outros Serviços da AWS , como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) para SQL Server e FSx Amazon para Windows File Server.
- AWS Directory Service for Microsoft Active Directorypermite que suas cargas de trabalho e AWS recursos com reconhecimento de diretório usem o Microsoft Active Directory no. Nuvem AWS
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los. Com o IAM, você pode especificar em quem ou o que pode acessar serviços e recursos AWS, gerenciar centralmente permissões refinadas e analisar o acesso para refinar as permissões. AWS
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando

necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala.
- AWS Systems Manager os documentos definem as ações que o Systems Manager executa em suas instâncias gerenciadas. O Systems Manager inclui mais de 100 documentos pré-configurados, que você pode usar especificando parâmetros no runtime.
- AWS Systems Manager O Parameter Store é um recurso AWS Systems Manager e fornece armazenamento seguro e hierárquico para gerenciamento de dados de configuração e gerenciamento de segredos.

Outras ferramentas

- HashiCorp O Terraform é uma ferramenta de infraestrutura de código aberto como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.
- PowerShellé um programa de gerenciamento de automação e configuração da Microsoft executado em Windows, Linux e macOS.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código C

O código desse padrão está disponível no repositório da solução GitHub Custom AD Cleanup Automation.

Práticas recomendadas

- Ingresse automaticamente em domínios.Ao iniciar uma instância do Windows que fará parte de um AWS Directory Service domínio, entre no domínio durante o processo de criação da instância, em vez de adicioná-la manualmente posteriormente. Para ingressar automaticamente em um domínio, selecione o diretório correto na lista suspensa Diretório de ingresso no domínio ao iniciar uma nova instância. Para obter mais detalhes, consulte Unir perfeitamente uma instância EC2 do Amazon Windows ao seu AWS Managed Microsoft AD Active Directory no Guia de AWS Directory Service Administração.

- Exclua contas não utilizadas.É comum encontrar contas no AD que nunca foram usadas. Assim como contas desativadas ou inativas que permanecem no sistema, contas não utilizadas negligenciadas podem desacelerar seu sistema AD ou tornar sua organização vulnerável a violações de dados.
- Automatize as limpezas do Active Directory.Para ajudar a mitigar os riscos de segurança e evitar que contas obsoletas afetem o desempenho do AD, é necessário realizar limpezas do AD em intervalos regulares. Você pode realizar a maioria das tarefas de gerenciamento e limpeza do AD escrevendo scripts. Exemplos de tarefas incluem remover contas desativadas e inativas, excluir grupos vazios e inativos e localizar contas de usuário e senhas expiradas.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Crie uma pasta de projeto e adicione os arquivos.	Para clonar o repositório e criar uma pasta de projeto, faça o seguinte: 1. Abra o GitHub repositório desse padrão. 2. Escolha o botão Código para ver as opções de clonagem no menu suspenso Clonar. 3. Na guia HTTPS, copie o URL fornecido em Clone usando o URL da web. 4. Crie uma pasta na sua máquina e nomeie-a com o nome do seu projeto. 5. Abra um terminal em sua máquina local e navegue até essa pasta.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	6. Para clonar o repositório git, use o comando a seguir.
	
	`git clone <repository-URL>.git`
	
	7. Depois que o repositório for clonado, use o comando a seguir para acessar o diretório clonado.
	
	`cd <directory name>`
	
	8. No repositório clonado, abra esse projeto em um ambiente de desenvolvimento integrado (IDE) de sua escolha.	

Provisione a arquitetura de destino usando a configuração do Terraform

Tarefa	Descrição	Habilidades necessárias
Inicialize a configuração do Terraform.	Para inicializar seu diretório de trabalho que contém os arquivos do Terraform, execute o comando a seguir. `terraform init`	DevOps engenheiro
Pré-visualize as alterações.	Você pode visualizar as alterações que o Terraform fará na infraestrutura antes que sua infraestrutura seja implantada. Para validar se o Terraform fará as alterações	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	conforme necessário, execute o comando a seguir. `terraform plan`	
Execute as ações propostas.	Para verificar se os resultados do `terraform plan` comando são os esperados, faça o seguinte: 1. Execute o seguinte comando: `terraform apply` 2. Faça login no AWS Management Console e verifique se os recursos estão presentes.	DevOps engenheiro
Limpe a infraestrutura.	Para limpar a infraestrutura que você criou, use o comando a seguir. `terraform destroy` Para confirmar o comando destroy, digite`yes`.	DevOps engenheiro

Verificar a implantação

Tarefa	Descrição	Habilidades necessárias
Execute e teste a função Lambda.	Para verificar se a implantação ocorreu com êxito, faça o seguinte:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	1. Faça login no AWS Management Console e abra o console. Abra a página Funções e selecione o nome da função que começa com ADcleanup-Lambda-*. 2. Na página de visão geral da função, escolha Testar na guia Código na seção Fonte do código. 3. Para salvar o evento de teste, forneça um nome para o evento e escolha Salvar. Em seguida, para testar o evento, escolha Testar novamente. Os resultados da execução mostram a saída da função.	

Tarefa	Descrição	Habilidades necessárias
Veja os resultados da função Lambda.	Nesse padrão, uma EventBridge regra executa a função Lambda uma vez por dia. Para visualizar os resultados da função Lambda, faça o seguinte: 1. Faça login no AWS Management Console e abra o AWS Lambda console. Abra a página Funções e selecione o nome da função que começa com ADcleanup-Lambda-*. 2. Escolha a guia Monitor e escolha Exibir CloudWatch registros. No CloudWatch console, a página de grupos de registros mostra os resultados da função Lambda.	DevOps engenheiro

Limpe a infraestrutura após o uso

Tarefa	Descrição	Habilidades necessárias
Limpe a infraestrutura.	Para limpar a infraestrutura que você criou, use o comando a seguir. `terraform destroy`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para confirmar o comando destroy, digite`yes`.	
Verifique após a limpeza.	Verifique se os recursos foram removidos com sucesso.	DevOps engenheiro

Solução de problemas

Problema	Solução
Se você tentar remover o computador do AD, receberá uma mensagem “Acesso negado”. O computador do AD não pode ser removido porque, por padrão, a ação tenta remover dois endereços IP privados que estão conectados como parte dos serviços do AD.	Para evitar esse erro, use a operação Python a seguir para ignorar os dois primeiros computadores ao listar as diferenças entre a saída de um computador AD e a saída da sua máquina executando o Windows. `Difference = Difference[2:]`
Quando o Lambda executa um PowerShell script em um servidor Windows, ele espera que os módulos do Active Directory estejam disponíveis por padrão. Se os módulos não estiverem disponíveis, uma função Lambda cria um erro que indica “Get- não AdComputer está instalado na instância”.	Para evitar esse erro, instale os módulos necessários usando os dados do usuário das EC2 instâncias. Use o EC2WindowsUserdata script que está no GitHub repositório desse padrão.

Recursos relacionados

AWS documentação

- Amazon EventBridge e AWS Identity and Access Management
- Configurar permissões de instância obrigatórias para o Systems Manager
- Gerenciamento de identidade e acesso para AWS Directory Service

- Associe manualmente uma instância EC2 do Amazon Windows ao seu AWS Managed Microsoft AD Active Directory
- Trabalhando com políticas de IAM baseadas em identidade em AWS Lambda

Outros recursos

- AWS Provedor (documentação do Terraform)
- Configuração de back-end (documentação do Terraform)
- Instale o Terraform (documentação do Terraform)
- Módulo de inicialização do Python (repositório Python Package Index)
- Download do binário do Terraform (documentação do Terraform)

Execute testes de unidade para trabalhos de ETL do Python AWS Glue usando a estrutura pytest

Criado por Praveen Kumar Jeyarajan (AWS) e Vaidy Sankaran (AWS)

Resumo

Você pode executar testes unitários para trabalhos de extração, transformação e carregamento (ETL) do Python AWS Glue em um ambiente de desenvolvimento local, mas replicar esses testes em um DevOps pipeline pode ser difícil e demorado. O teste unitário pode ser especialmente desafiador quando você está modernizando o processo de ETL de mainframe em AWS pilhas de tecnologia. Esse padrão mostra como simplificar os testes de unidade, mantendo intactas as funcionalidades existentes, evitando interrupções nas principais funcionalidades do aplicativo ao lançar novos atributos e mantendo um software de alta qualidade. Você pode usar as etapas e os exemplos de código nesse padrão para executar testes de unidade para trabalhos de ETL do Python AWS Glue usando a estrutura pytest em. AWS CodePipeline Você também pode usar esse padrão para testar e implantar vários AWS Glue trabalhos.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um URI de imagem do Amazon Elastic Container Registry (Amazon ECR) para AWS Glue sua biblioteca, baixado da Galeria Pública do Amazon ECR
- Terminal Bash (em qualquer sistema operacional) com um perfil para o alvo Conta da AWS e Região da AWS
- Python 3.10 ou posterior
- Pytest
- Biblioteca Moto Python para testes Serviços da AWS

Arquitetura

O diagrama a seguir descreve como incorporar testes unitários para processos de AWS Glue ETL baseados em Python em um pipeline típico AWS DevOps de escala empresarial.

O diagrama mostra o seguinte fluxo de trabalho:

1. No estágio de origem, AWS CodePipeline usa um bucket versionado do Amazon Simple Storage Service (Amazon S3) para armazenar e gerenciar ativos de código-fonte. Esses ativos incluem um exemplo de job (`sample.py`) de ETL em Python, um arquivo de teste unitário (`test_sample.py`) e um modelo. AWS CloudFormation Em seguida, CodePipeline transfere o código mais recente da ramificação principal para o AWS CodeBuild projeto para processamento adicional.
2. No estágio de criação e publicação, o código mais recente do estágio de origem anterior é testado em unidade com a ajuda de uma imagem AWS Glue pública do Amazon ECR. Em seguida, o relatório do teste é publicado nos grupos de CodeBuild relatórios. A imagem do contêiner no repositório público do Amazon ECR para AWS Glue bibliotecas inclui todos os binários necessários para executar tarefas ETL PySparkbaseadas em testes unitários localmente. AWS Glue O repositório público de contêineres tem três tags de imagem, uma para cada versão suportada pelo AWS Glue. Para fins de demonstração, esse padrão usa a tag de imagem `glue_libs_4.0.0_image_01`. Para usar essa imagem de contêiner como imagem de tempo de execução em CodeBuild, copie o URI da imagem que corresponde à tag de imagem que você pretende usar e, em seguida, atualize o `pipeline.yml` arquivo no GitHub repositório do `TestBuild` recurso.
3. Na fase de implantação, o CodeBuild projeto é lançado e ele publica o código em um bucket do Amazon S3 se todos os testes forem aprovados.
4. O usuário implanta a AWS Glue tarefa usando o CloudFormation modelo na `deploy` pasta.

Ferramentas

Serviços da AWS

- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- AWS Glueé um serviço ETL totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e desempenho líderes do setor.

Outras ferramentas

- Python é uma linguagem de programação interpretada de alto nível e de uso geral.
- Moto é uma biblioteca Python para testes. Serviços da AWS
- O Pytest é uma estrutura para escrever pequenos testes unitários que se escalam para suportar testes funcionais complexos para aplicativos e bibliotecas.
- A biblioteca Python ETL for AWS Glue é um repositório para bibliotecas Python que são usadas no desenvolvimento local de trabalhos em lote para. PySpark AWS Glue

Repositório de código

O código desse padrão está disponível no repositório GitHub aws-glue-jobs-unit-testing. O repositório inclui os seguintes recursos:

- Um exemplo de AWS Glue tarefa baseada em Python na pasta `src`
- Casos de teste de unidade associados (criados usando a estrutura pytest) na pasta `tests`
- Um CloudFormation modelo (escrito em YAML) na pasta `deploy`

Práticas recomendadas

Segurança para CodePipeline recursos

É uma prática recomendada usar criptografia e autenticação para os repositórios de origem que se conectam aos seus pipelines em. CodePipeline Para obter mais informações, consulte as melhores práticas de segurança na CodePipeline documentação.

Monitoramento e registro de CodePipeline recursos

É uma prática recomendada usar os recursos de AWS registro para determinar quais ações os usuários realizam em sua conta e quais recursos eles usam. Os arquivos de log exibem o seguinte:

- Data e hora das ações.
- Endereço IP de origem das ações
- As ações que falharam devido a permissões inadequadas.

Os recursos de registro estão disponíveis no AWS CloudTrail Amazon CloudWatch Events. Você pode usar CloudTrail para registrar chamadas de AWS API e eventos relacionados feitos por ou em nome do seu Conta da AWS. Para obter mais informações, consulte Logging CodePipeline API de chamadas AWS CloudTrail na CodePipeline documentação.

Você pode usar CloudWatch Eventos para monitorar seus Nuvem AWS recursos e aplicativos em execução AWS. Você também pode criar alertas em CloudWatch Eventos. Para obter mais informações, consulte Monitoramento de CodePipeline eventos na CodePipeline documentação.

Épicos

Implantar o código-fonte

Tarefa	Descrição	Habilidades necessárias
Prepare o arquivo de código para implantação.	1. Faça o download `code.zip` do repositór io GitHub aws-glue-jobs-unit-testing ou crie você mesmo o arquivo.zip usando uma ferramenta de linha de comando. Por exemplo, você pode criar o arquivo .zip no Linux ou Mac executando os seguintes comandos no terminal: `git clone https://g ithub.com/aws-samp les/aws-glue-jobs- unit-testing.git cd aws-glue-jobs- unit-testing git checkout master zip -r code.zip src/ tests/ deploy/` 2. Faça login no AWS Management Consolee	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	escolha o Região da AWS de sua preferência. 3. Crie um bucket do Amazon S3 e, em seguida, carregue o pacote e o `code.zip` arquivo .zip (baixados anteriormente) para o bucket do Amazon S3 que você criou.	

Tarefa	Descrição	Habilidades necessárias
Crie a CloudFormation pilha.	1. Faça login no AWS Management Console e abra o CloudFormation console. 2. Escolha Criar pilha, e, em seguida, selecione Com recursos existentes (importar recursos). 3. Na seção Especificar modelo da página Criar pilha, escolha Carregar um arquivo de modelo e, em seguida, escolha o modelo pipeline.yml (baixado do repositório). GitHub Em seguida, escolha Próximo. 4. Em Nome da pilha glue-unit -testing-pipeline, insira ou escolha um nome de pilha de sua preferência. 5. Para ApplicationStackNa me, use o nome pré-preen chido. glue-codepipeline-app Esse é o nome da CloudFormation pilha criada pelo pipeline. 6. Para BucketName, use o nome pré-preenchido do bucket aws-glue-artifacts-us-east-1. Esse é o nome do bucket do Amazon S3 que contém o arquivo.z ip e é usado pelo pipeline	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	para armazenar artefatos de código. 7. Para CodeZipFile, use o valor code.zip pré-preen chido. Esse é o nome da chave do objeto Amazon S3 de código de amostra. O objeto deve ser um arquivo .zip. 8. Para TestReportGroupNam e, use o nome pré-preen chido. glue-unittest-report Esse é o nome do grupo de relatórios de CodeBuild teste criado para armazenar os relatórios de teste unitário. 9. Escolha Avançar e, em seguida, escolha Avançar novamente na página Configurar opções de pilha. 10. Na página de revisão, em Capacidades, escolha a opção Eu reconheço que CloudFormation pode criar recursos do IAM com nomes personalizados. 11. Selecione Enviar. Depois que a criação da pilha for concluída, você poderá ver os recursos criados na guia Recursos. A pilha leva aproximadamente 5-7 minutos para ser criada.	

Tarefa	Descrição	Habilidades necessárias
	A pilha cria uma CodePipeline visualização usando o Amazon S3 como fonte. Nas etapas acima, o pipeline é aws-glue-unit-test-pipeline.	

Execute os testes de unidade

Tarefa	Descrição	Habilidades necessárias
Execute os testes de unidade no pipeline.	1. Para testar o pipeline implantado, faça login no AWS Management Console e abra o CodePipeline console. 2. Selecione o pipeline criado pela CloudFormation pilha e escolha Release change. O pipeline começa a ser executado (usando o código mais recente no bucket do Amazon S3). 3. Depois que a fase Testar e compilar for concluída, escolha a guia Detalhes e, em seguida, examine os logs. 4. Escolha a guia Relatórios e, em seguida, escolha o relatório de teste em Histórico de relatórios para visualizar os resultados do teste de unidade.	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	5. Depois que o estágio de implantação estiver concluído, execute e monitore o AWS Glue trabalho implantado no AWS Glue console. Para obter mais informações, consulte Monitoramento AWS Glue na AWS Glue documentação.	

Limpe todos os AWS recursos

Tarefa	Descrição	Habilidades necessárias
Limpe os recursos no seu ambiente.	Para evitar custos adicionais de infraestrutura, certifique-se de excluir a pilha depois de experimentar os exemplos fornecidos nesse padrão. 1. Abra o CloudFormation console e selecione a pilha que você criou. 2. Escolha Excluir. Isso exclui todos os recursos que sua pilha criou, incluindo funções AWS Identity and Access Management (IAM), políticas e CodeBuild projetos do IAM.	AWS DevOps, DevOps engenheiro

Solução de problemas

Problema	Solução
A função CodePipeline de serviço não pode acessar o bucket do Amazon S3.	• Para a política anexada à sua função de CodePipeline serviço, adicione `s3:ListBucket` à lista de ações em sua política. Para obter instruções sobre como visualizar a política da função de serviço, consulte Exibir o ARN do pipeline e o ARN da função de serviço (console). Edite a declaração de política para sua função de serviço conforme detalhado em Adicionar permissões à função CodePipeline de serviço. • Para a política baseada em recursos anexada ao bucket de artefatos do Amazon S3 para seu pipeline, também chamada de política de compartimento de artefatos, adicione uma declaração que permita que a função de serviço use CodePipeline a permissão. `s3:ListBucket`
CodePipeline retorna um erro informando que o bucket do Amazon S3 não está versionado.	CodePipeline exige que o bucket de origem do Amazon S3 seja versionado. Ative o controle de versão em seu bucket do Amazon S3. Para obter instruções, consulte Habilitar o controle de versão em buckets.

Recursos relacionados

- AWS Glue
- Desenvolvendo e testando AWS Glue trabalhos localmente
- AWS CloudFormation para AWS Glue

Mais informações

Além disso, você pode implantar os AWS CloudFormation modelos usando o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Implantação rápida de modelos com transformações na CloudFormation documentação.

Configurar um repositório de chart do Helm v3 no Amazon S3

Criado por Abhishek Sharma (AWS)

Resumo

Aviso: CodeCommit A AWS não está mais disponível para novos clientes. Os clientes atuais da AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão ajuda você a gerenciar os gráficos do Helm v3 de forma eficiente ao integrar o repositório do Helm v3 ao Amazon Simple Storage Service (Amazon S3) na nuvem da Amazon web Services (AWS). Para usar esse padrão, você precisa estar familiarizado com o Kubernetes e com o Helm, que é um gerenciador de pacotes do Kubernetes. Usar repositórios Helm para armazenar gráficos e controlar versões de gráficos pode melhorar o tempo médio de restauração (MTTR) durante interrupções.

Esse padrão usa o AWS CodeCommit para a criação do repositório Helm e usa um bucket S3 como repositório de gráficos do Helm, para que os gráficos possam ser gerenciados e acessados centralmente por desenvolvedores em toda a organização.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Python, versão 2.7.12 ou superior.
- pip
- Uma nuvem privada virtual (VPC) com sub-redes e uma instância do Amazon Elastic Compute Cloud (Amazon) EC2
- Git instalado na instância EC2
- Acesso ao AWS Identity and Access Management (IAM) para criar o bucket S3
- Acesso por IAM (programático ou por perfil) ao Amazon S3 a partir da máquina cliente
- CodeCommit Repositório AWS
- AWS Command Line Interface (AWS CLI)

Versões do produto

- Helm v3

- Python, versão 2.7.12 ou superior.

Arquitetura

Pilha de tecnologias de destino

- Amazon S3
- AWS CodeCommit
- Helm
- Kubectl
- Python e pip
- Git
- plugin helm-s3

Arquitetura de destino

Automação e escala

- Você pode incorporar o Helm à sua ferramenta de automação existente integration/continuous delivery (CI/CD (contínua) para automatizar o empacotamento e o controle de versão dos gráficos do Helm (fora do escopo desse padrão).
- GitVersion ou os números de compilação do Jenkins podem ser usados para automatizar o controle de versão dos gráficos.

Ferramentas

- Helm: o Helm é um gerenciador de pacotes Helm para o Kubernetes ajuda a instalar e gerenciar aplicações em seu cluster do Kubernetes.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.
- plugin helm-s3 – O plug-in helm-s3 suporta interação com o Amazon S3. Ele pode ser usado com o Helm v2 ou o Helm v3.

Épicos

Instale e valide o Helm v3

Tarefa	Descrição	Habilidades necessárias
Instalar o cliente do Helm v3	Para baixar e instalar o cliente do Helm no sistema local, execute o seguinte comando: `sudo curl https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3 | bash`	Administrador de nuvem, DevOps engenheiro
Valide a instalação do Helm.	Para validar o cliente do Helm, execute o seguinte comando: `helm version --short`	Administrador de nuvem, DevOps engenheiro

Inicializar um bucket do S3 como um repositório do Helm

Tarefa	Descrição	Habilidades necessárias
Crie um bucket do S3 para charts do Helm.	Crie um bucket exclusivo do S3. No bucket, crie uma pasta denominada `stable/myapp` . O exemplo desse padrão usa `s3://my-helm-charts/stable/myapp` como repositório do gráfico de destino.	Administrador de nuvem, DevOps engenheiro
Instale o plug-in do Helm-s3 para o Amazon S3.	Para instalar o plug-in helm-s3 na máquina cliente, use o comando a seguir: `helm plugin install https://github.com`	Administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`/hypnoglow/helm-s3.git`	
Inicialize o repositório do Helm no Amazon S3.	Para inicializar a pasta de destino como um repositório do Helm, use o comando a seguir: `helm s3 init s3://my-helm-charts/stable/myapp` O comando cria um arquivo `index.yaml` no destino para rastrear todas as informações do gráfico armazenadas nesse local.	Administrador de nuvem, DevOps engenheiro
Verifique o repositório Helm recém-criado.	Para verificar se o `index.yaml` arquivo foi criado, execute o seguinte comando: `aws s3 ls s3://my-helm-charts/stable/myapp/`	Administrador de nuvem, DevOps engenheiro
Adicione o repositório Amazon S3 ao Helm na máquina cliente.	Para adicionar o alias do repositório de destino à máquina cliente Helm, use o seguinte comando: `helm repo add stable-myapp s3://my-helm-charts/stable/myapp/`	Administrador de nuvem, DevOps engenheiro

Package e publique gráficos no repositório Amazon S3 Helm

Tarefa	Descrição	Habilidades necessárias
Clone seus charts do Helm.	Se nenhum gráfico local do Helm estiver presente em seu CodeCommit repositór io, clone-o do seu GitHub repositório executand o o seguinte comando: `git clone <url_of_y our_helm_source_co de>.git`	Administrador de nuvem, DevOps engenheiro
Embalar o chart do Helm local.	Para embalar o gráfico que você criou ou clonou, use o seguinte comando: `helm package ./my-app` Como exemplo, esse padrão usa o `my-app` gráfico. O comando empacota todo o conteúdo da pasta do gráfico `my-app` em um arquivo, que é nomeado usando o número da versão mencionado no arquivo `Chart.yaml` .	Administrador de nuvem, DevOps engenheiro
Armazene o pacote local no repositório do Helm no Amazon S3.	Para fazer o upload do pacote local para o repositório do Helm no Amazon S3, execute o seguinte comando: `helm s3 push ./my-app-0.1.0.tgz stable-my app` No comando, `my-app` é o nome da pasta do gráfico,	Administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`0.1.0` é a versão do gráfico mencionada em `Chart.yaml` e `stable-myapp` é o alias do repositório de destino.	
Pesquise pelo chart do Helm.	Para confirmar se o gráfico aparece localmente e no repositório Amazon S3 Helm, execute o seguinte comando: `helm search repo stable-myapp`	Administrador de nuvem, DevOps engenheiro

Atualize seu repositório Helm

Tarefa	Descrição	Habilidades necessárias
Modificar e embalar o gráfico.	Em `values.yaml` , defina o `replicaCount` valor como e`1`, em seguida, empacote o gráfico, desta vez alterando a versão `Chart.yaml` para`0.1.1`. O controle de versão é obtido idealmente por meio da automação usando ferramentas como os números GitVersion de compilação do Jenkins em um pipeline de CI/CD. A automação do número da versão está fora do escopo desse padrão. Para embalar o gráfico, execute o seguinte comando: `helm package ./my-app/`	Administrador de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Envie a nova versão para o repositório do Helm no Amazon S3.	Para enviar o novo pacote, versão 0.1.1, para o repositório my-helm-chartsHelm no Amazon S3, execute o seguinte comando: `helm s3 push ./my-app-0.1.1.tgz stable-myapp`	Administrador de nuvem, DevOps engenheiro

Verifique o chart do Helm atualizado.	Para confirmar se o gráfico atualizado aparece localmente e no repositório Amazon S3 Helm, execute os seguintes comandos.
	`helm repo update`
	`helm search repo stable-myapp`
		Administrador de nuvem, DevOps engenheiro

Pesquise e instale um gráfico do repositório do Helm no Amazon S3

Tarefa	Descrição	Habilidades necessárias
Pesquise todas as versões do gráfico my-app.	Para ver todas as versões disponíveis de um gráfico, execute o seguinte comando com o `--versions` sinalizador: `helm search repo my-app --versions` Sem o sinalizador, o Helm, por padrão, exibe a versão	DevOps Engenheiro

Tarefa	Descrição	Habilidades necessárias
	mais recente carregada de um gráfico.	
Instale um gráfico do repositório do Helm no Amazon S3.	A instalação automatizada está fora do escopo desse padrão, mas você pode instalar manualmente. Os resultados da pesquisa da tarefa anterior mostram as várias versões do gráfico `my-app`. Para instalar a nova versão (0.1.1) do repositório do Helm no Amazon S3, use o comando a seguir: `helm upgrade --install my-app-release stable-myapp/my-app --version 0.1.1 --namespace dev`	DevOps Engenheiro

Reverter para uma versão anterior usando o Helm

Tarefa	Descrição	Habilidades necessárias
Revise os detalhes de uma revisão específica.	A reversão automatizada está fora do escopo desse padrão, mas você pode reverter para uma versão anterior manualmente. Antes de alternar ou reverter para uma versão funcional e para obter uma camada adicional de validação antes de instalar uma revisão, veja quais valores foram passados	DevOps Engenheiro

Tarefa	Descrição	Habilidades necessárias
	para cada uma das revisões usando o comando a seguir: `helm get values --revision=2 my-app-release`	
Reverter para uma versão anterior.	A reversão automatizada está fora do escopo desse padrão. Para reverter manualmente para uma revisão anterior, use o seguinte comando: `helm rollback my-app-release 1` Este exemplo está revertendo para a revisão número 1.	DevOps Engenheiro

Recursos relacionados

- Documentação do HELM
- Plug-in helm-s3 (licença MIT)
- Amazon S3

Configure um pipeline de CI/CD usando a AWS e o CodePipeline AWS CDK

Criado por Konstantin Zarudaev (AWS), Cizer Pereira (AWS), Lars Kinder (AWS) e Yasha Dabas (AWS)

Início

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais Automatizar seu processo de criação e lançamento de software com integração e entrega contínuas (CI/CD) supports repeatable builds and rapid delivery of new features to your users. You can quickly and easily test each code change, and you can catch and fix bugs before releasing your software. By running each change through your staging and release process, you can verify the quality of your application or infrastructure code. CI/CDincorpora uma cultura, um conjunto de princípios operacionais e um conjunto de práticas que ajudam as equipes de desenvolvimento de aplicativos a realizar alterações de código com mais frequência e confiabilidade). A implementação também é conhecida como pipeline de CI/CD.

Esse padrão define um pipeline reutilizável de integração contínua e entrega contínua (CI/CD) na Amazon Web Services (AWS) com um repositório da AWS. CodeCommit O CodePipeline pipeline da AWS é escrito usando o AWS Cloud Development Kit (AWS CDK) v2.

Usando CodePipeline, você pode modelar os diferentes estágios do seu processo de lançamento de software por meio da interface do AWS Management Console, da AWS Command Line Interface (AWS CLI), da CloudFormation AWS ou da AWS. SDKs Esse padrão demonstra a implementação CodePipeline e seus componentes usando o AWS CDK. Além da estrutura de bibliotecas, o AWS CDK inclui um kit de ferramentas (o comando `cdk` CLI), que é a principal ferramenta para interagir com seu aplicativo do AWS CDK. Entre outras funções, o kit de ferramentas oferece a capacidade de converter uma ou mais pilhas em CloudFormation modelos e implantá-las em uma conta da AWS.

O pipeline inclui testes para validar a segurança de suas bibliotecas de terceiros e ajuda a garantir o lançamento rápido e automatizado nos ambientes especificados. Você pode aumentar a segurança geral de seus aplicativos submetendo-os a um processo de validação.

A intenção desse padrão é acelerar o uso de pipelines de CI/CD para implantar seu código e, ao mesmo tempo, garantir que os recursos implantados sigam as melhores práticas. DevOps Depois de implementar o código de exemplo, você terá uma AWS CodePipeline com processos de linting,

testes, verificação de segurança, implantação e pós-implantação. Esse padrão também inclui etapas para o Makefile. Usando um Makefile, os desenvolvedores podem reproduzir as etapas de CI/CD localmente e aumentar a velocidade do processo de desenvolvimento.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um entendimento básico sobre o seguinte:
  - AWS CDK
  - AWS CloudFormation
  - AWS CodePipeline
  - TypeScript

Limitações

Esse padrão usa o AWS CDK TypeScript apenas para. Ela não abrange outras linguagens suportadas pelo AWS CDK.

Versões do produto

Use as versões mais recentes das seguintes ferramentas:

- AWS Command Line Interface (AWS CLI)
- cfn_nag
- git-remote-codecommit
- Node.js

Arquitetura

Pilha de tecnologias de destino

- AWS CDK
- AWS CloudFormation
- AWS CodeCommit
- AWS CodePipeline

Arquitetura de destino

O pipeline é acionado por uma alteração no CodeCommit repositório da AWS (`SampleRepository`). No início, CodePipeline cria artefatos, se atualiza e inicia o processo de implantação. O pipeline resultante implanta uma solução em três ambientes independentes:

- Dev – Verificação de código em três etapas no ambiente de desenvolvimento ativo
- Teste: ambiente de teste de integração e regressão
- Prod: ambiente de produção

As três etapas incluídas no estágio de desenvolvimento são linting, segurança e testes unitários. Essas etapas são executadas paralelamente para acelerar o processo. Para garantir que o pipeline forneça somente artefatos funcionais, sua execução será interrompida sempre que uma etapa do processo falhar. Depois de uma implantação em fase de desenvolvimento, o pipeline executa testes de validação para verificar os resultados. Em caso de sucesso, o pipeline implantará os artefatos no ambiente de teste, que contém a validação pós-implantação. A etapa final é implantar os artefatos no ambiente do Prod.

O diagrama a seguir mostra o fluxo de trabalho do CodeCommit repositório até os processos de criação e atualização executados por CodePipeline, as três etapas do ambiente de desenvolvimento e a implantação e validação subsequentes em cada um dos três ambientes.

Ferramentas

Serviços da AWS

- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS. Nesse padrão, os CloudFormation modelos podem ser usados para criar um CodeCommit repositório e um pipeline de CodePipeline CI/CD.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.

- CodePipelineA AWS é um serviço de CI/CD que ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

Outras ferramentas

- cfn_nag é uma ferramenta de código aberto que procura padrões em CloudFormation modelos para identificar possíveis problemas de segurança.
- git-remote-codecommité um utilitário para enviar e extrair código de CodeCommit repositórios estendendo o Git.
- O Node.js é um ambiente de tempo de JavaScript execução orientado a eventos projetado para criar aplicativos de rede escaláveis.

Código

O código desse padrão está disponível no repositório de práticas CodePipeline de CI/CD GitHub da AWS.

Práticas recomendadas

Analise os recursos, como políticas do AWS Identity and Access Management (IAM), para confirmar se eles estão alinhados com as melhores práticas organizacionais.

Épicos

Instalar as ferramentas

Tarefa	Descrição	Habilidades necessárias
Instale ferramentas no Linux ou no macOS.	Se você estiver usando macOS ou Linux, poderá instalar as ferramentas executando o seguinte comando no terminal de sua preferência ou usando o Homebrew para Linux.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`brew install`
	`brew install git-remote-codecommit`
	`brew install ruby brew-gem`
	`brew-gem install cfn-nag`	

Configure a AWS CLI.	Para configurar a AWS CLI, use as instruções para seu sistema operacional: • Windows: etapas de configuração para conexões HTTPS com CodeCommit repositórios da AWS no Windows com o auxiliar de credenciais da AWS CLI • Linux, macOS, Unix: etapas de configuração para conexões HTTPS com CodeCommit repositórios da AWS em Linux, macOS ou Unix com o auxiliar de credenciais da AWS CLI	DevOps engenheiro

Configure a implantação inicial

Tarefa	Descrição	Habilidades necessárias
Faça download ou clonagem do código.	Para obter o código usado por esse padrão, siga um destes procedimentos:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	• Baixe o código-fonte mais recente das versões no GitHub repositório e descompacte o arquivo baixado em uma pasta.
	• Clonagem do projeto executando o seguinte comando:
	
	`git clone --depth 1 https://github.com/aws-samples/aws-codepipeline-cicd.git`
	
	Remova o diretório `.git` do repositório clonado.
	
	`cd ./aws-codepipeline-cicd`
	`rm -rf ./.git`
	
	Posteriormente, você usará um CodeCommit repositório AWS recém-criado como origem remota.	

Tarefa	Descrição	Habilidades necessárias

Conecte-se à conta da AWS.	Você pode se conectar usando um token de segurança temporário ou autenticação de zona de pouso. Para confirmar que você está usando a conta e a região da AWS corretas, execute os comandos a seguir.
	`AWS_REGION="eu-west-1"`
	`ACCOUNT_NUMBER=$(aws sts get-caller-identity --query Account --output text)`
	`echo "${ACCOUNT_NUMBER}"`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Faça o bootstrap do ambiente.	Para fazer o bootstrap de um ambiente AWS CDK, execute os seguintes comandos:
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Depois de inicializar o ambiente com sucesso, a saída a seguir deve ser exibida.
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
	Para obter mais informações sobre o bootstrapping do AWS CDK, consulte a documentação do AWS CDK.
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Sintetize um modelo.	Para sintetizar um aplicativo do AWS CDK, use o comando `cdk synth`.
	`npm run cdk synth`
	Você verá a saída a seguir.
	`Successfully synthesized to <path-to-directory>/aws-codepipeline-cicd/cdk.out`
	`Supply a stack id (CodePipeline, Dev-MainStack) to display its template.`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Implante a CodePipeline pilha.	Agora que você inicializou e sintetizou o CloudFormation modelo, você pode implantá-lo. A implantação criará o CodePipeline pipeline e um CodeCommit repositório, que serão a fonte e o gatilho do pipeline.
	`npm run cdk -- deploy CodePipeline --require-approval never`
	Depois de executar o comando, você deverá ver uma implantação bem-sucedida das informações de CodePipeline pilha e saída. `CodePipeline.RepositoryName` Fornece o nome do CodeCommit repositório na conta da AWS.
	`CodePipeline: deploying...`
	`CodePipeline: creating CloudFormation changeset...`
	`# CodePipeline Outputs:`
	`CodePipeline.RepositoryName = SampleRepository`
	`Stack ARN: arn:aws:cloudformation:REGION:ACCOUNT-ID`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`:stack/CodePipeline/STACK-ID`	

Tarefa	Descrição	Habilidades necessárias

Configure o CodeCommit repositório e a ramificação remotos.	Depois de uma implantação bem-sucedida, CodePipeline iniciará a primeira execução do pipeline, que você pode encontrar no CodePipeline console da AWS. Como o AWS CDK e CodeCommit não iniciam uma ramificação padrão, essa execução inicial do pipeline falhará e retornará a seguinte mensagem de erro.
	`The action failed because no branch named main was found in the selected AWS CodeCommit repository SampleRepository. Make sure you are using the correct branch name, and then try again. Error: null`
	Para corrigir esse erro, configure uma origem remota como `SampleRepository` e crie a ramificação `main` necessária.
	`RepoName=$(aws cloudformation describe-stacks --stack-name CodePipeline --query "Stacks[0].Outputs[?OutputKey=='RepositoryName'].OutputValue" --output text)`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`echo "${RepoName}"`
	`#`
	`git init`
	`git branch -m master main`
	`git remote add origin codecommit://${RepoName}`
	`git add .`
	`git commit -m "Initial commit"`
	`git push -u origin main`	

Teste o pipeline implantado CodePipeline

Tarefa	Descrição	Habilidades necessárias
Confirme uma alteração para ativar o pipeline.	Depois de uma implantação inicial bem-sucedida, você deve ter um pipeline de CI/CD completo com uma ramificação `main` para `SampleRepository` como ramificação de origem. Assim que você confirmar as alterações na ramificação `main`, o pipeline iniciará e executará a seguinte sequência de ações: 1. Obtenha seu código do CodeCommit repositório. 2. Compile seu código. 3. Atualize o próprio pipeline (`UpdatePipeline`).	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	4. Execute três trabalhos paralelos para verificaç ões de linting, segurança e testes unitários. 5. Em caso de sucesso, o pipeline implantará a pilha `Main` para `./lib/main-stack.ts` no ambiente de Desenvolvimento. 6. Execute uma verificaç ão pós-implantação dos recursos implantados. Você pode seguir todas CodePipeline as etapas e resultados no CodePipeline console. 7. Em caso de sucesso, o pipeline repetirá a implantaç ão e a validação para os ambientes de teste e produção.	

Teste localmente usando um Makefile

Tarefa	Descrição	Habilidades necessárias
Execute o processo de desenvolvimento usando um Makefile.	Você pode executar todo o pipeline localmente usando o comando`make` ou pode executar uma etapa individual (por exemplo, `make linting`).	Desenvolvedor de aplicativos, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para testar o uso de `make`, execute as seguintes ações: • Implemente o pipeline local: `make` • Execute somente o teste de unidade: `make unittest` • Implante na conta atual: `make deploy` • Limpe o meio ambiente: `make clean`	

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Exclua os recursos do aplicativo AWS CDK.	Para limpar seu aplicativo AWS CDK, execute o comando a seguir. `cdk destroy --all` Esteja ciente de que os buckets do Amazon Simple Storage Service (Amazon S3) criados durante a inicialização não são excluídos automaticamente. Eles precisam de uma política de retenção que permita a exclusão, ou você precisa excluí-los manualmente na sua conta da AWS.	DevOps engenheiro

Solução de problemas

Problema	Solução
O modelo não está funcionando conforme o esperado.	Se algo der errado e o modelo não estiver funcionando, verifique se você tem o seguinte: • As versões adequadas das ferramentas. • Acesso à conta de destino da AWS (conectividade de rede). • Permissões suficientes para a conta de destino da AWS.

Recursos relacionados

- Introdução às tarefas comuns do Centro de Identidade do IAM
- CodePipeline Documentação da AWS
- AWS CDK

Configure o registro centralizado em escala corporativa usando o Terraform

Criado por Aarti Rajput (AWS), Yashwant Patel (AWS) e Nishtha Yadav (AWS)

Resumo

O registro centralizado é vital para a infraestrutura de nuvem de uma organização, pois fornece visibilidade de suas operações, segurança e conformidade. À medida que sua organização expande seu AWS ambiente em várias contas, uma estratégia estruturada de gerenciamento de registros se torna fundamental para executar operações de segurança, atender aos requisitos de auditoria e alcançar a excelência operacional.

Esse padrão fornece uma estrutura escalável e segura para centralizar registros de vários serviços Contas da AWS e, a fim de permitir o gerenciamento de registros em escala empresarial em implantações complexas. AWS A solução é automatizada usando o Terraform, que é uma ferramenta de infraestrutura como código (IaC) HashiCorp que garante implantações consistentes e reproduzíveis e minimiza a configuração manual. Ao combinar o Amazon CloudWatch Logs, o Amazon Data Firehose e o Amazon Simple Storage Service (Amazon S3), você pode implementar um pipeline robusto de agregação e análise de logs que fornece:

- Gerenciamento centralizado de registros em toda a sua organização em AWS Organizations
- Coleta automatizada de registros com controles de segurança integrados
- Processamento de registros escalável e armazenamento durável
- Relatórios de conformidade e trilhas de auditoria simplificados
- Monitoramento e insights operacionais em tempo real

A solução coleta registros de contêineres e funções do Amazon Elastic Kubernetes Service (Amazon EKS AWS Lambda), funções e instâncias de banco de dados do Amazon Relational Database Service (Amazon RDS) por meio de registros. CloudWatch Ele encaminha automaticamente esses registros para uma conta de registro dedicada usando filtros de CloudWatch assinatura. O Firehose gerencia o pipeline de streaming de log de alto rendimento para o Amazon S3 para armazenamento de longo prazo. O Amazon Simple Queue Service (Amazon SQS) está configurado para receber notificações de eventos do Amazon S3 após a criação do objeto. Isso permite a integração com serviços de análise, incluindo:

- Amazon OpenSearch Service para pesquisa de registros, visualização e análise em tempo real
- Amazon Athena para consultas baseadas em SQL

- Amazon EMR para processamento em grande escala
- Lambda para transformação personalizada
- Amazon QuickSight para painéis

Todos os dados são criptografados usando AWS Key Management Service (AWS KMS), e toda a infraestrutura é implantada usando o Terraform para uma configuração consistente em todos os ambientes.

Essa abordagem de registro centralizado permite que as organizações melhorem sua postura de segurança, mantenham os requisitos de conformidade e otimizem a eficiência operacional em toda a AWS infraestrutura.

Pré-requisitos e limitações

Pré-requisitos

- Um landing zone para sua organização que é construído usando AWS Control Tower
- Account Factory for Terraform (AFT), implantado e configurado com as contas necessárias
- Terraform para provisionar a infraestrutura
- AWS Identity and Access Management Funções e políticas (IAM) para acesso entre contas

Para obter instruções sobre como configurar AWS Control Tower contas AFT e Application, consulte a seção Epics.

Contas obrigatórias

Sua organização AWS Organizations deve incluir as seguintes contas:

- Conta de aplicativo — Uma ou mais contas de origem nas quais Serviços da AWS (Amazon EKS, Lambda e Amazon RDS) são executadas e geram registros
- Conta de arquivamento de registros — uma conta dedicada para armazenamento e gerenciamento centralizados de registros

Versões do produto

- AWS Control Tower versão 3.1 ou posterior
- Terraform versão 0.15.0 ou posterior

Arquitetura

O diagrama a seguir ilustra uma arquitetura de registro AWS centralizada que fornece uma solução escalável para coletar, processar e armazenar registros de várias contas de aplicativos em uma conta dedicada do Log Archive. Essa arquitetura gerencia com eficiência os registros de Serviços da AWS, incluindo Amazon RDS, Amazon EKS e Lambda, e os encaminha por meio de um processo simplificado para os buckets regionais do S3 na conta do Log Archive.

O fluxo de trabalho inclui cinco processos:

1. Processo de fluxo de log
   - O processo de fluxo de registros começa nas contas do aplicativo, onde são Serviços da AWS gerados vários tipos de registros, como registros gerais, de erros, de auditoria, de consultas lentas do Amazon RDS, registros do plano de controle do Amazon EKS e registros de execução de funções e erros do Lambda.
   - CloudWatch serve como ponto de coleta inicial. Ele reúne esses registros no nível do grupo de registros em cada conta do aplicativo.
   - Em CloudWatch, os filtros de assinatura determinam quais registros devem ser encaminhados para a conta central. Esses filtros oferecem controle granular sobre o encaminhamento de registros, para que você possa especificar padrões de log exatos ou fluxos de log completos para centralização.
2. Transferência de registros entre contas
   - Os registros são movidos para a conta do Log Archive. CloudWatch os filtros de assinatura facilitam a transferência entre contas e preservam o contexto regional.
   - A arquitetura estabelece vários fluxos paralelos para lidar com diferentes fontes de log de forma eficiente, a fim de garantir desempenho e escalabilidade ideais.
3. Processamento de registros na conta do Log Archive
   - Na conta do Log Archive, o Firehose processa os fluxos de log recebidos.
   - Cada região mantém fluxos de entrega dedicados do Firehose que podem transformar, converter ou enriquecer os registros conforme necessário.
   - Esses streams do Firehose entregam os registros processados aos buckets do S3 na conta Log Archive, que está localizada na mesma região das contas do aplicativo de origem (Região A no diagrama) para manter os requisitos de soberania dos dados.
4. Notificações e fluxos de trabalho adicionais

- Quando os registros chegam aos buckets S3 de destino, a arquitetura implementa um sistema de notificação usando o Amazon SQS.
- As filas SQS regionais permitem o processamento assíncrono e podem acionar fluxos de trabalho adicionais, análises ou sistemas de alerta com base nos registros armazenados.

5. AWS KMS para segurança

   A arquitetura é incorporada AWS KMS para fins de segurança. AWS KMS fornece chaves de criptografia para os buckets do S3. Isso garante que todos os registros armazenados mantenham a criptografia em repouso, mantendo a criptografia regional para atender aos requisitos de residência de dados.

Ferramentas

Serviços da AWS

- CloudWatchA Amazon é um serviço de monitoramento e observabilidade que coleta dados operacionais e de monitoramento na forma de registros, métricas e eventos. Ele fornece uma visão unificada dos AWS recursos, aplicativos e serviços que são executados na AWS e em servidores locais.
- CloudWatch Os filtros de assinatura de registros são expressões que correspondem a um padrão nos eventos de registro recebidos e entregam eventos de registro correspondentes ao AWS recurso especificado para processamento ou análise adicionais.
- AWS Control Tower O Account Factory For Terraform (AFT) configura um pipeline do Terraform para ajudá-lo a provisionar e personalizar contas em. AWS Control Tower O AFT fornece provisionamento de contas baseado em Terraform, permitindo que você administre suas contas com. AWS Control Tower
- O Amazon Data Firehose fornece dados de streaming em tempo real para destinos como Amazon S3, Amazon Redshift e Amazon Service. OpenSearch Ele é escalonado automaticamente para corresponder à taxa de transferência de seus dados e não requer administração contínua.
- O Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço gerenciado de orquestração de contêineres que facilita a implantação, o gerenciamento e a escalabilidade de aplicativos em contêineres usando o Kubernetes. Ele gerencia automaticamente a disponibilidade e a escalabilidade dos nós do plano de controle do Kubernetes.
- AWS Key Management Service (AWS KMS) cria e controla chaves de criptografia para criptografar seus dados. AWS KMS se integra a outros Serviços da AWS para ajudá-lo a proteger os dados que você armazena com esses serviços.

- AWS Lambdaé um serviço de computação sem servidor que permite executar código sem provisionar ou gerenciar servidores. Ele escala automaticamente seus aplicativos executando o código em resposta a cada acionador e cobra somente pelo tempo de computação que você usa.
- O Amazon Relational Database Service (Amazon RDS) é um serviço gerenciado de banco de dados relacional que facilita a configuração, a operação e a escalabilidade de um banco de dados relacional na nuvem. Ele fornece capacidade econômica e redimensionável, ao mesmo tempo em que automatiza tarefas administrativas demoradas.
- O Amazon Simple Queue Service (Amazon SQS) é um serviço de enfileiramento de mensagens que permite separar e escalar microsserviços, sistemas distribuídos e aplicativos sem servidor. Ele elimina a complexidade de gerenciar e operar o middleware orientado a mensagens.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado em nuvem que oferece escalabilidade, disponibilidade de dados, segurança e desempenho. Ele pode armazenar e recuperar qualquer quantidade de dados de qualquer lugar na web.

Outras ferramentas

- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Código

O código desse padrão está disponível no repositório de registro GitHub centralizado.

Práticas recomendadas

- Use vários Contas da AWS em uma única organização em AWS Organizations. Essa prática permite o gerenciamento centralizado e o registro padronizado em todas as contas.
- Configure buckets S3 com controle de versão, políticas de ciclo de vida e replicação entre regiões. Implemente criptografia e registro de acesso para segurança e conformidade.
- Implemente padrões de registro comuns usando o formato JSON com campos e carimbos de data/hora padrão. Use uma estrutura de prefixo e correlação consistentes IDs para facilitar o rastreamento e a análise.
- Habilite controles de segurança com AWS KMS criptografia e acesso com privilégios mínimos. Mantenha o AWS CloudTrail monitoramento e a rotação regular de chaves para aumentar a segurança.

- Configure CloudWatch métricas e alertas para rastreamento de entrega. Monitore custos e desempenho com notificações automatizadas.
- Configure as políticas de retenção do Amazon S3 para atender aos requisitos de conformidade e habilite o registro de acesso ao servidor do Amazon S3 para rastrear todas as solicitações feitas aos seus buckets do S3. Mantenha a documentação das políticas e regras de ciclo de vida do bucket do S3. Realize análises periódicas dos registros de acesso, permissões do bucket e configurações de armazenamento para ajudar a garantir as melhores práticas de conformidade e segurança.

Épicos

Contas de configuração AWS Control Tower, AFT e de aplicativos

Tarefa	Descrição	Habilidades necessárias
Configure um AWS Control Tower ambiente com o AFT.	1. Implante AWS Control Tower seguindo as instruções na AWS Control Tower documentação. 2. Implante o AFT seguindo as instruções na AWS Control Tower documentação.	Administrador da AWS
Ative o compartilhamento de recursos para a organização.	1. Configure AWS Command Line Interface (AWS CLI) com credenciais da conta de gerenciamento, que fornecem permissõe s administrativas para gerenciar AWS Control Tower. 2. Execute o seguinte AWS CLI comando em qualquer Região da AWS:	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`aws ram enable-sharing-with-aws-organization` Isso permite o compartilhamento de recursos em sua organização em AWS Organizations todas as regiões que oferecem suporte AWS Resource Access Manager (AWS RAM).	
Verifique ou provisione contas do aplicativo.	Para provisionar novas contas de aplicativos para seu caso de uso, crie-as por meio do AFT. Para obter mais informações, consulte Provisionar uma nova conta com o AFT na AWS Control Tower documentação.	Administrador da AWS

Configurar arquivos de configuração para contas de aplicativos

Tarefa	Descrição	Habilidades necessárias
Copie o conteúdo da `Application_account` pasta para o `aft-account-customizations` repositório.	1. Crie uma pasta nomeada `Application_account` no caminho raiz do `aft-account-customizations` repositório. Esse repositório é criado automaticamente quando	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	você configura o AFT (veja o épico anterior). 2. Navegue até o diretório raiz do scale-using-terraform repositório centralised-logging-at-enterprise-, copie o conteúdo do `aft/account` diretório e cole-o no `Application_account` diretório que você criou na etapa 1 do `aft-account-customizations` repositório. 3. Do diretório raiz do `centralised-logging-at-enterprise-scale-using-terraform` repositório, copie o conteúdo do `Application_account` diretório para o `Application_account/terraform` diretório no `aft-account-customizations` repositório. 4. No `aft-account-customizations/Application_account/terraform.tfvars` arquivo, confirme se todos os parâmetros foram passados como argumentos nos arquivos de configura	

Tarefa	Descrição	Habilidades necessárias
	ção correspondentes do Terraform.	

Tarefa	Descrição	Habilidades necessárias
Revise e edite os parâmetros de entrada para configurar a conta do aplicativo.	Nesta etapa, você configura o arquivo de configuração para criar recursos em contas de aplicativos, incluindo grupos de CloudWatch log, filtros de CloudWatch assinatura, funções e políticas do IAM e detalhes de configuração das funções Amazon RDS, Amazon EKS e Lambda. No seu `aft-account-customizations` repositório, na `Application_account` pasta, configure os parâmetros de entrada no `terraform.tfvars` arquivo com base nos requisitos da sua organização: • `environment` : o nome do ambiente (por exemplo,, `proddev`,`staging`) em que os recursos serão implantados. • `account_name` : o nome do Conta da AWS local onde os recursos serão criados. • `log_archive_account_id` : o Conta da AWS ID em que os registros serão arquivados.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• `admin_role_name` : o nome da função administrativa que será usada para gerenciar recursos. • `tags`: um mapa de pares de valores-chave que representam tags comuns a serem aplicadas a todos os recursos. • `rds_config` : um objeto que contém detalhes de configuração para instâncias do Amazon RDS. • `allowed_cidr_blocks` : uma lista de blocos CIDR que têm permissão para acessar os recursos. • `destination_name:` Uma variável usada para criar o Amazon Resource Name (ARN) do CloudWatch destino em que os registros serão transmitidos. • `rds_parameters:` Um objeto que contém as configurações do grupo de parâmetros do Amazon RDS. • `vpc_config` : um objeto que contém detalhes da configuração da VPC.	

Tarefa	Descrição	Habilidades necessárias
	• `eks_config` : um objeto que contém detalhes de configuração para clusters do Amazon EKS. • `lambda_config` : um objeto que contém detalhes de configuração para funções Lambda. • `restrictive_cidr_range` : uma lista de intervalos de CIDR restritivos para regras de grupos de segurança. • `target_account_id` : o Conta da AWS ID da conta do Log Archive de destino na qual os recursos serão implantados.	

Configurar arquivos de configuração para a conta do Log Archive

Tarefa	Descrição	Habilidades necessárias
Copie o conteúdo da `Log_archive_account` pasta para o `aft-account-customizations` repositório.	1. Crie uma pasta nomeada `Log_archive_account` no caminho raiz do `aft-account-customizations` repositório. Esse repositório é criado automaticamente quando você configura o AFT. 2. Navegue até o diretório raiz do `centralised-`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`logging-at-enterprise-scale-using-terraform` repositório, copie o conteúdo do `aft/account` diretório e cole-o no `Log_archive_account` diretório que você criou na etapa anterior do `aft-account-customizations` repositório. 3. Do diretório raiz do `centralised-logging-at-enterprise-scale-using-terraform` repositório, copie o conteúdo do `Log_archive_account` diretório para o `Log_archive_account/terraform` diretório no `aft-account-customizations` repositório. 4. No `aft-account-customizations/Log_archive_account/terraform.tfvars` arquivo, confirme se todos os parâmetros foram passados como argumentos nos arquivos de configuração correspondentes do Terraform.	

Tarefa	Descrição	Habilidades necessárias
Revise e edite os parâmetros de entrada para configurar a conta do Log Archive.	Nesta etapa, você configura o arquivo de configuração para criar recursos na conta do Log Archive, incluindo fluxos de entrega do Firehose, buckets S3, filas SQS e funções e políticas do IAM. Na `Log_archive_account` pasta do seu `aft-account-customizations` repositório, configure os parâmetros de entrada no `terraform.tfvars` arquivo com base nos requisitos da sua organização: • `environment` : o nome do ambiente (por exemplo,, `proddev`,`staging`) em que os recursos serão implantados. • `destination_name` : uma variável usada para criar o ARN do CloudWatch destino em que os registros serão transmitidos. • `source_account_ids` : uma lista dos Conta da AWS IDs que podem colocar filtros de assinatura no destino do registro. Você pode inserir IDs quantas	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	contas quiser habilitar para o registro centralizado.	

Execute comandos do Terraform para provisionar recursos

Tarefa	Descrição	Habilidades necessárias

Opção 1 - Implantar os arquivos de configuração do Terraform a partir do AFT.	No AFT, o pipeline do AFT é acionado depois que você envia o código com as alterações de configuração para o GitHub `aft-account-customizations` repositório. O AFT detecta automaticamente as alterações e inicia o processo de personalização da conta.
	
	Depois de fazer alterações nos arquivos do Terraform (`terraform.tfvars`), confirme e envie suas alterações para o seu `aft-account-customizations` repositório:
	
	`$ git add *`
	`$ git commit -m "update message"`
	`$ git push origin main`
	
	Note
	Se você estiver usando uma
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ramificação diferente (como `dev`), `main` substitua pelo nome da ramificação.	

Tarefa	Descrição	Habilidades necessárias

Opção 2 - Implantar o arquivo de configuração do Terraform manualmente.	Se você não estiver usando o AFT ou quiser implantar a solução manualmente, poderá usar os seguintes comandos do Terraform `Log_archive_account` nas pastas `Application_account` e:
	1. Clone o GitHub repositório e configure os parâmetros de entrada no `terraform.tfvars` arquivo.
	2. Execute o seguinte comando:
	`$ terraform init`
	3. Pré-visualize as alterações:
	`$ terraform plan`
	Esse comando avalia a configuração do Terraform para determinar o estado desejado dos recursos e o compara com o estado atual da sua infraestrutura.
	4. Aplique as alterações:
	`$ terraform apply`
	5. Revise as alterações planejadas e digite yes no
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	prompt para continuar com a inscrição.	

Validar recursos

Tarefa	Descrição	Habilidades necessárias
Verifique os filtros de assinatura.	Para verificar se os filtros de assinatura encaminham os registros corretamente dos grupos de registros da conta do aplicativo para a conta do Log Archive: 1. Na conta do aplicativo, abra o CloudWatch console. 2. No painel de navegação esquerdo, escolha Log groups (Grupos de log). 3. Selecione cada grupo de registros (`/aws/rds`,`/aws/eks`,`/aws/lambda`) e escolha a guia Filtros de assinatura. Você deve ver filtros de assinatura ativos que apontam para o ARN de destino, com base no nome que você especificou no arquivo de configuração do Terraform.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	4. Escolha qualquer filtro de assinatura para verificar sua configuração e status.	
Verifique os streams do Firehose.	Para verificar se os streams do Firehose na conta do Log Archive processam os registros do aplicativo com êxito: 1. Na conta do Log Archive, abra o console do Firehose. 2. No painel de navegação esquerdo, escolha Firehose streams. 3. Escolha qualquer stream do Firehose e verifique o seguinte: • O destino mostra o bucket S3 correto. • A guia Monitoramento mostra métricas de entrega bem-sucedidas. • A data e hora da entrega recente é atual.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Valide os buckets S3 centralizados.	Para verificar se os buckets S3 centralizados recebem e organizam os registros adequadamente: 1. Na conta do Log Archive, abra o console do Amazon S3. 2. Selecione cada bucket de registro central. 3. Navegue pela estrutura de pastas: AWSLogs/AccountID/Region/Service. Você deve ver os arquivos de log organizados por timestamp () YYYY/MM/DD/HH. 4. Escolha qualquer arquivo de log recente e verifique seu formato e integridade dos dados.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Valide as filas do SQS.	Para verificar se as filas do SQS recebem notificações para novos arquivos de log: 1. Na conta do Log Archive, abra o console do Amazon SQS. 2. No painel de navegação à esquerda, escolha Queues (Filas). 3. Selecione cada fila configurada e escolha Enviar e receber mensagens. Você deve ver mensagens que contêm notificações de eventos do S3 para novos arquivos de log. 4. Escolha qualquer mensagem para verificar se ela contém as informações corretas do objeto S3.	DevOps engenheiro

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Opção 1 - Desative o arquivo de configuração do Terraform do AFT.	Quando você remove os arquivos de configuração do Terraform e envia as alterações, o AFT inicia automaticamente o processo de remoção de recursos.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	1. Navegue até o `aft-account-customizations` repositório.
	2. Acesse o diretório `terraform .`
	3. Exclua os seguintes arquivos:
	• Diretório `modules`
	• `iam.tf`
	• `versions.tf`
	• `variables.tf`
	• `outputs.tf`
	• `terraform.tfvars`
	4. Limpe o conteúdo do `main.tf` arquivo.
	5. Envie suas alterações para o repositório:
	`# Stage all changes`
	`$ git add *`
	`# Commit cleanup changes`
	`$ git commit -m "Remove AFT customizations"`
	`# Push to repository`
	`$ git push origin main`
	Note
	Se você estiver usando uma	

Tarefa	Descrição	Habilidades necessárias
	ramificaç ão diferente (comodev), `main` substitua pelo nome da ramificação.	

Tarefa	Descrição	Habilidades necessárias

Opção 2 — Limpe os recursos do Terraform manualmente.	Se você não estiver usando o AFT ou quiser limpar os recursos manualmente, use os seguintes comandos do Terraform `Log_archive_account` nas pastas `Application_account` e:
	1. Inicialize a configuração do Terraform:
	`$ terraform init`
	Esse comando inicializa o Terraform e garante o acesso ao estado atual.
	2. Pré-visualize as alterações de limpeza:
	`$ terraform destroy`
	Esse comando avalia quais recursos serão destruídos e compara o estado desejado com o estado atual da sua infraestrutura.
	3. Execute a limpeza. Quando solicitado, digite yes para confirmar e executar o plano de destruição.
		DevOps engenheiro

Solução de problemas

Problema	Solução
O destino dos CloudWatch registros não foi criado ou está inativo.	Valide o seguinte: 1. Na conta do Log Archive, verifique se a política de destino inclui: • O principal correto da conta de origem. • A ação correta (`logs:PutSubscriptionFilter`). • Um ARN de destino válido. 2. Confirme se o stream do Firehose existe e está ativo. 3. Verifique se a função do IAM anexada ao destino tem permissões para o Firehose.
O filtro de assinatura falhou ou está preso no status pendente.	Verifique o seguinte: 1. Na conta do aplicativo, verifique se a função do IAM tem: • Permissões para ligar`PutSubscriptionFilter` . • Uma relação de confiança com a CloudWatch Logs. 2. Confirme se o ARN de destino está correto. 3. Verifique CloudWatch os registros para ver se há mensagens de erro específicas.
O stream de entrega do Firehose não mostra registros recebidos.	Verifique o seguinte: 1. Confirme se a função Firehose IAM tem: • Permissões para gravar no Amazon S3. • Acesso à AWS KMS chave se a criptografia estiver ativada. 2. Analise CloudWatch as métricas para:

Problema	Solução
	• `IncomingRecords` • `DeliveryToS3.Records` 3. Verifique as configurações de buffer e de entrega.

Recursos relacionados

- Configuração da infraestrutura do Terraform (documentação do Terraform)
- Implante o AWS Control Tower Account Factory for Terraform (AFT) (AWS Control Tower documentação)
- Tutorial do IAM: delegue o acesso Contas da AWS usando funções do IAM () IAMdocumentation

Configure a end-to-end criptografia para aplicativos no Amazon EKS usando cert-manager e Let's Encrypt

Criado por Mahendra Revanasiddappa (AWS) e Vasanth Jeyaraj (AWS)

Resumo

A implementação da end-to-end criptografia pode ser complexa e você precisa gerenciar certificados para cada ativo em sua arquitetura de microsserviços. Embora você possa encerrar a conexão Transport Layer Security (TLS) na borda da rede Amazon Web Services (AWS) com um Network Load Balancer ou Amazon API Gateway, algumas organizações exigem criptografia. end-to-end

Esse padrão usa o controlador do Ingress NGINX para entrada. Isso ocorre porque quando você cria uma entrada do Kubernetes, o recurso de entrada usa um Network Load Balancer. O Network Load Balancer não permite fazer o upload de certificados de cliente. Portanto, você não pode obter o TLS mútuo com a entrada do Kubernetes.

Esse padrão é destinado a organizações que exigem autenticação mútua entre todos os microsserviços em seus aplicativos. O TLS mútuo reduz a carga de manter nomes de usuário ou senhas e também pode usar a estrutura de segurança turnkey. A abordagem desse padrão é compatível se sua organização tiver um grande número de dispositivos conectados ou precisar cumprir rígidas diretrizes de segurança.

Esse padrão ajuda a aumentar a postura de segurança da sua organização implementando end-to-end criptografia para aplicativos executados no Amazon Elastic Kubernetes Service (Amazon EKS). Esse padrão fornece um exemplo de aplicativo e código na GitHub End-to-end criptografia no repositório Amazon EKS para mostrar como um microsserviço é executado com end-to-end criptografia no Amazon EKS. A abordagem do padrão usa o gerenciador de certificados, um complemento do Kubernetes, com o Let's Encrypt como autoridade de certificação (CA). O Let's Encrypt é uma solução econômica para gerenciar certificados e fornece certificados gratuitos válidos por 90 dias. O Gerenciador de certificados automatiza o provisionamento sob demanda e a alternância de certificados quando um novo microsserviço é implantado no Amazon EKS.

Público-alvo

Esse padrão é recomendado para usuários com experiência com Kubernetes, TLS, Amazon Route 53 e Sistema de Nomes de Domínio (DNS).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um cluster do Amazon EKS existente.
- AWS Command Line Interface (AWS CLI) versão 1.7 ou superior, instalada e configurada no macOS, Linux ou Windows
- O utilitário de linha de comando `kubectl`, instalado e configurado para acessar o cluster Amazon EKS. Para obter mais informações, consulte Instalação do kubectl na documentação do Amazon EKS.
- O nome de um DNS existente para testar o aplicativo. Para obter mais informações, consulte Registrar nomes de domínio usando o Amazon Route 53 na documentação do Amazon Route 53.
- A versão mais recente do Helm instalada em sua máquina local. Para obter mais informações sobre isso, consulte Usando o Helm com o Amazon EKS na documentação do Amazon EKS e no repositório do GitHub Helm.
- A GitHub End-to-end criptografia no repositório Amazon EKS, clonada em sua máquina local.
- Substitua os seguintes valores nos `trustpolicy.json` arquivos `policy.json` e da GitHub End-to-end criptografia clonada no repositório Amazon EKS:
  - `<account number>`: substitua pelo ID da conta da AWS para a conta na qual você deseja implantar a solução.
  - `<zone id>`: substitua pelo ID de zona do Route 53 do nome de domínio.
  - `<node_group_role>`: substitua pelo nome do AWS Identity and Access Management perfil do (IAM) associado aos nós do Amazon EKS.
  - `<namespace>`: substitua pelo namespace Kubernetes no qual você implanta o controlador do Ingress NGINX e o aplicativo de amostra.
  - `<application-domain-name>`: substitua pelo nome de domínio DNS do Route 53.

Limitações

- Esse padrão não descreve como alternar certificados e apenas demonstra como usar certificados com microsserviços no Amazon EKS.

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho e os componentes da arquitetura desse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um cliente envia uma solicitação para acessar o aplicativo para o nome DNS.
2. O registro do Route 53 é um CNAME para o Network Load Balancer.
3. O Network Load Balancer encaminha a solicitação para o controlador do Ingress NGINX que está configurado com um receptor TLS. A comunicação entre o controlador do Ingress NGINX e o Network Load Balancer segue o protocolo HTTPS.
4. O controlador do Ingress NGINX executa o roteamento baseado em caminhos conforme a solicitação do cliente ao serviço do aplicativo.
5. O serviço do aplicativo encaminha a solicitação para o pod do aplicativo. O aplicativo é projetado para usar o mesmo certificado chamando segredos.
6. Os pods executam o aplicativo de amostra usando os certificados do gerenciador de certificados. A comunicação entre o controlador do Ingress NGINX e os pods usa HTTPS.

> **Note**
>
> O Cert-manager é executado em seu próprio namespace. Ele usa uma função de cluster do Kubernetes para provisionar certificados como segredos em namespaces específicos. Você pode anexar esses namespaces aos pods de aplicativos e ao controlador do Ingress NGINX.

Ferramentas

Serviços da AWS

- O Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço gerenciado que você pode usar para executar o Kubernetes na AWS , eliminando a necessidade de instalar, operar e manter seus próprios nós ou ambiente de gerenciamento ou nós do Kubernetes.
- O Balanceador de carga Elastic distribui automaticamente seu tráfego de entrada entre vários destinos, contêineres e endereços IP.

- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.

Outras ferramentas

- O gerenciador de certificado é um complemento do Kubernetes que solicita certificados, os distribui para contêineres do Kubernetes e automatiza a renovação de certificados.
- O controlador do Ingress NGINX é uma solução de gerenciamento de tráfego para aplicativos nativos de nuvem em Kubernetes e ambientes em contêineres.

Épicos

Crie e configure uma zona hospedada pública com o Route 53

Tarefa	Descrição	Habilidades necessárias
Crie uma zona hospedada no Route 53.	Faça login no Console de Gerenciamento da AWS, abra o console do Amazon Route 53, escolha zona hospedada e, em seguida, escolha Criar zona hospedada. Crie uma zona hospedada pública e registre o ID da zona. Para obter mais informações, consulte Criar uma zona hospedada pública na documentação do Amazon Route 53. **Note** O ACME DNS01 usa o provedor de DNS para publicar um desafio para o cert-manager	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	emitir o certificado. Esse desafio pede que você comprove que controla o DNS do seu nome de domínio colocando um valor específico em um registro TXT sob esse nome de domínio. Depois que o Let's Encrypt fornece um token ao seu cliente ACME, seu cliente cria um registro TXT derivado desse token e da chave da sua conta, e coloca esse registro em `_acme-challenge.<YOURDOMAIN>` . Depois, o Let's Encrypt consulta o DNS desse registro. Se encontrar uma correspondência, você pode continuar a emitir um certificado.	

Configure um perfil do IAM para permitir que o gerenciador de certificado acesse a zona hospedada pública

Tarefa	Descrição	Habilidades necessárias
Crie a política do IAM para o gerenciador de certificado.	É necessária uma política do IAM para fornecer ao gerenciador de certificado permissão para validar que você é proprietário do domínio Route 53. O `policy.json` exemplo de política do IAM é fornecido no `1-IAMRole` diretório na GitHub End-to-end criptografia clonada no repositório Amazon EKS. Use o seguinte comando da AWS CLI para criar a política do IAM. `aws iam create-policy \ --policy-name PolicyForCertManager \ --policy-document file://policy.json`	AWS DevOps
Crie o perfil do IAM para gerenciador de certificado.	Após criar a política do IAM, é necessário criar um perfil do IAM. O exemplo `trustpolicy.json` de perfil do IAM é fornecido no diretório `1-IAMRole` . Use o seguinte comando da AWS CLI para criar o perfil do IAM.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`aws iam create-role \ --role-name RoleForCertManager \ --assume-role-policy-document file://trustpolicy.json`	
Anexe a política ao perfil.	Execute o comando a seguir para anexar a política do IAM ao perfil do IAM. Substitua `AWS_ACCOUNT_ID` pelo seu ID da sua conta da AWS. `aws iam attach-role-policy \ --policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/PolicyForCertManager \ --role-name RoleForCertManager`	AWS DevOps

Configure o controlador de entrada NGINX no Amazon EKS

Tarefa	Descrição	Habilidades necessárias
Implante o controlador de entrada NGINX.	Instale a versão mais recente do `nginx-ingress` usando o Helm. Você pode modificar a configuração `nginx-ingress` de acordo com seus requisitos antes de implantá-la. Esse padrão usa um Network Load Balancer anotado voltado para o	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	interior e que está disponíve l no diretório `5-Nginx-I ngress-Controller` . Instale o controlador de entrada NGINX executando o seguinte comando Helm a partir do diretório `5-Nginx-I ngress-Controller` . `helm install test- nginx nginx-stable/ nginx-ingress -f 5-Nginx-Ingress-Co ntroller/values_in ternal_nlb.yaml`	
Verifique se o controlador do Ingress NGINX está instalado.	Digite o comando `helm list`. A saída deve mostrar que o controlador do Ingress NGINX está instalado.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Crie um registro A da Route 53.	O registro A aponta para o Network Load Balancer criado pelo controlador do Ingress NGINX. 1. Obtenha o nome DNS do Network Load Balancer. Para obter instruções, consulte Obter o nome do DNS para um balanceador de carga do ELB. 2. No console do Amazon Route 53, escolha zonas hospedadas. 3. Selecione a zona hospedada pública na qual você deseja criar o registro e escolha Criar registro. 4. Insira um nome para o registro. 5. Em Tipo de registro, escolha A - Encaminha o tráfego para IPv4 e alguns recursos da AWS. 6. Ative o Alias. 7. Em Rotear tráfego para, faça o seguinte: a. Escolha um Alias para Network Load Balancer. b. Escolha a região da AWS na qual o Network Load Balancer está implantado.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	c. Insira o nome DNS do Network Load Balancer. 8. Escolha Criar registros.	

Configure o NGINX no VirtualServer Amazon EKS

Tarefa	Descrição	Habilidades necessárias
Implante o NGINX VirtualServer.	O VirtualServer recurso NGINX é uma configuração de balanceamento de carga que é uma alternativa ao recurso de entrada. A configuração para criar o VirtualServer recurso NGINX está disponível no `nginx_virtualserver.yaml` arquivo no `6-Nginx-Virtual-Server` diretório. Digite o comando a seguir `kubectl` para criar o recurso NGINX VirtualServer . `kubectl apply -f nginx_virtualserver.yaml` **Important** Certifique-se de atualizar o nome de domínio do aplicativo, o segredo do certificado e o nome do serviço do aplicativ	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	o no `nginx_vir tualserver.yaml` arquivo.	
Verifique se o NGINX VirtualServer foi criado.	Digite o comando a seguir `kubectl` para verificar se o VirtualServer recurso NGINX foi criado com sucesso. `kubectl get virtualse rver` **Note** Verifique se a `Host` coluna corresponde ao nome de domínio do seu aplicativo.	AWS DevOps
Implante o servidor web NGINX com o TLS ativado.	Esse padrão usa um servidor web NGINX com TLS habilitad o como aplicativo para testar a criptografia. end-to-end Os arquivos de configuração necessários para implantar o aplicativo de teste estão disponíveis no diretório `demo-webserver` . Execute o seguinte comando no `kubectl` para implantar o aplicativo. `kubectl apply -f nginx-tls-ap.yaml`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Verifique se os recursos do aplicativo de teste foram criados.	Insira os seguintes comandos `kubectl` para verificar se os recursos necessários foram criados para o aplicativo de teste: • `kubectl get deployments` **Note** Valide a `Ready` coluna e a `Available` coluna. • `kubectl get pods | grep -i example-deploy` **Note** Os frutos devem estar no `running` estado. • `kubectl get configmap` • `kubectl get svc`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Valide o aplicativo.	1. Digite o comando a seguir substituindo o `<application-domain-name>` pelo nome DNS Route53 que você criou anteriormente. `curl --verbose https://<application-domain-name>` 2. Verifique se você consegue acessar o aplicativo.	AWS DevOps

Recursos relacionados

Recursos da AWS

- Criar registros usando o console do Amazon Route 53 (documentação do Amazon Route 53)
- Como usar um Network Load Balancer com o controlador de entrada NGINX no Amazon EKS (publicação no blog da AWS)

Outros recursos

- Route 53 (documentação do gerenciador de certificado)
- Como configurar o DNS01 Challenge Provider (documentação do gerenciador de certificado)
- Desafio do Let's Encrypt DNS (documentação do Let's Encrypt)

Simplifique a implantação de aplicativos multilocatários do Amazon EKS usando o Flux

Criado por Nadeem Rahaman (AWS), Aditya Ambati (AWS), Aniket Dekate (AWS) e Shrikant Patil (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Muitas empresas que oferecem produtos e serviços são setores regulados por dados que precisam manter barreiras de dados entre suas funções comerciais internas. Esse padrão descreve como você pode usar o recurso de multilocação no Amazon Elastic Kubernetes Service (Amazon EKS) para criar uma plataforma de dados que obtenha isolamento lógico e físico entre locatários ou usuários que compartilham um único cluster do Amazon EKS. O padrão fornece isolamento por meio das seguintes abordagens:

- Isolamento do namespace Kubernetes
- Regras de controle de acesso com base em função (RBAC)
- Políticas de rede
- Cotas de recurso
- AWS Identity and Access Management Funções (IAM) para contas de serviço (IRSA)

Além disso, essa solução usa o Flux para manter a configuração do locatário imutável quando você implanta aplicativos. Você pode implantar seus aplicativos de locatário especificando o repositório de locatários que contém o arquivo Flux `kustomization.yaml` em sua configuração.

Esse padrão implementa o seguinte:

- Um AWS CodeCommit repositório, AWS CodeBuild projetos e um AWS CodePipeline pipeline, que são criados com a implantação manual de scripts do Terraform.
- Componentes de rede e computação necessários para hospedar os inquilinos. Eles são criados por meio CodePipeline e CodeBuild usando o Terraform.
- Namespaces de inquilinos, políticas de rede e cotas de recursos, que são configurados por meio de um gráfico do Helm.

- Aplicativos que pertencem a diferentes locatários, implantados usando o Flux.

Recomendamos que você planeje e crie cuidadosamente sua própria arquitetura para multilocação com base em seus requisitos exclusivos e considerações de segurança. Esse padrão fornece um ponto de partida para sua implementação.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- AWS Command Line Interface (AWS CLI) versão 2.11.4 ou posterior, instalada e configurada
- Terraform versão 0.12 ou posterior instalada em sua máquina local
- Terraform AWS Provider versão 3.0.0 ou posterior
- Kubernetes Provider versão 2.10 ou posterior
- Helm Provider versão 2.8.0 ou posterior
- Kubectl Provider versão 1.14 ou posterior

Limitações

- Dependência das implantações manuais do Terraform: a configuração inicial do fluxo de trabalho, incluindo a criação de CodeCommit repositórios, CodeBuild projetos e CodePipeline pipelines, depende de implantações manuais do Terraform. Isso introduz uma limitação potencial em termos de automação e escalabilidade, porque requer intervenção manual para mudanças na infraestrutura.
- CodeCommit dependência do repositório: o fluxo de trabalho depende dos CodeCommit repositórios como solução de gerenciamento de código-fonte e é fortemente acoplado a. Serviços da AWS

Arquitetura

Arquiteturas de destino

Esse padrão implanta três módulos para criar a infraestrutura de pipeline, rede e computação para uma plataforma de dados, conforme ilustrado nos diagramas a seguir.

Arquitetura do pipeline:

Arquitetura de rede:

Arquitetura de computação:

Ferramentas

Serviços da AWS

- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeCommité um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes.
- AWS Transit Gatewayé um hub central que conecta nuvens privadas virtuais (VPCs) e redes locais.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- As políticas de rede Cilium oferecem suporte às políticas de rede L3 e L4 do Kubernetes. Eles podem ser estendidos com políticas L7 para fornecer segurança em nível de API para HTTP, Kafka e gRPC e outros protocolos similares.
- O Flux é uma ferramenta de entrega contínua (CD) baseada em Git que automatiza as implantações de aplicativos no Kubernetes.

- O Helm é um gerenciador de pacotes de código aberto para Kubernetes que ajuda você a instalar e gerenciar aplicativos em seu cluster Kubernetes.
- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Repositório de código

O código desse padrão está disponível no repositório GitHub EKS Multi-Tenancy Terraform Solution.

Práticas recomendadas

Para obter diretrizes e melhores práticas para usar essa implementação, consulte o seguinte:

- Melhores práticas de multilocação do Amazon EKS
- Documentação do Flux

Épicos

Crie pipelines para os estágios de construção, teste e implantação do Terraform

Tarefa	Descrição	Habilidades necessárias
Clone o repositório do projeto.	Clone o repositório GitHub EKS Multi-Tenancy Terraform Solution executando o seguinte comando em uma janela de terminal: `git clone https://github.com/aws-samples/aws-eks-multitenancy-deployment.git`	AWS DevOps
Inicialize o bucket do Terraform S3 e o Amazon DynamoDB.	1. Na `bootstrap` pasta, abra o `bootstrap.sh` arquivo e atualize os valores das variáveis para o nome do bucket do	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	S3, o nome da tabela do DynamoDB e: Região da AWS
	
	`S3_BUCKET_NAME="<S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME="<DYNAMODB_NAME>" REGION="<AWS_REGION>"`
	
	2. Execute o script `bootstrap.sh` . O script requer o AWS CLI, que você instalou como parte dos pré-requisitos.
	
	`cd bootstrap ./bootstrap.sh`	

Tarefa	Descrição	Habilidades necessárias

Atualize `run.sh` os `locals.tf` arquivos e.	1. Depois que o processo de bootstrap for concluído com êxito, copie o bucket do S3 e o nome da tabela do DynamoDB da seção do script: `variables bootstrap.sh`
	`# Variables S3_BUCKET_NAME="< S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME ="<DYNAMODB_NAME"`
	2. Cole esses valores no `run.sh` script, que está no diretório raiz do projeto:
	`BACKEND_BUCKET_ID= "<SAME_NAME_AS_S3_ BUCKET_NAME>" DYNAMODB_ID=" <SAME_NAME_AS_DYNA MODB_NAME>"`
	3. Faça o upload do código do projeto em um CodeCommi t repositório. Você pode criar automaticamente esse repositório por meio do Terraform definindo a seguinte variável `true` no `demo/pipeline/loca ls.tf` arquivo:
	`create_new_repo = true`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	4. Atualize o `locals.tf` arquivo de acordo com seus requisitos para criar recursos de pipeline.	

Implante o módulo de pipeline.	Para criar recursos de pipeline, execute os seguintes comandos do Terraform manualmente. Não há orquestração para executar esses comandos automatic amente.
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t init`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t plan`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t apply`
		AWS DevOps

Crie a infraestrutura de rede

Tarefa	Descrição	Habilidades necessárias
Iniciar o pipeline.	1. Na `templates` pasta, verifique se os `buildspec` arquivos têm a seguinte variável definida como`network`: `TF_MODULE_TO_BUILD: "network"`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	2. No CodePipeline console, na página de detalhes do pipeline, inicie o pipeline escolhendo Release change. Após essa primeira execução, o pipeline é iniciado automatic amente sempre que você confirma uma alteração na ramificação principal do CodeCommit repositório. O pipeline inclui os seguintes estágios: • `validate`inicializa o Terraform, executa as verificações de segurança do Terraform usando as ferramentas checkov e tfsec e carrega os relatórios de verificação no bucket do S3. • `plan` mostra o plano do Terraform e carrega o plano no bucket do S3. • `apply`aplica a saída do plano Terraform do bucket S3 e cria AWS recursos. • `destroy`remove os AWS recursos criados durante o `apply` estágio. Para ativar esse estágio opcional, defina a seguinte variável	

Tarefa	Descrição	Habilidades necessárias
	`true` no `demo/pipeline/locals.tf` arquivo: `enable_destroy_stage = true`	

Tarefa	Descrição	Habilidades necessárias
Valide os recursos criados por meio do módulo de rede.	Confirme se os seguintes AWS recursos foram criados após a implantação bem-sucedida do pipeline: • Uma VPC de saída com três sub-redes públicas e três privadas, gateway de internet e gateway NAT. • Uma VPC Amazon EKS com três sub-redes privadas. • Locatário 1 e Locatário 2 VPCs com três sub-redes privadas cada. • Um gateway de trânsito com todos os anexos e rotas de VPC para cada sub-rede privada. • Uma rota estática de gateway de trânsito para a VPC de saída do Amazon EKS com um bloco CIDR de destino de. `0.0.0.0/0` Isso é necessário para permitir que todos tenham acesso de saída VPCs à Internet por meio da VPC de saída do Amazon EKS.	AWS DevOps

Crie a infraestrutura computacional

Tarefa	Descrição	Habilidades necessárias

Atualize `locals.tf` para permitir o acesso do CodeBuild projeto à VPC.	Para implantar os complementos para o cluster privado do Amazon EKS, o CodeBuild projeto deve ser anexado à VPC do Amazon EKS.
	1. Na `demo/pipeline` pasta, abra o `locals.tf` arquivo e defina a `vpc_enabled` variável como `true`.
	2. Execute o `run.sh` script para aplicar as alterações no módulo de pipeline:
	`demo/pipeline/locals.tf`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd init`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd plan`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd apply`
		AWS DevOps

Atualize os `buildspec` arquivos para criar o módulo computacional.	Na `templates` pasta, em todos os arquivos `buildspec` YAML, defina o valor da `TF_MODULE_TO_BUILD`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	variável de `network` para `compute`: `TF_MODULE_TO_BUILD: "compute"`	

Tarefa	Descrição	Habilidades necessárias

Atualize o `values` arquivo do gráfico Helm de gerenciam ento de inquilinos.	1. Abra o `values.yaml` arquivo no seguinte local:
	`cd cfg-terraform/demo/compute/cfg-tenant-mgmt`
	O arquivo tem a seguinte aparência:
	`---`
	`global:`
	`  clusterRoles:`
	`  operator:`
	`  platform-tenant`
	`  flux: flux-tenant-applier`
	`  flux:`
	`  tenantCloneBaseUrl: ${TEANT_BASE_URL}`
	`  repoSecret:`
	`  ${TENANT_REPO_SECRET}`
	`tenants:`
	`  tenant-1:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 1Gi`
	`  flux:`
	`  path: overlays/tenant-1`
	`  tenant-2:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 2Gi`
	`  flux:`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`path: overlays/tenant-2` 2. Nas `tenants` seções `global` e, atualize a configuração com base em seus requisitos: • `tenantCloneBaseUrl` — Caminho para o repositório que hospeda o código para todos os locatários (usamos o mesmo repositório Git para todos os inquilinos) • `repoSecret` — Segredo do Kubernetes que contém as chaves SSH e os hosts conhecidos para autenticação no repositório Git global de locatários • `quotas`— Cotas de recursos do Kubernetes que você deseja aplicar para cada inquilino • `flux path`— Caminho para os arquivos YAML do aplicativo inquilino no repositório global de inquilinos	

Tarefa	Descrição	Habilidades necessárias
Valide os recursos computacionais.	Depois de atualizar os arquivos nas etapas anteriores, CodePipeline inicia automaticamente. Confirme se ele criou os seguintes AWS recursos para a infraestrutura computacional: • Cluster Amazon EKS com endpoint privado • Nós de trabalho do Amazon EKS • Complementos do Amazon EKS: segredos externos `aws-loadbalancer-controller` e `metrics-server` • GitOps módulo, gráfico Flux Helm, gráfico Cilium Helm e gráfico Helm de gerenciamento de inquilinos	AWS DevOps

Verifique o gerenciamento de inquilinos e outros recursos

Tarefa	Descrição	Habilidades necessárias
Valide os recursos de gerenciamento de inquilinos no Kubernetes.	Execute os comandos a seguir para verificar se os recursos de gerenciamento de inquilinos foram criados com êxito com a ajuda do Helm. 1. Os namespaces do inquilino foram criados,	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	conforme especificado em: `values.yaml`
	`kubectl get ns -A`
	2. As cotas são atribuídas a cada namespace de inquilino, conforme especificado em: `values.yaml`
	`kubectl get quota --namespace=<tenant_namespace>`
	3. Os detalhes das cotas estão corretos para cada namespace de inquilino:
	`kubectl describe quota cpu-memory-resource-quota-limit -n <tenant_namespace>`
	4. As políticas de rede Cilium foram aplicadas a cada namespace de inquilino:
	`kubectl get CiliumNetworkPolicy -A`	

Tarefa	Descrição	Habilidades necessárias

Verifique as implantações de aplicativos do locatário.	Execute os comandos a seguir para verificar se os aplicativos do locatário foram implantados.
	
	1. O Flux é capaz de se conectar ao CodeCommit repositório especificado no GitOps módulo:
	
	`kubectl get gitrepositories -A`
	
	2. O controlador de personalização do Flux implantou os arquivos YAML no repositório: CodeCommit
	
	`kubectl get kustomizations -A`
	
	3. Todos os recursos do aplicativo são implantados em seus namespaces de locatário:
	
	`kubectl get all -n <tenant_namespace>`
	
	4. Uma entrada foi criada para cada inquilino:
	
	`kubectl get ingress -n <tenant_namespace>`	

Solução de problemas

Problema	Solução

Você encontra uma mensagem de erro semelhante à seguinte:
 	
`Failed to checkout and determine revision: unable to clone unknown error: You have successfully authenticated over SSH. You can use Git to interact with AWS CodeCommit.`
	Siga estas etapas para solucionar o problema:
	
	1. Verifique o repositório do aplicativo inquilino : um repositório vazio ou mal configurado pode estar causando o erro. Certifique-se de que o repositório do aplicativo do locatário contenha o código necessário.
	2. Reimplante o `tenant_mgmt` módulo: no arquivo de configuração do `tenant_mgmt` módulo, localize o `app` bloco e defina o `deploy` parâmetro como: `0`
	
	`deploy = 0`
	
	Depois de executar o `apply` comando do Terraform, altere o valor do `deploy` parâmetro de volta para`1`:
	
	`deploy = 1`
	
	3. Verifique novamente o status: depois de executar as etapas anteriores, use o comando a seguir para verificar se o problema persiste:
	
	`kubectl get gitrepositories -A`
	
	Se persistir, considere se aprofundar nos registros do Flux para obter mais detalhes ou consulte o guia geral de solução de problemas do Flux.

Recursos relacionados

- Amazon EKS Blueprints para Terraform
- Guias de melhores práticas do Amazon EKS, seção de multilocação
- Site do Flux
- Site do Helm

Mais informações

Aqui está um exemplo de estrutura de repositório para implantar aplicativos de locatários:

```
applications
sample_tenant_app
### README.md
### base
#   ### configmap.yaml
#   ### deployment.yaml
#   ### ingress.yaml
#   ### kustomization.yaml
#   ### service.yaml
### overlays
    ### tenant-1
    #   ### configmap.yaml
    #   ### deployment.yaml
    #   ### kustomization.yaml
    ### tenant-2
        ### configmap.yaml
        ### kustomization.yaml
```

Assinar vários endpoints de e-mail em um tópico do SNS usando um recurso personalizado

Criado por Ricardo Morais (AWS)

Resumo

Observação, agosto de 2022: a AWS CloudFormation agora oferece suporte à assinatura de vários recursos por meio do AWS::SNS::Topicobjeto e de seu atributo Subscription.

Esse padrão descreve como assinar vários endereços de e-mail para receber notificações de um tópico do Amazon Simple Notification Service (Amazon SNS). Ele usa uma função do AWS Lambda como um recurso personalizado em um modelo da AWS CloudFormation . A função do Lambda está associada a um parâmetro de entrada que especifica os endpoints de e-mail para o tópico do SNS.

Atualmente, você pode usar os objetos de CloudFormation modelo da AWS AWS::SNS::Topice AWS::SNS::Subscriptioninscrever endpoints únicos em tópicos do SNS. Para assinar vários endpoints, você precisa invocar o objeto várias vezes. Ao usar a função do Lambda como um recurso personalizado, você pode assinar vários endpoints por meio de um parâmetro de entrada. Você pode usar essa função Lambda como um recurso personalizado em qualquer modelo da AWS CloudFormation .

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um perfil da AWS configurado em seu ambiente local com uma chave de acesso e uma chave secreta.
- Permissões para o seguinte:
  - Perfil e política do AWS do perfil do Identity and Access Management (IAM)
  - Função do AWS Lambda
  - Amazon Simple Storage Service (Amazon S3) para fazer upload da função do Lambda
  - Política e tópico do Amazon SNS
  - Pilhas da AWS CloudFormation

Limitações

- O código é compatível com estações de trabalho Linux e macOS.

Versões do produto

- AWS Command Line Interface (AWS CLI) versão 2 ou superior.

Arquitetura

Pilha de tecnologias de destino

- AWS CloudFormation
- Amazon SNS
- AWS Lambda

Ferramentas

Ferramentas

- AWS CLI versão 2

Código

O anexo inclui os seguintes arquivos:

- Função do Lambda: `lambda_function.py`
- CloudFormation Modelo da AWS: `template.yaml`
- Dois arquivos de parâmetros para lidar com várias assinaturas de endpoint de e-mail ou de um único terminal: `parameters-multiple-values.json` (usado como padrão) e `parameters-one-value.json`

Para implantar a pilha, você pode usar qualquer um dos arquivos de parâmetros. Para especificar vários endpoints de e-mail:

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>
```

Para especificar um único endpoint de e-mail:

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json
```

Épicos

Opção 1 - Implantar um tópico do SNS com uma assinatura de e-mail

Tarefa	Descrição	Habilidades necessárias
Configurar o endpoint de e-mail para assinaturas de tópicos do SNS.	Editar o arquivo `parameters-one-value.json` (em anexo) e alterar o valor do parâmetro `pSNSNotificationsEmail` para refletir o endereço de e-mail que você deseja usar, como `someone@example.com` .	
Implante a CloudFormation pilha da AWS que cria os recursos e a assinatura.	Execute o comando deploy.sh com o nome do seu perfil da AWS, a região da AWS e o arquivo `parameters-one-value.json` . `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json`	Perfil do IAM com permissões adequadas

Opção 2 - Implantar um tópico do SNS com uma ou mais assinaturas de e-mail

Tarefa	Descrição	Habilidades necessárias
Configurar os endpoints de e-mail para assinaturas de tópicos do SNS.	Editar o arquivo `parameters-multiple-values.json` (em anexo) e alterar o valor do parâmetro `pSNSNotificationsEmail` para refletir o endereço de e-mail que você deseja usar, separado por vírgulas, como a seguir: `someone1@example.com, someone2@example.com` .	
Implante a CloudFormation pilha da AWS que cria os recursos e a assinatura.	Execute o comando deploy.sh com o nome do seu perfil da AWS e a região da AWS. Você não precisa especificar o arquivo `parameters-multiple-values.json` porque ele é usado por padrão. `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>`	Perfil do IAM com permissões adequadas

Opção 3 - Implantar um tópico do SNS por meio de um modelo da AWS CloudFormation

Tarefa	Descrição	Habilidades necessárias
Criar um tópico do SNS.	Crie um tópico do SNS por meio de um CloudFormation modelo da AWS, sem	Perfil do IAM com permissões adequadas

Tarefa	Descrição	Habilidades necessárias
	especificar endpoints de assinatura no objeto do `AWS::SNS::Topic` modelo. Você pode usar `template.yaml` no anexo como ponto de partida.	
Criar uma política de tópico do SNS.	Crie uma política de tópicos do SNS no CloudFormation modelo da AWS.	Perfil do IAM com permissões adequadas
Inscreva a lista de endpoints de e-mail no tópico do SNS.	Com base na lista de endpoints de e-mail (um ou mais), inscreva os endpoints no tópico do SNS que você criou.	Perfil do IAM com permissões adequadas

Recursos relacionados

Referências

- Recursos CloudFormation personalizados da AWS (documentação da AWS)
- Criação de recursos CloudFormation personalizados da AWS com Python, AWS Lambda e crhelper (postagem do blog)

Ferramentas necessárias

- AWS CLI versão 2

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Coordene a dependência de recursos e a execução de tarefas usando a AWS Fargate WaitCondition construção de gancho

Criado por Stan Fan (AWS)

Resumo

Esse padrão descreve o pacote WaitCondition hook (`waitcondition-hook-for-aws-fargate-task`) npm, que é uma solução nativa da nuvem projetada para orquestrar AWS Fargatetarefas em clusters do Amazon Elastic Container Service (Amazon ECS).

O WaitCondition gancho é uma AWS Cloud Development Kit (AWS CDK) construção especificamente adaptada para integração com AWS CloudFormation. O WaitCondition gancho fornece os seguintes recursos principais:

- Atua como um mecanismo de condição de espera, pausando a execução da CloudFormation pilha até que uma tarefa específica do Fargate seja concluída, o que ajuda nas implantações ordenadas e no provisionamento de recursos.
- Suportes TypeScript e Python, o que o torna ideal para AWS CDK projetos.
- Permite que desenvolvedores e arquitetos orquestrem implantações coordenando a conclusão de tarefas e o gerenciamento de recursos para aplicativos em contêineres no. AWS
- Permite executar tarefas do Fargate com um ou vários contêineres incorporados em um CloudFormation ciclo de vida e pode lidar com falhas de tarefas e reverter a pilha após uma falha na CloudFormation tarefa.
- Oferece flexibilidade para adicionar dependências entre os recursos e os resultados da execução de tarefas do Fargate, permitindo tarefas personalizadas ou invocando outros endpoints. Por exemplo, você pode pausar uma CloudFormation pilha e aguardar a migração do banco de dados (feita por uma tarefa do Fargate) e provisionar outros recursos que podem depender do sucesso da migração do banco de dados.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.

- AWS Cloud Development Kit (AWS CDK) Interface de linha de comando (CLI) instalada em uma estação de trabalho local. Para obter mais informações, consulte a referência da AWS CDK CLI na AWS CDK documentação.
- Gerenciador de pacotes Node (npm), instalado em uma estação de trabalho local e configurado para entrada.AWS CDK TypeScript Para obter mais informações, consulte Download e instalação do Node.js e npm, na documentação do npm.
- Yarn instalado em uma estação de trabalho local. Para obter mais informações, consulte Instalação na documentação do Yarn.

Limitações

- Essa solução é implantada em um único Conta da AWS.
- O código de retorno esperado do contêiner é `0` para o sucesso. Qualquer outro código de retorno indica falha e a CloudFormation pilha será revertida.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra a arquitetura da construção.

O diagrama mostra o fluxo de trabalho de`waitcondition-hook-for-aws-fargate-task`:

1. `WaitCondition`e `WaitConditionHandler` são provisionados para ouvir a resposta das AWS Lambda funções.
2. Dependendo do resultado da tarefa, o `CallbackFunction` ou o `ErrorHandlerFunction` é acionado pelo término da tarefa do Fargate.
3. A função Lambda envia um sinal de SUCESSO ou FALHA para. `WaitConditionHandler`
4. `WaitConditionHandler`continua provisionando os recursos se o resultado da execução da tarefa do Fargate for bem-sucedido ou reverte a pilha se a tarefa falhar.

O diagrama a seguir mostra um exemplo de fluxo de trabalho para realizar uma migração de banco de dados.

O exemplo de fluxo de trabalho usa a `waitcondition-hook-for-aws-fargate-task` construção para realizar uma migração de banco de dados, da seguinte forma:

1. Uma instância do Amazon Relational Database Service (Amazon RDS) é provisionada.
2. A `waitcondition-hook-for-aws-fargate-task` construção executa a tarefa de migração do banco de dados e pausa a pilha como uma instância do Amazon Elastic Compute Cloud (Amazon EC2).
3. Se a tarefa de migração for concluída com êxito, ela enviará um sinal de sucesso para CloudFormation. Caso contrário, ele envia um sinal de falha CloudFormation e reverte a pilha.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir a infraestrutura de nuvem em código e provisioná-la por meio dela AWS CloudFormation.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- AWS Fargateajuda você a executar contêineres sem precisar gerenciar servidores ou EC2 instâncias da Amazon. É usado em conjunto com o Amazon ECS.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual se assemelha a uma rede tradicional que você operaria em seu próprio data center, com os benefícios de usar a infraestrutura escalável do. AWS

Outras ferramentas

- O npm é um registro de software executado em um ambiente Node.js e usado para compartilhar ou emprestar pacotes e gerenciar a implantação de pacotes privados.
- O Yarn é um gerenciador de pacotes de código aberto que você pode usar para gerenciar dependências em JavaScript projetos. O Yarn pode ajudá-lo a instalar, atualizar, configurar e remover dependências de pacotes.

Repositório de código

O código desse padrão está disponível no repositório GitHub waitcondition-hook-for-aws-fargate-task.

Práticas recomendadas

- Ao criar seu AWS CDK aplicativo, siga as melhores práticas para desenvolver e implantar a infraestrutura de nuvem AWS CDK na documentação AWS CDK v2.
- Para a AWS Fargate tarefa, siga as melhores práticas para imagens de contêineres do Amazon ECS na documentação do Amazon ECS.

Épicos

Configure o AWS CDK

Tarefa	Descrição	Habilidades necessárias
Instale AWS CDK o.	Para instalar o AWS CDK em sua máquina local ou em outro ambiente, execute o seguinte comando:	Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`npm install -g aws-cdk@latest`	
Inicialize o. AWS CDK	O bootstrapping é o processo de preparar um ambiente para implantação. Para inicializar seu AWS CDK kit de ferramentas para o destino Conta da AWS e Região da AWS, execute o seguinte comando: `cdk bootstrap aws://ACCOUNT-NUMBER-1/REGION-1` Esse comando cria uma CloudFormation pilha chamada`CDKToolkit` .	Arquiteto de nuvem

Execute o WaitCondition gancho para construir AWS Fargate tarefas

Tarefa	Descrição	Habilidades necessárias
Crie o projeto CDK.	Crie um projeto CDK usando a linguagem que você preferir. Esse padrão usa TypeScript. Para criar um projeto CDK usando TypeScript, execute o seguinte comando: `cdk init app –language typescript`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Instale o pacote .	Execute `npm install` no caminho raiz do seu projeto CDK. Depois que a biblioteca CDK for instalada, execute o seguinte comando para instalar`waitcondition-hook-for-aws-fargate-task` : `yarn add waitcondition-hook-for-aws-fargate-task`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

Crie seu aplicativo CDK e componentes do Amazon ECS.	Crie seu projeto CDK. É necessário um recurso de definição de tarefas do Amazon ECS. Para obter informações sobre a criação de uma definição de tarefa, consulte as definições de tarefas do Amazon ECS na documentação do Amazon ECS.
	
	O exemplo a seguir usa essa construção:
	
	`import * as cdk from 'aws-cdk-lib';`
	`import { Vpc } from 'aws-cdk-lib/aws-ec2';`
	`import * as ecr from 'aws-cdk-lib/aws-ecr';`
	`import * as ecs from 'aws-cdk-lib/aws-ecs';`
	`import { Construct } from 'constructs';`
	`import { FargateRunner } from 'waitcondition-hook-for-aws-fargate-task';`
	`import { Queue } from 'aws-cdk-lib/aws-sqs';`
	
	`export class FargateRunnerStack extends cdk.Stack {`
		Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

	constructor(scope: Construct, id: string, props?: cdk.StackProps) {
	super(scope, id, props);
	// Define the VPC
	const vpc = new Vpc(this, 'MyVpc')
	// Define the Fargate Task
	const taskDefinition = new ecs.FargateTaskDefinition(this, 'MyTask', {});
	// Import exiting ecr repo
	const repo = ecr.Repository.fromRepositoryName(this, 'MyRepo', 'RepoName');
	// Add a container to the task
	taskDefinition.addContainer('MyContainer', {
	image: ecs.ContainerImage.fromEcrRepository(repo),
	});
	// Create the Fargate runner
	const myFargateRunner = new FargateRunner(this, 'MyRunner', {
	fargateTaskDef: taskDefinition,
	timeout: `${60 * 5}`,	

Tarefa	Descrição	Habilidades necessárias

	<pre>vpc: vpc,
	        });
	        // Create the SQS queue
	        const myQueue = new Queue(this, 'MyQueue', {});
	        // Add dependency
	        myQueue.node.addDependency(myFargateRunner);
	    }
	}</pre>	

Sintetize e inicie o aplicativo CDK.	1. Para gerar os ativos e o CloudFormation modelo, execute o seguinte comando no caminho raiz do CDK:
	
	`cdk synth`
	
	2. Depois que o `synth` comando for bem-sucedido, execute o comando a seguir para implantar os recursos:
	
	`cdk deploy`
	
	A `waitcondition-hook-for-aws-fargate-task` construção executa a tarefa Fargate.
		Arquiteto de nuvem

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpar os recursos	Para limpar os recursos provisionados na etapa anterior, execute o seguinte comando: `cdk destroy`	Arquiteto de nuvem

Solução de problemas

Problema	Solução
Falha geral CloudFormation na pilha	Para ajudar a solucionar falhas gerais de CloudFormation pilha, adicione o `--no-rollback` sinalizador conforme mostrado no exemplo a seguir: `cdk deploy --no-rollback` Esse comando interromperá a reversão da CloudFormation pilha, o que fornece recursos para solucionar problemas. Para obter mais informações, consulte Escolha como lidar com falhas ao provisionar recursos na AWS CloudFormation documentação.
AWS Step Functions falha	Uma máquina de AWS Step Functions estado pode falhar na execução por diferente s motivos. Com `–disable-rollback` configurado, use as seguintes etapas para solucionar problemas:

Problema	Solução
	1. Faça login no AWS Management Console, insira Step Functions no campo Pesquisar e escolha o serviço Step Functions. 2. No painel de navegação esquerdo, escolha Máquinas de estado e, em seguida, selecione a máquina de estado que é provisionada pela pilha. CloudFormation 3. Em Execuções, escolha o nome da execução que falhou inesperadamente. 4. Na visualização do Evento, escolha a etapa que falhou. Para obter mais informações, consulte Solução de problemas no Step Functions e Visualização dos detalhes da execução no console do Step Functions na AWS Step Functions documentação.

Problema	Solução
AWS Lambda falha de função	Essa construção provisiona duas funções Lambda: e. `CallbackFunction` `Errorhandlerfunction` Eles podem falhar por vários motivos, como exceções não tratadas. Use as etapas a seguir para solucionar problemas: 1. Faça login no AWS Management Console, insira CloudWatchno campo Pesquisar e escolha o CloudWatch serviço. 2. No painel de navegação esquerdo, escolha Log groups (Grupos de log). 3. No campo Pesquisar, insira o nome da função Lambda. 4. Escolha o nome do grupo de registros associado à função Lambda. 5. Para acessar o resultado da execução da função Lambda, escolha o fluxo de log mais recente. Para obter mais informações, consulte Solução de problemas no Lambda na AWS Lambda documentação.

Recursos relacionados

AWS documentação

- AWS CDK Referência da API Construct
- Começando com o AWS CDK
- Saiba como criar e usar os recursos do Amazon ECS
- Saiba como começar a usar o Step Functions
- O que AWS CDKé

Outros recursos

- Gancho de condição de espera para AWS Fargate tarefa (npm)
- waitcondition-hook-for-aws-fargate-task 1.0.6 (pypi.org)

Use repositórios de origem Git de terceiros na AWS CodePipeline

Criado por Kirankumar Chandrashekar (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão descreve como usar a AWS CodePipeline com repositórios de origem Git de terceiros.

CodePipelineA AWS é um serviço de entrega contínua que automatiza tarefas para criar, testar e implantar seu software. Atualmente, o serviço oferece suporte a repositórios Git gerenciados pela GitHub AWS e pela Atlassian CodeCommit Bitbucket. No entanto, algumas empresas usam repositórios Git de terceiros que são integrados ao serviço de autenticação única (SSO) e ao Microsoft Active Directory para autenticação. Você pode usar esses repositórios Git de terceiros como fontes para criar ações e CodePipeline webhooks personalizados.

Um webhook é uma notificação HTTP que detecta eventos em outra ferramenta, como um GitHub repositório, e conecta esses eventos externos a um pipeline. Quando você cria um webhook no CodePipeline, o serviço retorna uma URL que você pode usar no webhook do seu repositório Git. Se você enviar o código para uma ramificação específica do repositório Git, o webhook do Git iniciará o CodePipeline webhook por meio dessa URL e definirá o estágio de origem do pipeline como Em andamento. Quando o pipeline está nesse estado, um funcionário pesquisa CodePipeline o trabalho personalizado, executa o trabalho e envia um status de sucesso ou falha para CodePipeline. Nesse caso, como o pipeline está no estágio de origem, o operador de trabalho obtém o conteúdo do repositório Git, compacta o conteúdo e o carrega no bucket do Amazon Simple Storage Service (Amazon S3), onde os artefatos do pipeline são armazenados, usando a chave de objeto fornecida pelo trabalho pesquisado. Você também pode associar uma transição para a ação personalizada a um evento na Amazon CloudWatch e iniciar o funcionário com base no evento. Essa configuração permite que você use repositórios Git de terceiros para os quais o serviço não oferece suporte nativo como fontes. CodePipeline

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um repositório Git que suporta webhooks e pode se conectar a uma CodePipeline URL de webhook pela Internet

- AWS Command Line Interface (AWS CLI), instalada e configurada para trabalhar com a conta da AWS

Arquitetura

O padrão envolve as seguintes etapas:

1. O usuário confirma o código em um repositório Git.
2. O webhook do Git é chamado.
3. O CodePipeline webhook é chamado.
4. O pipeline é definido como Em andamento e o estágio de origem está definido para o estado Em andamento.
5. A ação do estágio de origem inicia uma regra de CloudWatch Eventos, indicando que ela foi iniciada.
6. O CloudWatch evento inicia uma função Lambda.
7. A função do Lambda obtém os detalhes do trabalho de ação personalizado.
8. A função Lambda inicia a CodeBuild AWS e passa todas as informações relacionadas ao trabalho.
9. CodeBuild obtém a chave SSH pública ou as credenciais do usuário para acesso HTTPS Git do Secrets Manager.
10. CodeBuild clona o repositório Git para uma ramificação específica.
11. CodeBuild compacta o arquivo e o carrega no bucket do S3 que serve como armazenamento de artefatos. CodePipeline

Ferramentas

- AWS CodePipeline — CodePipeline A AWS é um serviço de entrega contínua totalmente gerenciado que ajuda você a automatizar seus pipelines de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura. CodePipeline automatiza as fases de criação, teste e implantação do seu processo de lançamento para cada alteração de código, com base no modelo de lançamento que você define. Isso permite entregar recursos e atualizações de forma rápida e confiável. Você pode integrar a AWS CodePipeline com serviços de terceiros, como GitHub ou com seu próprio plug-in personalizado.

- AWS Lambda: o AWS Lambda permite executar código sem provisionar ou gerenciar servidores. Com o Lambda, você pode executar o código em praticamente qualquer tipo de aplicação ou serviço de backend sem a necessidade de administração. Você carrega seu código e o Lambda cuidará de tudo que for necessário para executar e escalar seu código com alta disponibilidade. Você pode configurar o seu código para que ele seja iniciado automaticamente por meio de outros serviços da AWS ou chamá-lo diretamente usando qualquer aplicativo móvel ou da web.
- AWS CodeBuild — CodeBuild A AWS é um serviço de integração contínua totalmente gerenciado que compila código-fonte, executa testes e produz pacotes de software prontos para implantação. Com CodeBuild, você não precisa provisionar, gerenciar e escalar seus próprios servidores de compilação. CodeBuild escala continuamente e processa várias compilações simultaneamente, para que suas compilações não fiquem esperando em uma fila. Você pode começar a usar ambientes de compilação pré-empacotados rapidamente ou criar ambientes de compilação personalizados que usem suas próprias ferramentas de compilação.
- AWS Secrets Manager: o AWS Secrets Manager ajuda você a proteger os segredos necessários para acessar seus aplicativos, serviços e recursos de TI. O serviço permite alternar, gerenciar e recuperar credenciais de banco de dados, chaves de API e outros segredos durante seu ciclo de vida. Usuários e aplicativos recuperam segredos chamando o Secrets Manager APIs, sem precisar codificar informações confidenciais em texto simples. O Secrets Manager oferece alternância secreta com integração embutida para o Amazon Relational Database Service (Amazon RDS), o Amazon Redshift e o Amazon DocumentDB. O serviço pode ser estendido para oferecer suporte a outros tipos de segredos, incluindo chaves e OAuth tokens de API. Além disso, o Secrets Manager permite que você controle o acesso a segredos usando permissões refinadas e audite centralmente a rotação de segredos para recursos na nuvem AWS, serviços de terceiros e ambientes on-premises.
- Amazon CloudWatch — CloudWatch A Amazon é um serviço de monitoramento e observação criado para DevOps engenheiros, desenvolvedores, engenheiros de confiabilidade de sites (SREs) e gerentes de TI. CloudWatch fornece dados e insights acionáveis para monitorar seus aplicativos, responder às mudanças de desempenho em todo o sistema, otimizar a utilização de recursos e obter uma visão unificada da integridade operacional. CloudWatch coleta dados operacionais e de monitoramento na forma de registros, métricas e eventos, fornecendo a você uma visão unificada dos recursos, aplicativos e serviços da AWS que são executados na AWS e em servidores locais. Você pode usar CloudWatch para detectar comportamentos anômalos em seus ambientes, definir alarmes, visualizar registros e métricas lado a lado, realizar ações automatizadas, solucionar problemas e descobrir insights para manter seus aplicativos funcionando sem problemas.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que permite armazenar e proteger qualquer volume de dados para uma variedade de

casos de uso, como sites, aplicativos móveis, backup e restauração, arquivamento, aplicativos corporativos, dispositivos IoT e análise de big data. O Amazon S3 fornece recursos easy-to-use de gerenciamento para ajudá-lo a organizar seus dados e configurar controles de acesso bem ajustados para atender aos seus requisitos comerciais, organizacionais e de conformidade específicos.

Épicos

Crie uma ação personalizada no CodePipeline

Tarefa	Descrição	Habilidades necessárias
Crie uma ação personalizada usando a AWS CLI ou a AWS. CloudFormation	Essa etapa envolve a criação de uma ação de origem personalizada que pode ser usada no estágio de origem de um pipeline em sua conta da AWS em uma região específica. Você deve usar a AWS CLI ou a AWS CloudFormation (não o console) para criar a ação de origem personalizada. Para obter mais informações sobre os comandos e etapas descritos neste e em outros épicos, consulte a seção “Recursos relacionados” no final desse padrão. Na AWS CLI, use o create-custom-action-type comando. Use --configuration-properties para fornecer todos os parâmetros necessários para o trabalhador processar ao pesquisar um trabalho. CodePipeline Certifique-se de observar os	AWS geral

Tarefa	Descrição	Habilidades necessárias
	valores fornecidos às opções --provider e --action-version, para que você possa usar os mesmos valores ao criar o pipeline com esse estágio de origem personalizado. Você também pode criar a ação de origem personalizada na AWS CloudFormation usando o tipo de recurso AWS::CodePipeline::CustomActionType.	

Configurar a autenticação

Tarefa	Descrição	Habilidades necessárias
Crie um par de chaves SSH.	Crie um par de chaves do Secure Shell (SSH). Para obter instruções, consulte a GitHub documentação.	Sistemas/engenheiro DevOps
Crie um segredo no AWS Secrets Manager.	Copie o conteúdo da chave privada do par de chaves do SSH e crie um segredo no AWS Secrets Manager. Esse segredo é usado para autenticação ao acessar o repositório Git.	AWS geral
Adicione a chave pública ao repositório Git.	Adicione a chave pública do par de chaves do SSH às configurações da conta do repositório Git para autentica ção na chave privada.	Sistemas/engenheiro DevOps

Criar um pipeline e um webhook

Tarefa	Descrição	Habilidades necessárias
Crie um pipeline que inclua a ação de origem personalizada.	Crie um pipeline em CodePipeline. Ao configurar o estágio de origem, escolha a ação de origem personalizada que você criou anteriormente. Você pode fazer isso no CodePipeline console da AWS ou na AWS CLI. CodePipeline solicita as propriedades de configuração que você definiu na ação personalizada. Essas informações são necessárias para que o funcionário processe o trabalho para a ação personalizada. Siga o assistente e crie a próxima etapa para o pipeline.	AWS geral
Crie um CodePipeline webhook.	Crie um webhook para o pipeline que você criou com a ação de origem personalizada. Você deve usar a AWS CLI ou a AWS CloudFormation (não o console) para criar o webhook. Na AWS CLI, execute o comando put-webhook e forneça os valores apropriados para as opções de webhook. Anote os valores do URL do webhook que o comando retorna. Se você estiver usando CloudFormation a AWS para	AWS geral

Tarefa	Descrição	Habilidades necessárias
	criar o webhook, use o tipo AWS::CodePipeline::Webhook de recurso. Certifique-se de enviar o URL do webhook do recurso criado e anote-o.	

Tarefa	Descrição	Habilidades necessárias
Crie uma função e um projeto Lambda. CodeBuild	Nesta etapa, você usa o Lambda e CodeBuild cria um funcionário que pesquisará as solicitações de trabalho CodePipeline para a ação personalizada, executará o trabalho e retornará o resultado do status para. CodePipeline Crie uma função Lambda que seja iniciada por uma regra da Amazon CloudWatch Events quando o estágio de ação da fonte personalizada do pipeline passa para “Em andamento”. Quando a função do Lambda é iniciada, ela deve obter os detalhes do trabalho de ação personalizada pesquisan do os trabalhos. Você pode usar a PollForJobs API para retornar essas informaçõ es. Depois que as informaçõ es do trabalho pesquisado forem obtidas, a função do Lambda deve retornar uma confirmação e, em seguida, processar as informações com os dados obtidos das propriedades de configura ção da ação personalizada. Quando o trabalhador estiver pronto para conversar com o repositório Git, você poderá	AWS geral e desenvolvedor de código

Tarefa	Descrição	Habilidades necessárias
	iniciar um CodeBuild projeto, pois é conveniente lidar com tarefas do Git usando o cliente SSH.	

Crie um evento em CloudWatch

Tarefa	Descrição	Habilidades necessárias
Crie uma regra de CloudWatch eventos.	Crie uma regra de CloudWatch eventos que inicie a função Lambda como alvo sempre que o estágio de ação personalizado do pipeline fizer a transição para “Em andamento”.	AWS geral

Recursos relacionados

Criando uma ação personalizada no CodePipeline

- Crie e adicione uma ação personalizada no CodePipeline
- AWS::CodePipeline::CustomActionType recurso

Configuração da autenticação

- Criação e gerenciamento de segredos com o AWS Secrets Manager

Criar um pipeline e um webhook

- Crie um pipeline em CodePipeline
- Referência do comando put-webhook
- AWS::CodePipeline::Webhook recurso

- PollForJobs Referência de API
- Crie e adicione uma ação personalizada no CodePipeline
- Crie um projeto de construção na AWS CodeBuild

Criar um evento

- Detecte e reaja às mudanças no estado do pipeline com o Amazon CloudWatch Events

Referências adicionais

- Trabalhando com oleodutos em CodePipeline
- Guia do desenvolvedor do AWS Lambda

Crie um pipeline de CI/CD para validar as configurações do Terraform usando a AWS CodePipeline

Criado por Aromal Raj Jayarajan (AWS) e Vijesh Vijayakumaran Nair (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão mostra como testar as configurações do HashiCorp Terraform usando um pipeline de integração contínua e entrega contínua (CI/CD) implantado pela AWS. CodePipeline

O Terraform é um aplicativo de interface da linha de comando que ajuda você a usar o código para fornecer e gerenciar a infraestrutura e os recursos da nuvem. A solução fornecida nesse padrão cria um pipeline de CI/CD que ajuda você a validar a integridade de suas configurações do Terraform executando cinco estágios: CodePipeline

1. `"checkout"`extrai a configuração do Terraform que você está testando de um repositório da AWS CodeCommit .
2. `"validate"`executa ferramentas de validação de infraestrutura como código (IaC), incluindo tfsec e TFLintcheckov. O estágio também executa os seguintes comandos de validação do Terraform IaC: `terraform validate` e `terraform fmt`.
3. `"plan"` mostra quais mudanças serão aplicadas à infraestrutura se a configuração do Terraform for aplicada.
4. `"apply"` usa o plano gerado para provisionar a infraestrutura necessária em um ambiente de teste.
5. `"destroy"` remove a infraestrutura de teste que foi criada durante o estágio `"apply"`.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI), instalado e configurado
- Git, instalado e configurado em sua máquina local

- Terraform, instalado e configurado em sua máquina local

Limitações

- A abordagem desse padrão implanta a AWS CodePipeline em uma conta da AWS e somente em uma região da AWS. Alterações na configuração são necessárias para implantações em várias contas e em várias regiões.
- O perfil do AWS Identity and Access Management (IAM) que esse padrão fornece (codepipeline_iam_role) segue o princípio do privilégio mínimo. As permissões desse perfil do IAM devem ser atualizadas com base nos recursos específicos que seu pipeline precisa criar.

Versões do produto

- AWS CLI versão 2.9.15 ou superior
- Terraform versão 1.3.7 ou superior

Arquitetura

Pilha de tecnologias de destino

- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- AWS IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Service (AWS KMS)
- Terraform

Arquitetura de destino

O diagrama a seguir mostra um exemplo de fluxo de trabalho de pipeline de CI/CD para testar as configurações do Terraform em. CodePipeline

O diagrama mostra o seguinte fluxo de trabalho:

1. Em CodePipeline, um usuário da AWS inicia as ações propostas em um plano do Terraform executando o `terraform apply` comando na CLI da AWS.
2. A AWS CodePipeline assume uma função de serviço do IAM que inclui as políticas necessárias para acessar CodeCommit o AWS KMS e o Amazon S3. CodeBuild
3. CodePipeline executa o estágio de `“checkout”` pipeline para extrair a configuração do Terraform de um CodeCommit repositório da AWS para testes.
4. CodePipeline executa o `“validate”` estágio para testar a configuração do Terraform executando as ferramentas de validação do IaC e executando os comandos de validação do Terraform IaC em um projeto. CodeBuild
5. CodePipeline executa o `“plan”` estágio para criar um plano no CodeBuild projeto com base na configuração do Terraform. O usuário da AWS pode revisar esse plano antes que as alterações sejam aplicadas ao ambiente de teste.
6. O Code Pipeline executa o `“apply”` estágio de implementação do plano usando o CodeBuild projeto para provisionar a infraestrutura necessária no ambiente de teste.
7. CodePipeline executa o `“destroy”` estágio, que é usado CodeBuild para remover a infraestrutura de teste que foi criada durante o `“apply”` estágio.
8. Um bucket do Amazon S3 armazena artefatos de pipeline, que são criptografados e descriptografados usando uma chave gerenciada pelo cliente do AWS KMS.

Ferramentas

Ferramentas

Serviços da AWS

- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outros serviços

- HashiCorp O Terraform é um aplicativo de interface de linha de comando que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.

Código

O código desse padrão está disponível no GitHub aws-codepipeline-terraform-cicdsamplesrepositório. O repositório contém as configurações do Terraform necessárias para criar a arquitetura de destino descrita nesse padrão.

Épicos

Provisione os componentes da solução

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Clone o GitHub aws-codepipeline-terraform-cicdsamplesrepositório executando o seguinte comando em uma janela de terminal: `git clone https://github.com/aws-samples/aws-codepipeline-terraform-cicd-samples.git` Para obter mais informações, consulte Clonar um repositório na GitHub documentação.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Crie um arquivo de definições de variáveis do Terraform.	Crie um arquivo `terraform.tfvars` com base nos requisitos do seu caso de uso. Você pode atualizar as variáveis no arquivo `examples/terraform.tfvars` que está no repositório clonado. Para obter mais informações, consulte Atribuição de valores às variáveis do módulo raiz na documentação do Terraform. **Note** O `Readme.md` arquivo do repositório inclui mais informaçõ es sobre as variáveis necessárias.	DevOps engenheiro
Configure a AWS como o provedor do Terraform.	1. Em um editor de código, abra o arquivo `main.tf` do repositório clonado. 2. Adicione as configurações necessárias para estabelec er a conectividade com a conta de destino da AWS. Para obter mais informaçõ es, consulte o provedor da AWS na documentação do Terraform.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Atualize a configuração do provedor Terraform para criar o bucket de replicação do Amazon S3.	1. Abra o diretório `S3` do repositório executando o seguinte comando: `cd ./modules/s3` 2. Atualize a configuração do provedor Terraform para criar o bucket de replicação do Amazon S3 atualizando o valor `region` no arquivo `tf` . Certifique-se de inserir a região para a qual você deseja que o Amazon S3 replique objetos. 3. (Opcional) Por padrão, o Terraform usa arquivos de estado locais para gerenciamento de estado. Se você quiser adicionar o Amazon S3 como backend remoto, você deve atualizar a configuração do Terraform. Para obter mais informações, consulte Configuração de backend na documentação do Terraform. **Note** A replicação ativa a cópia automática e assíncrona de	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	objetos nos buckets do Amazon S3.	
Inicialize a configuração do Terraform.	Para inicializar seu diretório de trabalho que contém os arquivos de configuração Terraform, execute o seguinte comando na pasta raiz do repositório clonado: `terraform init`	DevOps engenheiro
Crie o plano do Terraform.	Para criar um plano do Terraform, execute o seguinte comando na pasta raiz do repositório clonado: `terraform plan --var-file=terraform.tfvars -out=tfplan` **Note** O Terraform avalia os arquivos de configuração para determinar o estado de destino dos recursos declarados. Em seguida, ele compara o estado de destino com o estado atual e cria um plano.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Verifique o plano do Terraform .	Revise o plano do Terraform e confirme se ele configura a arquitetura necessária em sua conta da AWS de destino.	DevOps engenheiro
Implante a solução.	1. Para aplicar o plano do Terraform, execute o seguinte comando na pasta raiz do repositório clonado: `terraform apply "tfplan"` 2. Digite yes para confirmar que você deseja implantar os recursos. **Note** O Terraform cria, atualiza ou destrói a infraestrutura para atingir o estado de destino declarado nos arquivos de configuração.	DevOps engenheiro

Valide as configurações do Terraform executando o pipeline

Tarefa	Descrição	Habilidades necessárias
Configure o repositório de código-fonte.	1. Na saída do Terraform, obtenha os detalhes do repositório de origem do	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	repositório que contém as configurações do Terraform que você deseja validar. 2. Faça login no Console de Gerenciamento da AWS. Em seguida, abra o CodeCommit console. 3. Crie uma nova ramificação no repositório de origem chamada `main`. Para obter instruções, consulte Criar uma filial CodeCommit na AWS na CodeCommit documentação. 4. Clone a ramificação `main` do repositório de origem na sua estação de trabalho local. Para obter instruções, consulte Etapas de configuração para conexões HTTPS com CodeCommit repositórios da AWS no Windows com o auxiliar de credenciais da AWS CLI na documenta ção. CodeCommit 5. Copie a **`templates`** pasta do GitHub aws-codep ipeline-terraform-cicdsampl esrepositório executando o seguinte comando:	

Tarefa	Descrição	Habilidades necessárias
	`cp -r templates $YOUR_CODECOMMIT_REPO_ROOT` **Note** A `templates` pasta contém os arquivos de especificação de compilação e o script de validação do diretório raiz do repositório de origem. 6. Adicione as configurações necessárias do Terraform IaC à pasta raiz do repositório de origem. 7. Adicione os detalhes do backend remoto na configuração do Terraform do seu projeto. Para obter mais informações, consulte S3 na documentação do Terraform. 8. (Opcional) Atualize as variáveis na pasta `templates` para ativar ou desativar as verificações pré-configuradas, as versões de alteração da ferramenta e para especific	

Tarefa	Descrição	Habilidades necessárias
	ar seu diretório em arquivos de script personalizados. Para obter mais informaçõ es, consulte a seção Informações adicionais desse padrão. 9. Envie as alterações para a ramificação `main` do repositório de origem.	

Tarefa	Descrição	Habilidades necessárias
Valide os estágios do pipeline.	1. Faça login no Console de Gerenciamento da AWS e abra o console do CodePipeline . 2. Na saída gerada a partir do `terraform apply "tfplan"` comando na seção Epic anterior, encontre o nome do gerado CodePipeline. 3. Abra o pipeline no CodePipeline console e escolha Release change. 4. Revise cada estágio do pipeline e confirme se está funcionando conforme o esperado. Para obter mais informações, consulte Visualizar detalhes e histórico do pipeline (console) no Guia CodePipeline do usuário da AWS. **Important** Quando uma alteração é confirmada na ramificação principal do repositório de origem, o pipeline de teste é ativado automaticamente.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Verifique a saída do relatório.	1. No CodePipeline console, no painel de navegação esquerdo, escolha Construir. Em seguida, escolha Histórico de relatórios. 2. Revise os relatórios de verificação tfsec e checkov que o pipeline gera. Esses relatórios podem ajudá-lo a identificar problemas por meio de visualizações e representações gráficas. **Note** O `<project_name>-validate` CodeBuild projeto gera relatórios de vulnerabilidade para seu código durante a `“validate”` etapa.	DevOps engenheiro

Limpe os seus recursos

Tarefa	Descrição	Habilidades necessárias
Limpe o pipeline e os recursos associados.	Para excluir os recursos de teste da sua conta da AWS, execute o seguinte comando na pasta raiz do repositório clonado:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`terraform destroy --var-file=terraform.tfvars`	

Solução de problemas

Problema	Solução
Você recebe um AccessDenied erro durante a “`apply`” etapa.	1. Analise os registros de execução do CodeBuild projeto associado ao “`apply`” estágio para identificar as permissões ausentes do IAM. Para obter mais informaçõ es, consulte Exibir detalhes da construção na AWS CodeBuild no Guia CodeBuild do usuário da AWS. 2. Em um editor de código, abra a pasta `modules`do repositório clonado. Em seguida, navegue até a pasta `iam-role` e abra o arquivo `main.tf` que está nessa pasta. 3. Na declaração `codepipeline_polic y` , adicione as políticas do IAM que são necessárias para provisionar recursos em sua conta da AWS.

Recursos relacionados

- Blocos de módulos (documentação do Terraform)
- Como usar o CI/CD para implantar e configurar serviços de segurança da AWS com o Terraform (postagem no blog da AWS)
- Usando funções vinculadas ao serviço (documentação do IAM)
- create-pipeline (documentação da AWS CLI)

- Configure a criptografia do lado do servidor para artefatos armazenados no Amazon S3 para (documentação da AWS) CodePipeline CodePipeline
- Cotas para a AWS CodeBuild (CodeBuild documentação da AWS)
- Proteção de dados na AWS CodePipeline (CodePipeline documentação da AWS)

Mais informações

Módulos personalizados do Terraform

A seguir está uma lista de módulos personalizados do Terraform que são usados nesse padrão:

- `codebuild_terraform`cria os CodeBuild projetos que formam cada estágio do pipeline.
- `codecommit_infrastructure_source_repo`captura e cria o CodeCommit repositório de origem.
- `codepipeline_iam_role` cria os perfis do IAM necessários para o pipeline.
- `codepipeline_kms` cria a chave do AWS KMS necessária para criptografia e descriptografia de objetos do Amazon S3.
- `codepipeline_terraform`cria o pipeline de teste para o CodeCommit repositório de origem.
- `s3_artifacts_bucket` cria um bucket do Amazon S3 para gerenciar artefatos de pipeline.

Arquivos de especificação de compilação

Veja a seguir uma lista de arquivos de especificação de compilação (buildspec) que esse padrão usa para executar cada estágio do pipeline:

- `buildspec_validate.yml` executa o estágio "`validate`".
- `buildspec_plan.yml` executa o estágio "`plan`".
- `buildspec_apply.yml` executa o estágio "`apply`".
- `buildspec_destroy.yml` executa o estágio "`destroy`".

Variáveis do arquivo de especificação de compilação

Cada arquivo buildspec usa as seguintes variáveis para ativar diferentes configurações específicas da compilação:

Variável	Valor padrão	Descrição
CODE_SRC_DIR	"."	Define o CodeCommit diretório de origem
TF_VERSION	"1.3.7"	Define a versão do Terraform para o ambiente de construçã o

O arquivo buildspec_validate.yml também suporta as seguintes variáveis para ativar diferentes configurações específicas da compilação:

Variável	Valor padrão	Descrição
SCRIPT_DIR	"./templates/scripts"	Define o diretório do script
ENVIRONMENT	"dev"	Define o nome do ambiente
SKIPVALIDATIONFAIL URE	"Y"	Ignora a validação em caso de falhas
ENABLE_TFVALIDATE	"Y"	Ativa a validação do Terraform
ENABLE_TFFORMAT	"Y"	Ativa o formato do Terraform
ENABLE_TFCHECKOV	"Y"	Ativa varredura checkov
ENABLE_TFSEC	"Y"	Ativa varredura tfsec
TFSEC_VERSION	“v1.28.1"	Define a versão do tfsec

Mais padrões

- Acesse aplicativos de contêineres de forma privada no Amazon EKS usando a AWS PrivateLink e um Network Load Balancer
- Associe um AWS CodeCommit repositório em um Conta da AWS com o Amazon SageMaker AI Studio Classic em outra conta
- Automatize a criação de contas usando o Landing Zone Accelerator em AWS
- Automatizar a adição ou atualização de entradas de registro do Windows usando o AWS Systems Manager
- Automatize backups para instâncias de banco de dados do Amazon RDS para PostgreSQL usando o AWS Batch
- Automatize a implantação de aplicativos aninhados usando o AWS SAM
- Automatize a implantação do Manipulador do término do nó no Amazon EKS usando um pipeline de CI/CD
- Automatize a configuração RabbitMQ no Amazon MQ
- Automatize a replicação de instâncias do Amazon RDS em Contas da AWS
- Compilar e implantar automaticamente uma aplicação em Java no Amazon EKS usando um pipeline de CI/CD
- Gere automaticamente um modelo PyNamoDB e funções CRUD para o Amazon DynamoDB usando um aplicativo Python
- Valide e implante automaticamente políticas e funções do IAM em uma conta da AWS usando o CodePipeline IAM Access Analyzer e macros da AWS CloudFormation
- Faça backup dos servidores Sun SPARC no emulador Stromasys Charon-SSP na nuvem AWS
- Crie um pipeline de dados para ingerir, transformar e analisar dados do Google Analytics usando o AWS DataOps Development Kit
- Crie um PAC de servidor corporativo da Micro Focus com o Amazon EC2 Auto Scaling e o Systems Manager
- Crie um pipeline para imagens de contêiner reforçadas usando o EC2 Image Builder e o Terraform
- Crie um MLOps fluxo de trabalho usando o Amazon SageMaker AI e o Azure DevOps
- Centralize a resolução de DNS usando o Microsoft AWS Managed Microsoft AD Active Directory local
- Reúna os serviços da AWS usando uma abordagem de tecnologia sem servidor

- Limpe os recursos AWS do Account Factory for Terraform (AFT) com segurança após a perda do arquivo de estado
- Configure o registro em log para aplicativos.NET no Amazon CloudWatch Logs usando NLog
- Implemente continuamente um aplicativo web moderno do AWS Amplify a partir de um repositório da AWS CodeCommit
- Crie uma imagem de contêiner Docker personalizada SageMaker e use-a para treinamento de modelos no AWS Step Functions
- Crie um pipeline em regiões da AWS que não oferecem suporte à AWS CodePipeline
- Crie alarmes para métricas personalizadas usando a detecção de CloudWatch anomalias da Amazon
- Personalize os nomes das funções padrão usando AWS CDK aspectos e escotilhas de escape
- Implemente um pipeline que detecte simultaneamente problemas de segurança em vários produtos de código
- Implante e gerencie um data lake de tecnologia sem servidor na Nuvem AWS usando a infraestrutura como código
- Implante recursos e pacotes do Kubernetes usando o Amazon EKS e um repositório de charts do Helm no Amazon S3
- Implante aplicativos de várias pilhas usando o AWS CDK com TypeScript
- Implante instâncias de cluster de failover do SQL Server na Amazon EC2 e na Amazon FSx usando o Terraform
- Implemente as automações de segurança para a AWS WAF solução usando o Terraform
- Desenvolva assistentes avançados baseados em bate-papo com IA generativa usando RAG e prompting ReAct
- Habilite a Amazon GuardDuty condicionalmente usando modelos AWS CloudFormation
- Configure o escalonamento automático orientado por eventos no Amazon EKS usando o Amazon EKS Pod Identity e o KEDA
- Gere recomendações personalizadas e reclassificadas usando o Amazon Personalize
- Receber notificações do Amazon SNS quando o estado de chave de uma chave do AWS KMS mudar
- Identifique automaticamente imagens de contêineres duplicadas ao migrar para um repositório Amazon ECR
- Implemente o controle de versão de API baseado em caminhos usando domínios personalizados no Amazon API Gateway

- Melhore o desempenho operacional habilitando o Amazon DevOps Guru em várias regiões e contas da AWS e OUs com o AWS CDK
- Instale o agente SSM nos nós de trabalho do Amazon EKS usando o Kubernetes DaemonSet
- Integre o controlador universal Stonebranch com o AWS Mainframe Modernization
- Modernização do mainframe: DevOps iniciada AWS com o Rocket Software Enterprise Suite
- Gerencie conjuntos de AWS IAM Identity Center permissões como código usando AWS CodePipeline
- Gerencie aplicativos de contêineres on-premises configurando o Amazon ECS Anywhere com o AWS CDK
- Gerencie AWS Organizations políticas como código usando o AWS CodePipeline Amazon Bedrock
- Migre registros de DNS em massa para uma zona hospedada privada do Amazon Route 53
- Migre o ML Crie, treine e implante cargas de trabalho para a Amazon SageMaker usando as ferramentas do desenvolvedor da AWS
- Monitore o uso de uma Amazon Machine Image compartilhada em várias Contas da AWS
- Otimizar imagens do Docker geradas pelo AWS App2Container
- Orquestre um pipeline de ETL com validação, transformação e particionamento usando o AWS Step Functions
- Automatize implantações azul/verdes dos bancos de dados globais Amazon Aurora usando princípios de IaC
- Preserve o espaço IP roteável em projetos de VPC com várias contas para sub-redes sem workload
- Provisione um produto Terraform AWS Service Catalog usando um repositório de código
- Replique imagens filtradas de contêineres do Amazon ECR entre contas ou regiões
- Alternar as credenciais do banco de dados sem reiniciar os contêineres
- Execute tarefas do AWS Systems Manager Automation de forma síncrona a partir do AWS Step Functions
- Configure um pipeline de CI/CD para cargas de trabalho híbridas no Amazon ECS Anywhere usando o AWS CDK e GitLab
- Configure um pipeline de CI/CD para migração de banco de dados usando o Terraform
- Configure a infraestrutura Multi-AZ para um SQL Server Always On FCI usando a Amazon FSx
- Configure bots de UiPath RPA automaticamente na Amazon EC2 usando a AWS CloudFormation

- Simplifique a autenticação de aplicativos com TLS mútuo no Amazon ECS usando o Application Load Balancer
- Integração de locatários na arquitetura de SaaS para o modelo de silo usando C# e o AWS CDK
- Use o Terraform para habilitar automaticamente a Amazon GuardDuty para uma organização
- Use agentes do Amazon Bedrock para automatizar a criação de controles de entrada de acesso no Amazon EKS por meio de prompts baseados em texto
- Valide o código do Account Factory for Terraform (AFT) localmente
- Visualize os resultados do modelo de IA/ML usando o Flask e o AWS Elastic Beanstalk

Infraestrutura

Tópicos

- Acesse um bastion host usando o Session Manager e o Amazon EC2 Instance Connect
- Centralize a resolução de DNS usando o Microsoft AWS Managed Microsoft AD Active Directory local
- Centralize o monitoramento usando o Amazon CloudWatch Observability Access Manager
- Verifique as EC2 instâncias para ver as tags obrigatórias no lançamento
- Limpe os recursos AWS do Account Factory for Terraform (AFT) com segurança após a perda do arquivo de estado
- Conecte-se a uma EC2 instância da Amazon usando o Gerenciador de Sessões
- Crie um pipeline em regiões da AWS que não oferecem suporte à AWS CodePipeline
- Personalize os nomes das funções padrão usando AWS CDK aspectos e escotilhas de escape
- Implemente um cluster Cassandra na Amazon EC2 com estática privada IPs para evitar o reequilíbrio
- Estenda VRFs para a AWS usando o AWS Transit Gateway Connect
- Receber notificações do Amazon SNS quando o estado de chave de uma chave do AWS KMS mudar
- Preserve o espaço IP roteável em projetos de VPC com várias contas para sub-redes sem workload
- Provisione um produto Terraform AWS Service Catalog usando um repositório de código
- Registrar várias contas da AWS com um único endereço de e-mail usando o Amazon SES
- Configure a resolução de DNS para redes híbridas em um ambiente de conta única da AWS
- Configure bots de UiPath RPA automaticamente na Amazon EC2 usando a AWS CloudFormation
- Configure uma PeopleSoft arquitetura altamente disponível na AWS
- Configure a recuperação de desastres para o Oracle JD Edwards com o EnterpriseOne AWS Elastic Disaster Recovery
- Configure a detecção de AWS CloudFormation desvios em uma organização multirregional e com várias contas
- Importe com sucesso um bucket do S3 como uma pilha da AWS CloudFormation
- Sincronize dados entre sistemas de arquivos Amazon EFS em diferentes regiões da AWS usando a AWS DataSync

- Teste a AWS infraestrutura usando LocalStack e Terraform Tests
- Atualize os clusters do SAP Pacemaker de para ENSA1 ENSA2
- Use zonas de disponibilidade consistentes VPCs em diferentes contas da AWS
- Use o usuário IDs nas políticas do IAM para controle de acesso e automação
- Valide o código do Account Factory for Terraform (AFT) localmente
- Mais padrões

Acesse um bastion host usando o Session Manager e o Amazon EC2 Instance Connect

Criado por Piotr Chotkowski (AWS) e Witold Kowalik (AWS)

Resumo

Um bastion host, às vezes chamado de jump box, é um servidor que fornece um único ponto de acesso de uma rede externa aos recursos localizados em uma rede privada. Um servidor exposto a uma rede pública externa, como a Internet, representa um potencial risco de segurança para acesso não autorizado. É importante proteger e controlar o acesso a esses servidores.

Esse padrão descreve como você pode usar o Session Manager e o Amazon EC2 Instance Connect para se conectar com segurança a um host bastion do Amazon Elastic Compute Cloud (Amazon EC2) implantado em seu. Conta da AWS O Gerenciador de Sessões é um recurso de AWS Systems Manager. Os benefícios desse padrão incluem:

- O bastion host implantado não tem nenhuma porta de entrada aberta exposta à Internet pública. Isso reduz a superfície de ataque potencial.
- Você não precisa armazenar e manter chaves Secure Shell (SSH) de longo prazo no seu Conta da AWS. Em vez disso, cada usuário gera um novo par de chaves SSH sempre que se conecta ao bastion host. AWS Identity and Access Management As políticas (IAM) anexadas às AWS credenciais do usuário controlam o acesso ao bastion host.

Público-alvo

Esse padrão é destinado a leitores com experiência com conhecimento básico da Amazon EC2, Amazon Virtual Private Cloud (Amazon VPC) e Hashicorp Terraform.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- AWS Command Line Interface (AWS CLI) versão 2, instalada e configurada
- Plugin do Gerenciador de Sessões para o AWS CLI, instalado
- CLI do Terraform, instalado

- Armazenamento para o estado do Terraform, como um bucket do Amazon Simple Storage Service (Amazon S3) e uma tabela do Amazon DynamoDB que serve como backend remoto para armazenar o estado do Terraform. Para obter mais informações sobre o uso de back-ends remotos para o estado do Terraform, consulte Amazon S3 Backends (documentação do Terraform). Para uma amostra de código que configura o gerenciamento remoto do estado com um back-end do Amazon S3, consulte remote-state-s3-back-end (Terraform Registry). Observe os seguintes requisitos:
  - O bucket do Amazon S3 e a tabela do DynamoDB devem estar no mesmo lugar. Região da AWS
  - Ao criar a tabela do DynamoDB, a chave de partição deve ser `LockID` (com distinção entre maiúsculas e minúsculas) e o tipo de chave de partição deve ser `String`. Todas as outras configurações devem estar em seus valores predefinidos. Para obter mais informações, consulte Sobre chaves primárias e Criar uma tabela na documentação do DynamoDB.
- Um SSH cliente, instalado

Limitações

- Esse padrão serve como uma prova de conceito (PoC) ou como base para um maior desenvolvimento. Ele não deve ser usado na sua forma atual em ambientes de produção. Antes da implantação, ajuste o código de amostra no repositório para atender aos seus requisitos e ao seu caso de uso.
- Esse padrão pressupõe que o bastion host de destino usa o Amazon Linux 2 como seu sistema operacional. Embora seja possível usar outras Amazon Machine Images (AMIs), outros sistemas operacionais estão fora do escopo desse padrão.

> **Note**
>
> O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs.

- Nesse padrão, o bastion host está localizado em uma sub-rede privada sem um gateway NAT e um gateway da internet. Esse design isola a EC2 instância da Amazon da Internet pública. Você pode adicionar uma configuração de rede específica que permita a comunicação com a internet. Para obter mais informações, consulte Conectar sua VPC a outras redes na documentação do Amazon VPC. Da mesma forma, seguindo o princípio do privilégio mínimo, o host bastion não tem acesso a nenhum outro recurso em seu, a Conta da AWS menos que você conceda

permissões explicitamente. Para obter mais informações, consulte Políticas baseadas em recurso na documentação do IAM.

Versões do produto

- AWS CLI versão 2
- Terraform versão 1.3.9

Arquitetura

Pilha de tecnologias de destino

- Uma VPC com uma única sub-rede privada.
- Os seguintes endpoints da VPC de interface:
  - `amazonaws.<region>.ssm`— O endpoint do AWS Systems Manager serviço.
  - `amazonaws.<region>.ec2messages`: o Systems Manager usa esse endpoint para fazer chamadas do SSM Agent para o serviço do Systems Manager.
  - `amazonaws.<region>.ssmmessages`— O Session Manager usa esse endpoint para se conectar à sua EC2 instância Amazon por meio de um canal de dados seguro.
- Uma EC2 instância `t3.nano` da Amazon executando o Amazon Linux 2
- Perfil do IAM de perfil de instância
- Grupos de segurança da Amazon VPC e regras de grupos de segurança para os endpoints e a instância da Amazon EC2

Arquitetura de destino

O diagrama mostra o seguinte processo:

1. O usuário assume um perfil do IAM que tem permissões para fazer o seguinte:
   - Autentique, autorize e conecte-se à instância da Amazon EC2
   - Iniciar a sessão com o Session Manager
2. O usuário inicia uma sessão SSH por meio do Session Manager.

3. O Session Manager autentica o usuário, verifica as permissões nas políticas do IAM associadas, verifica as configurações e envia uma mensagem ao SSM Agent para abrir uma conexão bidirecional.
4. O usuário envia a chave pública SSH para o Bastion Host por meio de metadados da Amazon. EC2 Isso deve ser feito antes de cada conexão. A chave pública SSH permanece disponível por 60 segundos.
5. O bastion host se comunica com os endpoints VPC da interface para Systems Manager e Amazon. EC2
6. O usuário acessa o bastion host por meio do Session Manager usando um canal de comunicação bidirecional criptografado TLS 1.2.

Automação e escala

As opções a seguir estão disponíveis para automatizar a implantação ou escalar essa arquitetura:

- Você pode implantar a arquitetura por meio de um pipeline de integração contínua e entrega contínua (CI/CD).
- Você pode modificar o código para alterar o tipo de instância do bastion host.
- Você pode modificar o código para implantar vários bastion hosts. No arquivo `bastion-host/main.tf`, no bloco de recursos `aws_instance`, adicione o meta-argumento `count`. Para obter mais informações, consulte a documentação do Terraform.

Ferramentas

Serviços da AWS

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com

segurança em grande escala. Esse padrão usa o Session Manager, um atributo do Systems Manager.

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Outras ferramentas

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem. Esse padrão usa o Terraform CLI.

Repositório de código

O código desse padrão está disponível no GitHub Access a bastion host usando o Session Manager e o repositório Amazon EC2 Instance Connect.

Práticas recomendadas

- Recomendamos o uso de ferramentas automatizadas de verificação de código para melhorar a segurança e a qualidade do código. Esse padrão foi verificado usando o Checkov, uma ferramenta estática de análise de código para IaC. No mínimo, recomendamos que você execute verificações básicas de validação e formatação usando os comandos `terraform validate` e `terraform fmt -check -recursive` do Terraform.
- É uma boa prática adicionar testes automatizados para IaC. Para obter mais informações sobre as diferentes abordagens para testar o código do Terraform, consulte Testando o HashiCorp Terraform (postagem no blog do Terraform).
- Durante a implantação, o Terraform usa a EC2 instância substitutiva da Amazon sempre que uma nova versão do Amazon Linux 2 AMI é detectada. Isso implanta a nova versão do sistema operacional, incluindo patches e atualizações. Se a programação de implantação não for frequente, isso pode representar um risco de segurança porque a instância não tem os patches mais recentes. É importante atualizar e aplicar patches de segurança com frequência às EC2 instâncias implantadas da Amazon. Para obter mais informações, consulte Gerenciamento de atualizações na Amazon EC2.
- Como esse padrão é uma prova de conceito, ele usa políticas AWS gerenciadas, como`AmazonSSMManagedInstanceCore`. AWS as políticas gerenciadas abrangem casos

de uso comuns, mas não concedem permissões de privilégios mínimos. Conforme necessário para seu caso de uso, recomendamos que você crie políticas personalizadas que concedam permissões de privilégio mínimo para os recursos implantados nessa arquitetura. Para obter mais informações, consulte Comece a usar políticas AWS gerenciadas e adote as permissões de privilégios mínimos.

- Use uma senha para proteger o acesso às chaves SSH e armazenar as chaves em um local seguro.
- Configure o registro em log e o monitoramento do bastion host. O registro em log e o monitoramento são partes importantes da manutenção de sistemas, tanto do ponto de vista operacional quanto de segurança. Há várias maneiras de monitorar conexões e atividades em seu bastion host. Para obter mais informações, consulte os tópicos a seguir na documentação do Systems Manager.
  - Monitoramento AWS Systems Manager
  - Registro e monitoramento em AWS Systems Manager
  - Auditar a atividade da sessão
  - Registrar a atividade de sessão de registro em log

Épicos

Implantar os recursos

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de códigos.	1. Em uma interface da linha de comando, altere seu diretório de trabalho para o local em que você deseja armazenar os arquivos de amostra. 2. Insira o comando da a seguir. `git clone https://github.com/aws-samples/secured-bastio`	DevOps engenheiro, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`n-host-terraform.git`	

Tarefa	Descrição	Habilidades necessárias
Iniciar o diretório de trabalho do Terraform.	Essa etapa é necessária somente para a primeira implantação. Se você estiver reimplantando o padrão, pule para a próxima etapa. No diretório raiz do repositór io clonado, insira o seguinte comando, onde: • `$S3_STATE_BUCKET` é o nome do bucket Amazon S3 que contém o estado do Terraform • `$PATH_TO_STATE_FILE` é a chave para o arquivo de estado do Terraform, como `infra/bastion-host/tetfstate` • `$AWS_REGION` é a região em que o bucket do Amazon S3 é implantado `terraform init \ -backend-config="bucket=$S3_STATE_BUCKET" \ -backend-config="key=$PATH_TO_STATE_FILE" \ -backend-config="region=$AWS_REGION`	DevOps engenheiro, desenvolvedor, Terraform

Tarefa	Descrição	Habilidades necessárias
	Note Como alternativa, você pode abrir o arquivo config.tf e, na `terraform` seção, fornecer manualmente esses valores.	
Implantar os recursos	1. No diretório raiz do repositório clonado, insira o seguinte comando: `terraform apply -var-file="dev.tfvars"` 2. Revise a lista de todas as alterações que serão aplicadas à sua Conta da AWS e confirme a implantação. 3. Espere até que todos os recursos sejam implantados.	DevOps engenheiro, desenvolvedor, Terraform

Configurar o ambiente local

Tarefa	Descrição	Habilidades necessárias
Configure a conexão do SSH.	Atualize o arquivo de configuração do SSH para permitir conexões do SSH através do Session Manager. Para obter instruções,	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	consulte Permitir conexões do SSH para o Session Manager. Isso permite que usuários autorizados insiram um comando proxy que inicia uma sessão do Session Manager e transfere todos os dados por meio de uma conexão bidirecional.	
Gerar as chaves SSH.	Insira o seguinte comando para gerar um par de chaves SSH privadas e públicas locais. Use esse par de chaves para se conectar ao bastion host. `ssh-keygen -t rsa -f my_key`	DevOps engenheiro, Desenvolvedor

Conecte-se ao bastion host usando o Session Manager

Tarefa	Descrição	Habilidades necessárias
Obtenha o ID da instância.	1. Para se conectar ao host bastion implantado, você precisa do ID da instância da Amazon EC2 . Faça um dos seguintes procedimentos para localizar o ID: • Abra o EC2 console da Amazon. No painel de navegação, escolha	AWS geral

Tarefa	Descrição	Habilidades necessárias

	Instâncias. Localize a instância do bastion host.
	• No AWS CLI, insira o seguinte comando.
	`aws ec2 describe-instances`
	Para filtrar os resultados, digite o comando a seguir, onde `$BASTION_HOST_TAG` é a tag que você atribuiu ao bastion host. O valor padrão desta etiqueta é `sandbox-dev-bastion-host`.
	`aws ec2 describe-instances \ --filters "Name=tag:Name,Values=$BASTION_HOST_TAG" \ --output text \ --query 'Reservations[*].Instances[*].InstanceId' \ --output text`
	2. Copie o ID da EC2 instância da Amazon. Você usará esse ID posteriormente.	

Tarefa	Descrição	Habilidades necessárias
Enviar a chave pública SSH.	**Note** Nesta seção, você carrega a chave pública para os metadados da instância do bastion host. Depois que a chave for carregada, você terá 60 segundos para iniciar uma conexão com o bastion host. Após 60 segundos, a chave pública é removida. Para obter mais informações, consulte a seção Solução de problemas desse padrão. Conclua as próximas etapas rapidamente para evitar que a chave seja removida antes de se conectar ao bastion host. 1. Envie a chave SSH para o Bastion Host usando o Amazon Instance EC2 Connect. Digite o comando a seguir, em que:	AWS geral

Tarefa	Descrição	Habilidades necessárias
	• `$INSTANCE_ID` é o ID da EC2 instância da Amazon • `$PUBLIC_KEY_FILE` é o caminho para seu arquivo de chave pública, como `my_key.pub` **Important** Certifique-se de usar a chave pública e não a chave privada. `aws ec2-instance-connect send-ssh-public-key \ --instance-id $INSTANCE_ID \ --instance-os-user ec2-user \ --ssh-public-key file://$PUBLIC_KEY_FILE` 2. Espere até receber uma mensagem indicando que a chave foi carregada com sucesso. Avance para a próxima etapa imediatamente.	

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao bastion host.	1. Insira o comando a seguir para se conectar ao bastion host por meio do Session Manager, onde: • `$PRIVATE_KEY_FILE` é o caminho para sua chave privada, como `my_key` • `$INSTANCE_ID` é o ID da EC2 instância da Amazon `ssh -i $PRIVATE_KEY_FILE ec2-user@$INSTANCE_ID` 2. Confirme a conexão inserindo `yes`. Isso abre uma conexão SSH usando o Session Manager. **Note** Existem outras opções para abrir uma conexão SSH com o host bastion. Para obter mais informações, consulte Abordagens alternativas para estabelecer uma conexão SSH com o bastion host na seção Informaçõ	AWS geral

Tarefa	Descrição	Habilidades necessárias
	es adicionais desse padrão.	

Limpar (opcional)

Tarefa	Descrição	Habilidades necessárias
Remova os recursos implantados.	1. Para remover todos os recursos implantados, execute o comando a seguir a partir do diretório raiz do repositório clonado. `terraform destroy -var-file="dev.tfvars"` 2. Confirme a remoção dos recursos.	DevOps engenheiro, desenvolvedor, Terraform

Solução de problemas

Problema	Solução
erro `TargetNotConnected` ao tentar se conectar ao bastion host	1. Reinicie o bastion host de acordo com as instruções em Reinicie sua instância na documentação da Amazon. EC2 2. Depois que a instância for reinicializada com sucesso, reenvie a chave pública para o bastion host e tente a conexão novamente.
erro `Permission denied` ao tentar se conectar ao bastion host	Depois que a chave for carregada aos bastion host, você terá 60 segundos para iniciar a conexão. Depois de 60 segundos, a chave é

Problema	Solução
	removida automaticamente e você não pode usá-la para se conectar à instância. Se isso ocorrer, você poderá repetir a etapa para reenviar a chave para a instância.

Recursos relacionados

AWS documentação

- AWS Systems Manager Session Manager(Documentação do Systems Manager)
- Instale o plug-in do Session Manager para o AWS CLI (documentação do Systems Manager)
- Permitindo conexões SSH para o Session Manager (documentação do Systems Manager)
- Sobre o uso do EC2 Instance Connect (EC2 documentação da Amazon)
- Conecte-se usando o EC2 Instance Connect (EC2 documentação da Amazon)
- Gerenciamento de identidade e acesso para a Amazon EC2 (EC2 documentação da Amazon)
- Usando uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon (documentação do IAM)
- Práticas recomendadas de segurança no IAM (documentação do IAM)
- Controlar o tráfego para recursos usando grupos de segurança (documentação da Amazon VPC)

Outros recursos

- Página da web do Desenvolvedor do Terraform
- Comando: validar (documentação do Terraform)
- Comando: fmt (documentação do Terraform)
- Testando o HashiCorp Terraform (postagem HashiCorp no blog)
- Página da Web de Checkov

Mais informações

Abordagens alternativas para estabelecer uma conexão SSH com o bastion host

Encaminhamento de portas

Você pode usar a opção `-D 8888` para abrir uma conexão SSH com encaminhamento dinâmico de portas. Para obter mais informações, consulte as instruções em explainshell.com. Veja a seguir um exemplo de um comando para abrir uma conexão SSH usando o encaminhamento de porta.

```
ssh -i $PRIVATE_KEY_FILE -D 8888 ec2-user@$INSTANCE_ID
```

Esse tipo de conexão abre um proxy SOCKS que pode encaminhar o tráfego do seu navegador local por meio do bastion host. Se você estiver usando Linux ou macOS, insira `man ssh` para ver todas as opções. Isso exibe o manual de referência do SSH.

Usando o script fornecido

Em vez de executar manualmente as etapas descritas em Conecte-se ao bastion host usando o Session Manager na seção Épicos, você pode usar o script connect.sh incluído no repositório de código. Esse script gera o par de chaves SSH, envia a chave pública para a EC2 instância da Amazon e inicia uma conexão com o host bastion. Ao executar o script, você passa a tag e o nome da chave como argumentos. Veja a seguir um exemplo do comando para executar o script.

```
./connect.sh sandbox-dev-bastion-host my_key
```

Centralize a resolução de DNS usando o Microsoft AWS Managed Microsoft AD Active Directory local

Criado por Brian Westmoreland (AWS)

Resumo

Esse padrão fornece orientação para centralizar a resolução de DNS em um ambiente de AWS várias contas usando AWS Directory Service for Microsoft Active Directory ()AWS Managed Microsoft AD e o Amazon Route 53. Nesse padrão, o namespace AWS DNS é um subdomínio do namespace DNS local. Esse padrão também fornece orientação sobre como configurar os servidores DNS locais para encaminhar consultas para AWS quando a solução de DNS local usa o Microsoft Active Directory.

Pré-requisitos e limitações

Pré-requisitos

- Um ambiente de AWS várias contas configurado usando AWS Organizations.
- Conectividade de rede estabelecida entre Contas da AWS.
- Conectividade de rede estabelecida entre AWS e o ambiente local (usando AWS Direct Connect ou qualquer tipo de conexão VPN).
- AWS Command Line Interface (AWS CLI) configurado em uma estação de trabalho local.
- AWS Resource Access Manager (AWS RAM) usado para compartilhar regras do Route 53 entre contas. Portanto, o compartilhamento deve ser ativado dentro do AWS Organizations ambiente, conforme descrito na seção Epics.

Limitações

- AWS Managed Microsoft AD A Edição Standard tem um limite de 5 compartilhamentos.
- AWS Managed Microsoft AD A Enterprise Edition tem um limite de 125 ações.
- A solução nesse padrão é limitada ao compartilhamento Regiões da AWS desse suporte AWS RAM.

Versões do produto

- Microsoft Active Directory em execução no Windows Server 2008, 2012, 2012 R2 ou 2016.

Arquitetura

Arquitetura de destino

Neste design, AWS Managed Microsoft AD é instalado nos serviços compartilhados Conta da AWS. Embora não seja um requisito, esse padrão pressupõe essa configuração. Se você configurar de AWS Managed Microsoft AD forma diferente Conta da AWS, talvez seja necessário modificar as etapas na seção Epics adequadamente.

Esse design usa resolvedores do Route 53 para oferecer suporte à resolução de nomes por meio do uso das regras do Route 53. Se a solução de DNS on-premises usa o Microsoft DNS, criar uma regra de encaminhamento condicional para o namespace da AWS (`aws.company.com`), que é um subdomínio do namespace do DNS da empresa (`company.com`), não é simples. Se você tentar criar um encaminhador condicional tradicional, isso resultará em um erro. Isso ocorre porque o Microsoft Active Directory já é considerado autoritário para qualquer subdomínio do `company.com`. Para contornar esse erro, primeiro você deve criar uma delegação para que `aws.company.com` delegue a autoridade desse namespace. Em seguida, você pode criar o encaminhador condicional.

A nuvem privada virtual (VPC) de cada conta spoke pode ter seu próprio namespace DNS exclusivo com base no namespace raiz. AWS Nesse design, cada conta spoke acrescenta uma abreviatura do nome da conta ao namespace base da AWS. Depois que as zonas hospedadas privadas na conta spoke forem criadas, elas serão associadas à VPC local na conta spoke, bem como à VPC na conta da rede central. AWS Isso permite que a conta da AWS rede central responda às consultas de DNS relacionadas às contas spoke. Dessa forma, tanto o Route 53 quanto o Route 53 AWS Managed Microsoft AD trabalham juntos para compartilhar a responsabilidade de gerenciar o AWS namespace ()`aws.company.com`.

Automação e escala

Esse design usa os endpoints do Route 53 Resolver para escalar as consultas de DNS entre AWS e seu ambiente local. Cada endpoint do Route 53 Resolver compreende várias interfaces de rede elástica (espalhadas por várias zonas de disponibilidade), e cada interface de rede pode lidar com até 10.000 consultas por segundo. O Route 53 Resolver suporta até 6 endereços IP por endpoint, então, no total, esse design suporta até 60.000 consultas ao DNS por segundo espalhadas por várias zonas de disponibilidade para alta disponibilidade.

Além disso, esse padrão é automaticamente responsável pelo crescimento futuro interno AWS. As regras de encaminhamento de DNS configuradas no local não precisam ser modificadas para oferecer suporte às zonas hospedadas privadas novas VPCs e associadas que são adicionadas. AWS

Ferramentas

Serviços da AWS

- AWS Directory Service for Microsoft Active Directorypermite que suas cargas de trabalho e AWS recursos com reconhecimento de diretório usem o Microsoft Active Directory no. Nuvem AWS
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar seus recursos com segurança Contas da AWS para reduzir a sobrecarga operacional e fornecer visibilidade e auditabilidade.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.

Ferramentas

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando. Nesse padrão, o AWS CLI é usado para configurar as autorizações do Route 53.

Épicos

Crie e compartilhe um AWS Managed Microsoft AD diretório

Tarefa	Descrição	Habilidades necessárias
Implantar AWS Managed Microsoft AD.	1. Crie e configure um novo diretório. Para obter etapas detalhadas, consulte Criando seu AWS Managed Microsoft AD no Guia de AWS Directory Service Administração.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	2. Registre os endereços IP dos controladores de AWS Managed Microsoft AD domínio. Eles serão referenciados em uma etapa posterior.	
Compartilhar o diretório.	Depois que o diretório for criado, compartilhe-o com outras Contas da AWS pessoas na AWS organizaç ão. Para obter instruções, consulte Compartilhar seu diretório no Guia de AWS Directory Service Administr ação. **Note** AWS Managed Microsoft AD A Edição Standard tem um limite de 5 compartil hamentos. A Enterpris e Edition tem um limite de 125 ações.	Administrador da AWS

Configure o Route 53

Tarefa	Descrição	Habilidades necessárias
Crie resolvedores do Route 53.	Os resolvedores do Route 53 facilitam a resolução de	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	consultas de DNS entre AWS e o data center local. 1. Instale os resolvedores do Route 53 seguindo as instruções no Guia do desenvolvedor do Route 53. 2. Configure os resolvedores do Route 53 em sub-redes privadas em pelo menos duas zonas de disponibilidade na AWS conta de rede central VPC para alta disponibilidade. **Note** Embora o uso da conta AWS de rede central VPC não seja obrigatório, as etapas restantes pressupõem essa configuração.	

Tarefa	Descrição	Habilidades necessárias

Crie regras do Route 53.	Seu caso de uso específico pode exigir um grande número de regras do Route 53, mas você precisará configurar as seguintes regras como linha de base:
	• Uma regra de saída para o namespace local (`company.com`) usando os resolvedores de saída do Route 53 da conta de rede central. Os endereços IP de destino são os servidores DNS locais.
	  • Associe essa regra à conta de rede central VPC.
	• Uma regra de saída para o AWS namespace (`aws.company.com`) usando os resolvedores de saída do Route 53 da conta de rede central. Os endereços IP de destino são os endereços IP do Route 53 Resolver de entrada da conta de rede central.
	  • Não associe essa regra à conta de AWS rede central VPC (que abriga os resolvedores do Route 53).
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	• Uma segunda regra de saída para o AWS namespace (`aws.company.com`) que aponta para os controladores de AWS Managed Microsoft AD domínio (use a IPs do épico anterior).
	  • Associe essa regra à conta de AWS rede central VPC (que abriga os resolvedores do Route 53).
	  • Não compartilhe nem associe essa regra a outras Contas da AWS.
	
	Para obter mais informações, consulte Gerenciar regras de encaminhamento no Guia do desenvolvedor do Route 53.	

Tarefa	Descrição	Habilidades necessárias
Configurar um perfil do Route 53.	Um perfil do Route 53 é usado para compartilhar as regras com contas spoke. 1. Crie um novo perfil do Route 53 na conta de rede central seguindo as instruções no Guia do desenvolvedor do Route 53. 2. Adicione a regra para o namespace local (`company.com`) ao Perfil. 3. Adicione a primeira regra para o AWS namespace (`aws.company.com`), que tem como alvo os endereços IP dos resolvedores de entrada do Route 53, ao Perfil. 4. Compartilhe o perfil do Route 53 com a AWS organização. 5. Aceite o compartilhamento de recursos do Perfil do Route 53 em cada conta spoke. 6. Associe o perfil do Route 53 a cada VPC da conta spoke.	Administrador da AWS

Configurar o DNS do Active Directory on-premises

Tarefa	Descrição	Habilidades necessárias
Crie a delegação.	Use o snap-in do Microsoft DNS (`dnsmgmt.msc`) para criar uma nova delegação para o namespace `company.com` no Active Directory. O nome do domínio delegado deve ser `aws`. Isso torna o nome de domínio totalmente qualificado (FQDN) da delegação `aws.company.com`. Use os endereços IP dos controladores de AWS Managed Microsoft AD domínio para os valores IP do servidor de nomes e use `server.aws.company.com` para o nome. (Essa delegação serve apenas para redundância, porque um encaminhador condicional será criado para esse namespace que tem precedência sobre a delegação.)	Active Directory
Crie o encaminhador condicional.	Use o snap-in do Microsoft DNS (`dnsmgmt.msc`) para criar um novo encaminhador condicional para `aws.company.com`. Use os endereços IP dos resolvedores de AWS entrada do Route 53 no DNS central Conta da AWS para	Active Directory

Tarefa	Descrição	Habilidades necessárias
	o destino do encaminhador condicional.	

Crie zonas hospedadas privadas do Route 53 para spoke Contas da AWS

Tarefa	Descrição	Habilidades necessárias
Crie as zonas hospedadas privadas do Route 53.	Crie uma zona hospedada privada do Route 53 em cada conta spoke. Associe essa zona hospedada privada à conta spoke VPC. Para obter etapas detalhadas, consulte Criação de uma zona hospedada privada no Guia do desenvolvedor do Route 53.	Administrador da AWS
Crie autorizações.	Use o AWS CLI para criar uma autorização para a conta de AWS rede central VPC. Execute este comando a partir do contexto de cada fala Conta da AWS: `aws route53 create-vpc-association-authorization --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>` em que:	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	• <hosted-zone-id> é a zona hospedada privada do Route 53 na conta spoke. • <region>e <vpc-id> são o ID da VPC Região da AWS e a VPC da conta de AWS rede central VPC.	
Criar associações.	Crie a associação de zona hospedada privada do Route 53 para a conta de AWS rede central VPC usando o. AWS CLI Execute este comando a partir do contexto da conta de AWS rede central: `aws route53 associate -vpc-with-hosted-z one --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion =<region>,VPCId=<vpc-id>` em que: • <hosted-zone-id> é a zona hospedada privada do Route 53 na conta spoke. • <region>e <vpc-id> são o Região da AWS ID da VPC da conta da AWS rede central.	Administrador da AWS

Recursos relacionados

- Simplifique o gerenciamento de DNS em um ambiente de várias contas com o Route 53 Resolver (AWS postagem no blog)
- Criando sua AWS Managed Microsoft AD (AWS Directory Service documentação)
- Compartilhamento de um AWS Managed Microsoft AD diretório (AWS Directory Service documentação)
- O que Amazon Route 53 Resolveré (Documentação do Amazon Route 53)
- Criação de uma zona hospedada privada (documentação do Amazon Route 53)
- O que são perfis do Amazon Route 53? (Documentação do Amazon Route 53)

Centralize o monitoramento usando o Amazon CloudWatch Observability Access Manager

Criado por Anand Krishna Varanasi (AWS), Jimmy Morgan (AWS), Ashish Kumar (AWS), Balaji Vedagiri (AWS), JAGDISH KOMAKULA (AWS), Sarat Chandra Pothula (AWS) e Vivek Thangamuthu (AWS)

Resumo

A observabilidade é crucial para monitorar, entender e solucionar problemas de aplicativos. Aplicativos que abrangem várias contas, como implementações de landing zone AWS Control Tower ou landing zone, geram um grande número de registros e rastreiam dados. Para solucionar problemas rapidamente ou entender a análise de usuários ou a análise de negócios, você precisa de uma plataforma de observabilidade comum em todas as contas. O Amazon CloudWatch Observability Access Manager oferece acesso e controle sobre vários registros de contas a partir de um local central.

Você pode usar o Gerente de Acesso à Observabilidade para visualizar e gerenciar registros de dados de observabilidade gerados pelas contas de origem. As contas de origem são individuais Contas da AWS que geram dados de observabilidade para seus recursos. Os dados de observabilidade são compartilhados entre contas de origem e as de monitoramento. Os dados de observabilidade compartilhados podem incluir métricas na Amazon CloudWatch, registros no Amazon CloudWatch Logs e rastreamentos. AWS X-Ray Para obter mais informações, consulte Referência de API do Gerente de Acesso à Observabilidade.

Esse padrão é para usuários que têm aplicativos ou infraestrutura executados em vários Contas da AWS e precisam de um local comum para visualizar os registros. Ele explica como você pode configurar o Gerente de Acesso à Observabilidade usando o Terraform para monitorar o status e a integridade desses aplicativos ou infraestrutura. Você pode instalar essa solução de várias maneiras:

- Como um módulo autônomo do Terraform que você configura manualmente
- Usando um pipeline de integração contínua e entrega contínua (CI/CD)
- Ao se integrar com outras soluções, como AWS Control Tower Account Factory for Terraform (AFT)

As instruções na seção Épicos abrangem a implementação manual. Para as etapas de instalação do AFT, consulte o arquivo README do repositório do GitHub Observability Access Manager.

Pré-requisitos e limitações

Pré-requisitos

- O Terraform instalado ou referenciado em seu sistema ou em tubulações automatizadas. (É recomendável usar a versão mais recente.)
- Uma conta que você pode usar como uma conta de monitoramento central. Outras contas criam links para a conta de monitoramento central para visualizar os logs.
- (Opcional) Um repositório de código-fonte GitHub, como AWS CodeCommit, Atlassian Bitbucket ou sistema similar. Um repositório de código-fonte não é necessário se você estiver usando pipelines automatizados de CI/CD.
- (Opcional) Permissões para criar pull requests (PRs) para revisão de código e colaboração de código em GitHub.

Limitações

O Gerente de Acesso à Observabilidade tem as seguintes Service Quotas, que não podem ser alteradas. Considere essas cotas antes de implantar esse atributo. Para obter mais informações, consulte as cotas de CloudWatch serviço na CloudWatch documentação.

- Links da conta de origem: você pode vincular cada conta de origem a no máximo cinco contas de monitoramento.
- Coletores: você pode criar vários coletores para uma conta, mas somente um coletor por conta Região da AWS é permitido.

Além disso:

- Os coletores e links devem ser criados da mesma forma Região da AWS; eles não podem ser interregionais.

Monitoramento entre regiões e contas

Para o monitoramento entre regiões e entre contas, você pode escolher uma das seguintes opções:

- Crie CloudWatch painéis entre contas e regiões para alarmes e métricas. Essa opção não é compatível com registros e rastreamentos.
- Implemente o registro centralizado usando o Amazon OpenSearch Service.

- Crie um coletor por região a partir de todas as contas de locatários, envie métricas para uma conta de monitoramento centralizada (conforme descrito neste padrão) e, em seguida, use fluxos de CloudWatch métricas para enviar os dados para um destino externo comum ou para produtos de monitoramento de terceiros, como Datadog, Dynatrace, Sumo Logic, Splunk ou New Relic.

Arquitetura

Componentes

CloudWatch O Observability Access Manager consiste em dois componentes principais que permitem a observabilidade entre contas:

- Um coletor permite que as contas de origem enviem dados de observabilidade para a conta de monitoramento central. Basicamente, um coletor fornece uma junção de gateway para as contas de origem se conectarem. Só pode haver um gateway ou conexão de coletor, e várias contas podem se conectar a ele.
- Cada conta de origem tem um link para a junção do gateway do coletor e os dados de observabilidade são enviados por meio desse link. Você deve criar um coletor antes de criar links de cada conta de origem.

Arquitetura

O diagrama a seguir ilustra o Gerente de Acesso à Observabilidade e seus componentes.

Ferramentas

Serviços da AWS

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.

Ferramentas

- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.
- AWS Control Tower O Account Factory for Terraform (AFT) configura um pipeline do Terraform para ajudá-lo a provisionar e personalizar contas em. AWS Control Tower Opcionalmente, você pode usar o AFT para configurar o Gerente de Acesso à Observabilidade em escala em várias contas.

Repositório de código

O código desse padrão está disponível no repositório do GitHub Observability Access Manager.

Práticas recomendadas

- Em AWS Control Tower ambientes, marque a conta de registro como a conta de monitoramento central (coletor).
- Se você tiver várias organizações com várias contas AWS Organizations, recomendamos que você inclua as organizações em vez de contas individuais na política de configuração. Se você tiver um pequeno número de contas ou se as contas não fizerem parte de uma organização na política de configuração do coletor, você pode optar por incluir contas individuais.

Épicos

Configure o módulo coletor

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Clone o repositório do GitHub Observability Access Manager: `git clone https://github.com/aws-samples/cloudwatch-observability-access-manager-terraform`	AWS DevOps, administrador da nuvem, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Especifique os valores das propriedades para o módulo coletor.	No arquivo `main.tf` (na pasta `deployments/aft-account-customizations/LOGGING/terraform/` do repositório), especifique valores para as seguintes propriedades: • `sink_name` : O nome da CloudWatch pia. • `allowed_oam_resource_types` : O Observability Access Manager atualmente oferece suporte a CloudWatch métricas, grupos de registros e AWS X-Ray rastreamentos. • `allowed_source_accounts` : as contas de origem que têm permissão para enviar registros para a conta do CloudWatch coletor central. • `allowed_source_organizations` : as AWS Control Tower organizações de origem que têm permissão para enviar registros para a conta do CloudWatch coletor central. Para obter mais informações, consulte AWS::Oam:	AWS DevOps, administrador da nuvem, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	:Sinka AWS CloudFormation documentação.	

Instale o módulo sink.	Exporte as credenciais da Conta da AWS que você selecionou como conta de monitoramento e instale o módulo coletor do Observabi lity Access Manager:
	`Terraform Init`
	`Terrafom Plan`
	`Terraform Apply`
		AWS DevOps, administrador da nuvem, administrador da AWS

Configure o módulo do coletor

Tarefa	Descrição	Habilidades necessárias

Especifique os valores da propriedade para o módulo de link.	No arquivo `main.tf` (na pasta `deployments/aft-account-customizations/LOGGING/terraform/` do repositório), especifiq ue valores para as seguintes propriedades:
	• `account_label` : use um dos seguintes valores:
	  • `$AccountName` : o nome da conta.
	  • `$AccountEmail` : um endereço de e-mail globalmente exclusivo , que inclui o domínio
		AWS DevOps, administrador de nuvem, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	de e-mail (por exemplo, `hello@example.com`) • `$AccountEmailNoDomain` : um endereço de e-mail sem o nome de domínio. • `allowed_oam_resource_types` : O Observability Access Manager atualmente oferece suporte a CloudWatch métricas, grupos de registros e AWS X-Ray rastreamentos. Para obter mais informações, consulte AWS::Oam::Link a AWS CloudFormation documentação.	

Instale o módulo de link para contas individuais.	Exporte as credenciais de contas individuais e instale o módulo de link do Gerente de Acesso à Observabilidade:
	
	`Terraform Plan`
	`Terraform Apply`
	
	Você pode configurar o módulo do link individualmente para cada conta ou usar o AFT para instalar automaticamente esse módulo em várias contas.
		AWS DevOps, administrador de nuvem, arquiteto de nuvem

Aprovar conexões sink-to-link

Tarefa	Descrição	Habilidades necessárias
Verificar a mensagem de status.	1. Faça login na conta de monitoramento. 2. Abra o console de CloudWatch . 3. No painel de navegação à esquerda, escolha Configurações. À direita, você deve ver a mensagem de status Conta de monitoramento habilitada com uma marca de seleção verde. Isso significa que a conta de monitoramento tem um coletor do Gerente de Acesso à Observabilidade ao qual os links de outras contas se conectarão.	
Aprove as link-to-sink conexões.	1. Escolha a opção Recursos para vincular contas abaixo da mensagem de status. As informações confirmam que essa é a conta de monitoramento, listam os dados compartilhados das contas de origem do inquilino (registros, métricas, rastreamentos) e mostram o rótulo da conta como $. AccountName	AWS DevOps, administrador de nuvem, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Essa tela fornece duas opções para vincular contas de inquilino à conta de monitoramento: aprovação em nível de organização ou aprovação em nível de conta. Para cada opção, você pode escolher baixar um AWS CloudFormation modelo para aprovação ou aprovar cada conta individualmente. 2. Para simplificar, escolha Qualquer conta para aprovar em cada nível de conta. Essa opção fornece um link de aprovação para a conta. 3. Escolha Copiar URL para copiar o link. 4. Faça login em cada conta de origem. 5. Em uma janela do navegador, cole o link e escolha Aprovar link para conectar ao coletor. 6. Repita o procedimento para contas de origem adicionais. Para obter mais informações, consulte Vincular contas de monitoramento com contas	

Tarefa	Descrição	Habilidades necessárias
	de origem na CloudWatch documentação.	

Verifique os dados de observabilidade entre contas

Tarefa	Descrição	Habilidades necessárias
Visualize dados entre contas.	1. Faça login na conta central de monitoramento. 2. Abra o console de CloudWatch . 3. No painel de navegação à esquerda, escolha as opções para visualizar logs, métricas e rastreamentos entre contas.	AWS DevOps, administrador de nuvem, arquiteto de nuvem

(Opcional) Permita que as contas de origem confiem na conta de monitoramento

Tarefa	Descrição	Habilidades necessárias
Visualize métricas, painéis, logs, widgets e alarmes de outras contas.	Como recurso adicional, você pode compartilhar CloudWatch métricas, painéis, registros, widgets e alarmes com outras contas. Cada conta usa uma função do IAM chamada CloudWatch- CrossAccountSharingRole para obter acesso a esses dados. As contas de origem que têm uma relação de confiança com a conta central de monitoram	AWS DevOps, administrador de nuvem, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	ento podem assumir essa função e visualizar dados da conta de monitoramento. CloudWatch fornece um CloudFormation script de exemplo para criar a função. Escolha Gerenciar perfil no IAM e execute esse script nas contas em que você deseja visualizar os dados. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root" ] }, "Action": "sts:AssumeRole" } ]`	

Tarefa	Descrição	Habilidades necessárias
	<pre>}</pre> Para obter mais informaçõ es, consulte Habilitando a funcionalidade entre contas CloudWatch na CloudWatch documentação.	

(Opcional) Visualizar entre contas e entre regiões a partir da conta de monitoramento

Tarefa	Descrição	Habilidades necessárias
Configure o acesso entre contas e entre regiões.	Na conta central de monitoram ento, você pode, opcionalm ente, adicionar um seletor de contas para alternar facilment e entre contas e visualizar seus dados sem precisar se autenticar. 1. Faça login na conta central de monitoramento. 2. Abra o console de CloudWatch . 3. No painel de navegação à esquerda, escolha Configurações. 4. Na seção Exibir entre contas e entre regiões, escolha Configurar. 5. Escolha Habilitar e marque a caixa de seleção Mostrar seletor no console.	AWS DevOps, administrador de nuvem, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	6. Escolha uma destas opções: • Entrada do ID da conta: essa opção pede que você insira manualmente o ID da conta sempre que quiser alterar as contas para visualizar os dados de várias contas. • Seletor de contas da AWS Organization: se você se integrou CloudWatch com AWS Organizations, essa opção fornece um seletor suspenso com uma lista completa de contas na organização. • Seletor de conta personalizado: essa opção permite inserir manualmente uma lista de contas IDs para preencher o seletor. 7. Escolha Salvar alterações. Para obter mais informações, consulte CloudWatch Console multiregional entre contas na CloudWatch documentação.	

Recursos relacionados

- CloudWatch observabilidade entre contas (documentação da Amazon CloudWatch)
- Referência da API do Amazon CloudWatch Observability Access Manager (CloudWatch documentação da Amazon)
- Recurso: aws_oam_sink (documentação do Terraform)
- Fonte de dados: aws_oam_link (documentação do Terraform)
- CloudWatchObservabilityAccessManager(Documentação AWS do Boto3)

Verifique as EC2 instâncias para ver as tags obrigatórias no lançamento

Criado por Susanne Kangnoh (AWS) e Archit Mathur (AWS)

Resumo

O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na nuvem da Amazon Web Services (AWS). O uso da Amazon EC2 elimina a necessidade de investir antecipadamente em hardware, para que você possa desenvolver e implantar aplicativos com mais rapidez.

Você pode usar a marcação para categorizar seus recursos da AWS de maneiras diferentes. EC2 a marcação de instâncias é útil quando você tem muitos recursos em sua conta e deseja identificar rapidamente um recurso específico com base nas tags. Você pode atribuir metadados personalizados às suas EC2 instâncias usando tags. Cada tag consiste em um valor e em uma chave definida pelo usuário. Recomendamos criar um conjunto consistente de tags para atender às necessidades da sua organização.

Esse padrão fornece um CloudFormation modelo da AWS para ajudar você a monitorar EC2 instâncias para tags específicas. O modelo cria um evento da Amazon CloudWatch Events que monitora a AWS CloudTrail TagResourceou UntagResourceos eventos para detectar novas marcações de EC2 instâncias ou remoção de tags. Se uma tag predefinida estiver ausente, ela chama uma função do Lambda da AWS, que envia uma mensagem de violação para um endereço de e-mail que você fornece, usando o Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do Amazon Simple Storage Service (Amazon S3) para carregar o código do Lambda fornecido.
- Um endereço de e-mail no qual você deseja receber notificações de violação.

Limitações

- Essa solução suporta CloudTrail TagResourcenossos UntagResourceeventos. Ela não cria notificações para nenhum outro evento.
- Essa solução verifica somente as chaves de tag. Ele não monitora os valores-chave.

Arquitetura

Arquitetura de fluxo de trabalho

Automação e escala

- Você pode usar o CloudFormation modelo da AWS várias vezes para diferentes regiões e contas da AWS. Você precisa executar o modelo somente uma vez em cada região ou conta.

Ferramentas

Serviços da AWS

- Amazon EC2 — O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço web que fornece capacidade computacional segura e redimensionável na nuvem. Ele foi projetado para facilitar a computação em nuvem na escala da web para os desenvolvedores.
- AWS CloudTrail — CloudTrail é um serviço da AWS que ajuda você com governança, conformidade e auditoria operacional e de risco da sua conta da AWS. As ações realizadas por um usuário, função ou serviço da AWS são registradas como eventos em CloudTrail.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS. CloudWatch Os eventos ficam cientes das mudanças operacionais à medida que elas ocorrem e tomam medidas corretivas conforme necessário, enviando mensagens para responder ao ambiente, ativando funções, fazendo alterações e capturando informações de estado.
- AWS Lambda: o Lambda é um serviço de computação que oferece suporte à execução de código sem a necessidade de provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço web que permite que aplicativos, usuários finais e dispositivos enviem e recebam notificações da nuvem instantaneamente.

Código

Esse padrão inclui um anexo com dois arquivos:

- `index.zip` é um arquivo compactado que inclui o código do Lambda para esse padrão.
- `ec2-require-tags.yaml`é um CloudFormation modelo que implanta o código Lambda.

Consulte a seção Tópicos para obter informações sobre como usar esses arquivos.

Épicos

Implantar o código do Lambda

Tarefa	Descrição	Habilidades necessárias
Faça upload do código para um bucket do S3.	Crie um novo bucket do S3 ou use um bucket do S3 existente para carregar o arquivo `index.zip` anexado (código do Lambda). Esse bucket deve estar na mesma região da AWS que os recursos (EC2 instâncias) que você deseja monitorar.	Arquiteto de nuvem
Implante o CloudFormation modelo.	Abra o console do Cloudform ation na mesma região da AWS do bucket S3 e implante o arquivo `ec2-require-tags.yaml` fornecido no anexo. No próximo épico, forneça valores para os parâmetros do modelo.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Dar o nome do bucket do S3.	Insira o nome do bucket do S3 que você criou ou selecionou no primeiro épico. Esse bucket do S3 contém o arquivo.zip do código Lambda e deve estar na mesma região da AWS do CloudFormation modelo e das EC2 instâncias que você deseja monitorar.	Arquiteto de nuvem
Fornecer a chave do S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `index.zip` ou `controls/index.zip`).	Arquiteto de nuvem
Fornecer um endereço de e-mail.	Forneça um endereço de e-mail ativo no qual você deseja receber notificações de violação.	Arquiteto de nuvem
Defina o nível de registro em log.	Especifique o nível de registro em log e a verbosidade. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo e deve ser usado somente para depuração. `Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`Warning` designa situações potencialmente prejudiciais.	
Inserir as chaves de tag necessárias.	Insira as chaves de tag que você deseja verificar . Se você quiser especific ar várias chaves, separe-as com vírgulas, sem espaços. (Por exemplo, `ApplicationId,CreatedBy,Environment,Organization` pesquisa quatro chaves.) O evento CloudWatch Events pesquisa essas chaves de tag e envia uma notificação se elas não forem encontradas.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirme a assinatura por e-mail.	Quando o CloudFormation modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail que você forneceu. Você precisa confirmar sua assinatura para começar a receber as notificações.	Arquiteto de nuvem

Recursos relacionados

- Criar um bucket (documentação do Amazon S3)
- Carregar objetos (documentação do Amazon S3)
- Marque seus EC2 recursos da Amazon (EC2 documentação da Amazon)
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS (documentação da CloudTrail Amazon CloudWatch)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Limpe os recursos AWS do Account Factory for Terraform (AFT) com segurança após a perda do arquivo de estado

Criado por Gokendra Malviya (AWS)

Resumo

Quando você usa o AWS Account Factory for Terraform (AFT) para gerenciar seu AWS Control Tower ambiente, o AFT gera um arquivo de estado do Terraform para rastrear o estado e a configuração dos recursos criados pelo Terraform. A perda do arquivo de estado do Terraform pode criar desafios significativos para o gerenciamento e a limpeza de recursos. Esse padrão fornece uma abordagem sistemática para identificar e remover com segurança os recursos relacionados ao AFT, mantendo a integridade do seu AWS Control Tower ambiente.

O processo foi projetado para garantir a remoção adequada de todos os componentes do AFT, mesmo sem a referência do arquivo de estado original. Esse processo fornece um caminho claro para restabelecer e reconfigurar com sucesso o AFT em seu ambiente, para ajudar a garantir o mínimo de interrupção em suas operações. AWS Control Tower

Para obter mais informações sobre o AFT, consulte a AWS Control Tower documentação.

Pré-requisitos e limitações

Pré-requisitos

- Uma compreensão completa da arquitetura AFT.
- Acesso de administrador às seguintes contas:
  - Conta de gerenciamento AFT
  - AWS Control Tower Conta de gerenciamento
  - Conta do Log Archive
  - Conta de auditoria
- Verificação de que nenhuma política de controle de serviço (SCPs) contém restrições ou limitações que bloqueariam a exclusão de recursos relacionados ao AFT.

Limitações

- Esse processo pode limpar recursos de forma eficaz, mas não pode recuperar arquivos de estado perdidos, e alguns recursos podem exigir identificação manual.

- A duração do processo de limpeza depende da complexidade do seu ambiente e pode levar várias horas.
- Esse padrão foi testado com a versão 1.12.2 do AFT e exclui os seguintes recursos. Se você estiver usando uma versão diferente do AFT, talvez seja necessário excluir recursos adicionais.

Nome do serviço	Número de recursos
AWS CodeBuild	6
AWS CodeCommit	4
AWS CodePipeline	4
Amazon DynamoDB	5
Nuvem de computação elástica da Amazon (Amazon EC2)	16
Amazon EventBridge	4
AWS Identity and Access Management Funções (IAM)	40
AWS Key Management Service (AWS KMS)	2
AWS Lambda	17
Amazon Simple Storage Service (Amazon S3)	2
Amazon Simple Notification Service (Amazon SNS)	2
Amazon Simple Queue Service (Amazon SQS)	2
AWS Systems Manager	62
AWS Step Functions	4

> **Important**
>
> Os recursos que são excluídos pelas etapas desse padrão não podem ser recuperados. Antes de seguir essas etapas, verifique cuidadosamente os nomes dos recursos e certifique-se de que eles foram criados pelo AFT.

Arquitetura

O diagrama a seguir mostra os componentes do AFT e o fluxo de trabalho de alto nível. O AFT configura um pipeline do Terraform que ajuda você a provisionar e personalizar suas contas em AWS Control Tower. O AFT segue um GitOps modelo para automatizar os processos de provisionamento de contas em. AWS Control Tower Você cria um arquivo Terraform para uma solicitação de conta e o submete em um repositório, que fornece a entrada que aciona o fluxo de trabalho AFT para provisionamento de contas. Depois que o provisionamento da conta for concluído, o AFT poderá executar etapas adicionais de personalização automaticamente.

Nesta arquitetura:

- AWS Control Tower A conta de gerenciamento Conta da AWS é dedicada ao AWS Control Tower serviço. Isso também é normalmente chamado de conta do AWS pagador ou conta AWS Organizations de gerenciamento.
- A conta de gerenciamento da AFT Conta da AWS é dedicada às operações de gerenciamento da AFT. Isso é diferente da conta de gerenciamento da sua organização.
- A conta vendida Conta da AWS contém todos os componentes e controles básicos que você selecionou. A AFT usa AWS Control Tower para vender uma nova conta.

Para obter informações adicionais sobre essa arquitetura, consulte Introdução ao AFT no AWS Control Tower workshop.

Ferramentas

Serviços da AWS

- AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas.

- AWS O Account Factory for Terraform (AFT) configura um pipeline do Terraform para ajudá-lo a provisionar e personalizar contas e recursos no. AWS Control Tower
- AWS Organizationsajuda você a gerenciar e governar centralmente seu ambiente à medida que você cresce e escala seus AWS recursos. Usando o Organizations, você pode criar contas e alocar recursos, agrupar contas para organizar seus fluxos de trabalho, aplicar políticas de governança e simplificar o faturamento usando um único método de pagamento para todas as suas contas.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los. Esse padrão requer funções e permissões do IAM.

Outras ferramentas

- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Práticas recomendadas

- Para AWS Control Tower isso, consulte Práticas recomendadas para AWS Control Tower administradores na AWS Control Tower documentação.
- Para o IAM, consulte as melhores práticas de segurança na documentação do IAM.

Épicos

Excluir recursos do AFT na conta de gerenciamento do AFT

Tarefa	Descrição	Habilidades necessárias
Exclua recursos identificados pela tag AFT.	1. Faça login na conta de gerenciamento do AFT com permissões de administr ador. 2. Abra o console de AWS Resource Groups.	Administrador da AWS, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	3. Selecione a região em AWS Control Tower que foi implantado. 4. No painel de navegação, escolha Editor de tags. 5. Em Tipos de recursos, escolha Todos os tipos de recursos compatíveis. 6. Para Tags, digite managed_by como a chave da tag e AFT como o valor da tag. 7. Escolha Recursos de pesquisa. Essa pesquisa exibe todos os recursos que foram criados pelo AFT. 8. Identifique os nomes dos recursos e exclua-os usando os consoles de serviço correspondentes. Por exemplo, para excluir recursos do Parameter Store: a. Abra o console de AWS Systems Manager. b. No painel de navegação , selecione Parameter Store (Repositório de parâmetros). c. Na caixa de pesquisa, clique para exibir a	

Tarefa	Descrição	Habilidades necessárias
	lista suspensa, escolha Nome, escolha igual a e digite /aft. d. Exclua os parâmetros em lotes de 10. (Esse é o número máximo que você pode excluir ao mesmo tempo.) Para a versão 1.12.2 do AFT, haverá aproximadamente 62 recursos do Parameter Store a serem excluídos. Todos os nomes de parâmetros começarão com /aft. No entanto, nem todos os recursos podem ser identificados por AWS Resource Groups. Nas etapas a seguir, você encontrará e excluirá os recursos restantes.	

Tarefa	Descrição	Habilidades necessárias
Exclua as funções do IAM.	1. Faça login na conta de gerenciamento do AFT com permissões de administrador. 2. Abra o console do IAM. 3. Exclua essas funções na ordem listada (a ordem é importante devido às dependências): • `aft-*` • `AWSAFTAdmin` • `AWSAFTExecution` • `AWSAFTService` • `codebuild_trigger_role`	Administrador da AWS, AWS DevOps, DevOps engenheiro
Exclua o cofre AWS Backup de backup.	1. Abra o console de AWS Backup. 2. Localize o cofre de backup chamado `aws_backup_vault` . 3. Confirme se o cofre não contém nenhum backup ativo. 4. Exclua `aws_backup_vault` .	Administrador da AWS, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Exclua CloudWatch os recursos da Amazon.	1. Abra o console de CloudWatch . 2. Exclua os seguintes recursos na ordem listada: a. Ônibus de eventos: Excluiraws_cloud watch_event_bus . b. Registros: pesquise o prefixo AFT e exclua todos os grupos de registros relacionados. c. Definições de consulta: exclua as seguintes consultas: • Customization Logs by Account ID • Customization Logs by Customization Request ID	Administrador da AWS, AWS DevOps, DevOps engenheiro
Exclua AWS KMS recursos.	1. Mude para a região secundária, que serve como back-end para o rastreamento do estado do próprio AFT. 2. Abra o console de AWS KMS. 3. Exclua o alias chamado AFT.	Administrador da AWS, AWS DevOps, DevOps engenheiro

Exclua recursos AFT na conta do Log Archive

Tarefa	Descrição	Habilidades necessárias
Exclua os buckets do S3.	1. Faça login na conta do Log Archive com permissões de administrador. 2. Abra o console Amazon S3. 3. Esvazie os seguintes baldes: • `aws-aft-logs-471112509802-us-east-1` • `aws-aft-s3-access-logs-471112509802-us-east-1` (`111122223333` Substitua pelo ID da sua conta.) 4. Exclua os dois compartim entos.	Administrador da AWS, AWS DevOps, DevOps engenheiro
Exclua as funções do IAM.	1. Abra o console do IAM. 2. Verifique se as seguintes funções não estão sendo usadas por nenhum serviço ativo: • `AWSAFTService` • `AWSAFTExecution` 3. Exclua as duas funções.	Administrador da AWS, AWS DevOps, DevOps engenheiro

Excluir recursos AFT na conta de auditoria

Tarefa	Descrição	Habilidades necessárias
Exclua as funções do IAM.	1. Faça login na conta de auditoria com permissões de administrador. 2. Abra o console do IAM. 3. Verifique se as seguintes funções não estão sendo usadas por nenhum serviço ativo: • `AWSAFTService` • `AWSAFTExecution` 4. Exclua as duas funções.	Administrador da AWS, AWS DevOps, DevOps engenheiro

Excluir recursos AFT na conta AWS Control Tower de gerenciamento

Tarefa	Descrição	Habilidades necessárias
Exclua as funções do IAM.	1. Faça login na conta AWS Control Tower de gerenciamento com permissões de administrador. 2. Abra o console do IAM. 3. Verifique se as seguintes funções não estão sendo usadas por nenhum serviço ativo: • `AWSAFTService` • `AWSAFTExecution` • `aft-control-tower-events-rule`	Administrador da AWS, AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	4. Exclua as três funções.	
Exclua EventBridge as regras.	1. Abra o EventBridge console da Amazon. 2. No painel de navegação à esquerda, escolha Rules (Regras). 3. Encontre e selecione a regra chamada`aft-capture-ct-events` . 4. Escolha Excluir e confirme a exclusão quando solicitado.	Administrador da AWS, AWS DevOps, DevOps engenheiro

Solução de problemas

Problema	Solução
A desconexão do gateway da Internet não teve êxito.	Ao excluir recursos identificados pela tag AFT, se você encontrar esse problema ao desanexar ou excluir o gateway da Internet, primeiro precisará excluir os VPC endpoints: 1. Faça login na conta de gerenciamento do AFT e abra o console da Amazon VPC. 2. No painel de navegação, na lista Filtrar por VPC, escolha a VPC chamada. aft-management-vpc 3. No painel de navegação, escolha Endpoints. 4. Selecione os endpoints associados à VPC aft-management-vpc.

Problema	Solução
	• Verifique novamente a coluna VPC ID antes da exclusão para evitar a remoção dos endpoints errados. • Tenha cuidado para excluir somente os endpoints associados ao AFT VPC. 5. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC). 6. Na caixa de diálogo de confirmação, digite delete e escolha Delete. 7. Aguarde até que o status do endpoint mude para Excluído. A exclusão pode levar alguns minutos para ser concluída.

Problema	Solução
Você não consegue encontrar as CloudWatch consultas especificadas.	Se você não conseguir encontrar CloudWatch as consultas que foram criadas pelo AFT, siga estas etapas: 1. Faça login na conta de gerenciamento do AFT e abra o CloudWatch console. 2. No painel de navegação, em Registros, escolha Logs Insights. 3. No canto superior direito, escolha o ícone Consultas salvas e amostras. Agora você deve conseguir ver as consultas do AFT. Para obter uma captura de tela, consulte a seção Informações adicionais. 4. Selecione as consultas a seguir e escolha Ações, Excluir para removê-las. • `Customization Logs by Account ID` • `Customization Logs by Customization Request ID`

Recursos relacionados

- POPA:
  - GitHub Repositório
  - Workshop
  - Documentação
- AWS Control Tower documentação

Mais informações

Para visualizar as consultas AFT no painel do CloudWatch Logs Insights, escolha o ícone de consultas salvas e de amostra no canto superior direito, conforme ilustrado na captura de tela a seguir:

Conecte-se a uma EC2 instância da Amazon usando o Gerenciador de Sessões

Criado por Jason Cornick (AWS), Abhishek Bastikoppa (AWS) e Yaniv Ron (AWS)

Resumo

Esse padrão descreve como se conectar a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) usando o Session Manager, um recurso do AWS Systems Manager. Usando esse padrão, você pode executar comandos bash em uma EC2 instância por meio de um navegador da web. O Gerenciador de Sessões não exige que você abra portas de entrada e não exige endereços IP públicos para EC2 instâncias. Além disso, elimina a necessidade de manter os bastion hosts com diferentes chaves Secure Shell (SSH). Você pode controlar o acesso ao Session Manager com as políticas do (IAM) AWS Identity and Access Management e configurar o registro em log, que registra informações importantes, como ações e acesso à instância.

Nesse padrão, você configura uma função do IAM e a associa a uma EC2 instância Linux que você provisiona usando uma Amazon Machine Image (AMI). Em seguida, você configura o login no Amazon CloudWatch Logs e usa o Session Manager para iniciar uma sessão com a instância.

Embora esse padrão se conecte a uma EC2 instância Linux na nuvem da Amazon Web Services (AWS), você pode usar essa abordagem para usar o Session Manager para conexões com outros servidores, como servidores locais ou outras máquinas virtuais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões para acessar o nó gerenciado. Para obter mais informações, consulte Controlar o acesso de sessão do usuário aos nós gerenciados.
- Endpoint da VPC para `ssm`, `ec2`, `ec2messages`, `ssmmessages` e `s3`. Para obter instruções, consulte Criar endpoints da VPC na documentação do Systems Manager.

Arquitetura

Pilha de tecnologias de destino

- Session Manager
- Amazon EC2
- CloudWatch Registros

Arquitetura de destino

1. O usuário autentica sua identidade e credenciais por meio do IAM.
2. O usuário inicia uma sessão SSH por meio do Session Manager e envia chamadas de API para a EC2 instância.
3. O AWS Systems Manager SSM Agent, que está instalado na EC2 instância, se conecta ao Session Manager e executa os comandos.
4. Para fins de auditoria e monitoramento, o Session Manager envia os dados de registro para o CloudWatch Logs. Como alternativa, você pode enviar dados de log para um bucket do Amazon Simple Storage Service (Amazon S3). Para obter mais informações, consulte Log de dados de sessão usando o Amazon S3 (Documentação do Systems Manager).

Ferramentas

Serviços da AWS

- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas, aplicativos e serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente. Esse padrão usa uma Amazon Machine Image (AMI) para provisionar uma EC2 instância Linux.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Systems Manager ajuda você a gerenciar seus aplicativos e infraestrutura em execução na nuvem AWS. Isso simplifica o gerenciamento de aplicações e recursos, diminui o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus recursos da AWS de modo seguro e em grande escala. Esse padrão usa o Session Manager, um atributo do Systems Manager.

Práticas recomendadas

Recomendamos que você leia mais sobre o pilar de segurança do AWS Well-Architected Framework, explore as opções de criptografia e aplique as recomendações de segurança em Configurando o Session Manager (Documentação do Systems Manager).

Épicos

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Crie o perfil do IAM.	Criar o perfil do IAM para o SSM Agent. Siga as instruções em Criação de uma função para um serviço da AWS (Documentação do IAM) e observe o seguinte: 1. Para o serviço da AWS, escolha EC2. 2. Para Políticas de permissões, escolha `AmazonSSMManagedInstanceCore` . 3. Em Nome da função, insira `EC2_SSM_Role` .	Administrador de sistemas AWS
Crie a EC2 instância.	1. Crie a EC2 instância. Siga as instruções em Iniciar uma instância (EC2 documentação da Amazon) e observe o seguinte: a. Na seção Nome e tags, escolha Adicionar tags adicionais. Em Key (Chave), insira `Name` e, em Value (Valor),	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	insira `Productio n_Server_One` . b. Escolha um Amazon Linux AMI que tenha o SSM Agent pré-instalado. Para obter uma lista completa, consulte AMIscom o SSM Agent pré-instalado (documentação do Systems Manager). c. Na seção Detalhes avançados, no perfil da instância do IAM, escolha EC2_SSM_Role. 2. Abra o console do Systems Manager em https://console.aws.amazon.com/systems-manager/. 3. No painel de navegação, escolha Fleet Manager. 4. Verificar se a instância aparecerá na lista de nós gerenciados.	

Tarefa	Descrição	Habilidades necessárias
Configurar registro em log.	1. Crie um grupo de CloudWatch registros em Registros. Siga as instruções em Criar um grupo de CloudWatch registros (documentação de registros). Escolha o novo grupo de logs `SessionManager` . 2. Configure o registro para o Session Manager. Siga as instruções em Registrar dados da sessão usando o Amazon CloudWatch Logs (documentação do Systems Manager) e observe o seguinte: a. Não selecione Permitir somente grupos de CloudWatch registros criptografados. b. Em Escolha um grupo de registros na lista, escolha SessionManager.	Administrador de sistemas AWS

Conectar à instância

Tarefa	Descrição	Habilidades necessárias
Conecte-se à EC2 instância.	1. Iniciar uma sessão no console do Systems Manager. Iniciar uma sessão consultar Iniciar uma sessão(Documentação	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	do Systems Manager). Na lista Instâncias de destino, escolha o botão de opção à esquerda da instância Production_Server_One. 2. Depois que a conexão for feita, execute vários comandos bash. 3. No console do Systems Manager, encerre a sessão. Para obter instruções, consulte Encerrar uma sessão (Documentação do Systems Manager).	
Valide o registro em log.	1. Em CloudWatch Registros, abra o fluxo de registros do grupo de registros. Para obter instruções, consulte Exibir dados de registro (documentação de CloudWatch registros). 2. Nos dados de log, confirme se os comandos que você executou na história anterior estão listados.	Administrador de sistemas AWS

Solução de problemas

Problema	Solução
Problemas do IAM	Para obter suporte, consulte Solução de problemas (Documentação do IAM).

Recursos relacionados

- Pré-requisitos completos do Session Manager (Documentação do Systems Manager)
- Projetando e implementando o registro e o monitoramento com a Amazon CloudWatch (AWS Prescriptive Guidance)

Crie um pipeline em regiões da AWS que não oferecem suporte à AWS CodePipeline

Criado por Anand Krishna Varanasi (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

CodePipeline A AWS é um serviço de orquestração de entrega contínua (CD) que faz parte de um conjunto de DevOps ferramentas da Amazon Web Services (AWS). Ele se integra a uma grande variedade de fontes (como sistemas de controle de versão e soluções de armazenamento), produtos e serviços de integração contínua (CI) da AWS e de parceiros da AWS e produtos de código aberto para fornecer um serviço de end-to-end fluxo de trabalho para implantações rápidas de aplicativos e infraestrutura.

No entanto, CodePipeline não é compatível com todas as regiões da AWS e é útil ter um orquestrador invisível que conecte CI/CD services. This pattern describes how to implement an end-to-end workflow pipeline in AWS Regions where CodePipeline isn't yet supported by using AWS CI/CD os serviços da AWS, como AWS CodeBuild, CodeCommit AWS e AWS. CodeDeploy

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- CLI do AWS Cloud Development Kit (AWS CDK) versão 2.28 ou superior

Arquitetura

Pilha de tecnologias de destino

O diagrama a seguir mostra um pipeline que foi criado em uma região que não oferece suporte CodePipeline, como a região da África (Cidade do Cabo). Um desenvolvedor envia os arquivos de CodeDeploy configuração (também chamados de scripts de gancho do ciclo de vida de implantação) para o repositório Git hospedado por. CodeCommit (Consulte o GitHub repositório fornecido com esse padrão.) Uma EventBridge regra da Amazon é iniciada automaticamente. CodeBuild

Os arquivos de CodeDeploy configuração são obtidos CodeCommit como parte do estágio de origem do pipeline e transferidos para o. CodeBuild

Na próxima fase, CodeBuild executa as seguintes tarefas:

1. Faz o download do arquivo TAR do código-fonte da aplicação. Você pode configurar o nome desse arquivo usando o Parameter Store, um recurso do AWS Systems Manager.
2. Faz o download dos arquivos de CodeDeploy configuração.
3. Cria um arquivo combinado de código-fonte e arquivos CodeDeploy de configuração do aplicativo que são específicos para o tipo de aplicativo.
4. Inicia a CodeDeploy implantação em uma instância do Amazon Elastic Compute Cloud EC2 (Amazon) usando o arquivamento combinado.

Ferramentas

Serviços da AWS

- CodeBuildA AWS é um serviço de criação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes unitários e produzir artefatos prontos para implantação.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- A AWS CodeDeploy automatiza implantações na Amazon EC2 ou em instâncias locais, funções do AWS Lambda ou serviços Amazon Elastic Container Service (Amazon ECS).
- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.

Código

O código desse padrão está disponível no repositório GitHub CodePipeline Unsupported Regions.

Épicos

Configurar a estação de trabalho do desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Instale a AWS CDK CLI.	Para obter instruções, consulte a documentação do AWS CDK.	AWS DevOps
Instalar um cliente Git.	Para criar commits, você pode usar um cliente Git instalado em seu computador local e, em seguida, enviar seus commits para o repositório. CodeCommit Para configurar CodeCommit com seu cliente Git, consulte a CodeCommit documentação.	AWS DevOps
Instale o npm.	Instale o gerenciador de pacotes npm. Para obter mais informações, consulte a documentação do npm.	AWS DevOps

Configurar o pipeline

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de códigos.	Clone o repositório de regiões GitHub CodePipeline não suportadas em sua máquina local executando o comando a seguir. `git clone https://github.com/aws-samp`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`les/invisible-code pipeline-unsupported-regions`	

Tarefa	Descrição	Habilidades necessárias
Defina os parâmetros em cdk.json.	Abra o arquivo `cdk.json` e forneça valores para os seguintes parâmetros: `"pipeline_account" :"XXXXXXXXXXXX", "pipeline_region":" us-west-2", "repo_name": "app-dev-repo", "ec2_tag_key": "test-vm", "configName" : "cbdeployconfig", "deploymentGroupName": "cbdeploygroup", "applicationName" : "cbdeployapplication", "projectName" : "CodeBuildProject"` em que: • `pipeline_account` é a conta da AWS na qual o pipeline será compilado. • `pipeline_region` é a região da AWS onde o pipeline será construído. • `repo_name` é o nome do CodeCommit repositório. • `ec2_tag_key` é a tag anexada à EC2 instância na qual você deseja implantar o código.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• `configName` é o nome do arquivo CodeDeploy de configuração. • `deploymentGroupNam e` é o nome do grupo CodeDeploy de implantaç ão. • `applicationName` é o nome do CodeDeploy aplicativo. • `projectName` é o nome CodeBuild do projeto.	

Configure a biblioteca de estruturas CDK da AWS.	No GitHub repositório clonado, use os comandos a seguir para instalar a biblioteca de construção do AWS CDK, criar seu aplicativo e sintetiza r para gerar o modelo da AWS CloudFormation para o aplicativo.
	`npm i aws-cdk-lib`
	`npm run build`
	`cdk synth`
		AWS DevOps

Implante a aplicação WS CDK CLI de exemplo.	Implante o código executand o o comando a seguir em uma região sem suporte (como `af-south-1`). `cdk deploy`	AWS DevOps

Configure o CodeCommit repositório para CodeDeploy

Tarefa	Descrição	Habilidades necessárias
Configure o CI/CD para o aplicativo.	Clone o CodeCommit repositório que você especific ou no `cdk.json` arquivo (chamado `app-dev-repo` por padrão) para configura r o pipeline de CI/CD para o aplicativo. `git clone https://g it-codecommit.us-w est-2.amazonaws.com/ v1/repos/app-dev-repo` onde o nome do repositór io e a região dependem dos valores fornecidos no arquivo `cdk.json`.	AWS DevOps

Teste o pipeline

Tarefa	Descrição	Habilidades necessárias
Teste o pipeline com instruçõe s de implantação.	A `CodeDeploy_Files` pasta do repositório GitHub CodePipeline Unsupport ed Regions inclui arquivos de amostra que instruem CodeDeploy a implantação do aplicativo. O `appspec.y ml` arquivo é um arquivo CodeDeploy de configura ção que contém ganchos para controlar o fluxo de	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	implantação do aplicativo. Você pode usar os arquivos de amostra `index.html` , `start_server.sh` , `stop_server.sh` e `install_dependencies.sh` para atualizar um site hospedado no Apache. Esses são exemplos: você pode usar o código no GitHub repositório para implantar qualquer tipo de aplicativo. Quando os arquivos são enviados para o CodeCommit repositório, o pipeline invisível é iniciado automaticamente. Para ver os resultados da implantação, verifique os resultados das fases individuais nos CodeBuild CodeDeploy consoles e.	

Recursos relacionados

- Conceitos básicos (documentação do AWS CDK)
- Introdução ao kit de desenvolvimento em nuvem (CDK) (AWS Workshop Studio)
- Workshop sobre o AWS CDK

Personalize os nomes das funções padrão usando AWS CDK aspectos e escotilhas de escape

Criado por SANDEEP SINGH (AWS) e James Jacob (AWS)

Resumo

Esse padrão demonstra como personalizar os nomes padrão das funções criadas por AWS Cloud Development Kit (AWS CDK) construções. A personalização dos nomes das funções geralmente é necessária se sua organização tiver restrições específicas com base nas convenções de nomenclatura. Por exemplo, sua organização pode definir limites de permissões AWS Identity and Access Management (IAM) ou políticas de controle de serviço (SCPs) que exijam um prefixo específico nos nomes das funções. Nesses casos, os nomes de função padrão gerados pelas AWS CDK construções podem não atender a essas convenções e talvez precisem ser alterados. Esse padrão atende a esses requisitos usando escotilhas de escape e aspectos no AWS CDK. Você usa escotilhas de escape para definir nomes de funções personalizados e aspectos para aplicar um nome personalizado a todas as funções, a fim de garantir a adesão às políticas e restrições da sua organização.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Pré-requisitos especificados na documentação AWS CDK

Limitações

- Os aspectos filtram os recursos com base nos tipos de recursos, para que todas as funções compartilhem o mesmo prefixo. Se você precisar de prefixos de função diferentes para funções diferentes, será necessária uma filtragem adicional com base em outras propriedades. Por exemplo, para atribuir prefixos diferentes a funções associadas a AWS Lambda funções, você pode filtrar por atributos ou tags de função específicos e aplicar um prefixo para funções relacionadas ao Lambda e um prefixo diferente para outras funções.
- Os nomes de função do IAM têm um comprimento máximo de 64 caracteres, portanto, os nomes de função modificados precisam ser cortados para atender a essa restrição.

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Pilha de tecnologias de destino

- AWS CDK
- AWS CloudFormation

Arquitetura de destino

- Um AWS CDK aplicativo consiste em uma ou mais AWS CloudFormation pilhas, que são sintetizadas e implantadas para gerenciar recursos. AWS
- Para modificar uma propriedade de um recurso AWS CDK gerenciado que não é exposta por uma construção de camada 2 (L2), use uma saída de emergência para substituir as CloudFormation propriedades subjacentes (nesse caso, o nome da função) e um aspecto para aplicar a função a todos os recursos no AWS CDK aplicativo durante o processo de síntese da pilha. AWS CDK

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- AWS CDK A interface de linha de comando (AWS CDK CLI) (também conhecida como kit de AWS CDK ferramentas) é um kit de desenvolvimento em nuvem de linha de comando que ajuda você a interagir com seu aplicativo. AWS CDK O `cdk` comando CLI é a principal ferramenta para interagir com seu aplicativo. AWS CDK Ele executa seu aplicativo, interroga o modelo de aplicativo que você definiu e produz e implanta os CloudFormation modelos gerados pelo. AWS CDK
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.

Repositório de código

O código-fonte e os modelos desse padrão estão disponíveis no repositório GitHub CDK Aspects Override.

Práticas recomendadas

Consulte as melhores práticas para usar o AWS CDK in TypeScript para criar projetos de IaC no site de Orientação AWS Prescritiva.

Épicos

Instale a AWS CDK CLI

Tarefa	Descrição	Habilidades necessárias
Instale a AWS CDK CLI.	Para instalar a AWS CDK CLI globalmente, execute o comando: `npm install -g aws-cdk`	AWS DevOps
Verificar a versão.	Execute o comando : `cdk --version` Confirme se você está usando a versão 2 da AWS CDK CLI.	AWS DevOps
Inicialize o AWS CDK ambiente.	Antes de implantar os AWS CloudFormation modelos, prepare a conta Região da AWS que você deseja usar. Execute o comando : `cdk bootstrap <account> /<Region>`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte AWS CDK bootstrapping na documentação. AWS	

Implante o AWS CDK aplicativo para demonstrar o uso de aspectos

Tarefa	Descrição	Habilidades necessárias

Configure o projeto.	1. Clone o GitHub repositório desse padrão em seu computador local:
	`git clone https://github.com/aws-samples/cdk-aspects-override`
	2. Navegue até o diretório do projeto em seu computador local.
	3. Instale as dependências do projeto:
	`npm ci`
		AWS DevOps

Implante pilhas com nomes de função padrão atribuídos pelo AWS CDK.	Implante duas CloudFormation pilhas (`ExampleStack1 eExampleStack2 `) que contenham as funções do Lambda e suas funções associadas: `npm run deploy:ExampleAppWithoutAspects`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	O código não passa explicitamente as propriedades das funções, portanto, os nomes das funções serão criados pelo AWS CDK. Para obter um exemplo de saída, consulte a seção Informações adicionais.	

Tarefa	Descrição	Habilidades necessárias

Implante pilhas com aspectos.	Nesta etapa, você aplica um aspecto que impõe uma convenção de nome de função adicionando um prefixo a todas as funções do IAM implantadas no projeto. AWS CDK O aspecto é definido no `lib/aspects.ts` arquivo. O aspecto usa uma saída de emergência para substituir o nome da função adicionando um prefixo. O aspecto é aplicado às pilhas no `bin/app-with-aspects.ts` arquivo. O prefixo do nome da função usado neste exemplo é `dev-unicorn` .
	
	1. Edite o arquivo `bin/app-with-aspects.ts` .
	2. No arquivo, atualize a variável `ROLE_NAME_PREFIX` com o prefixo `dev-unicorn` :
	
	`const app = new cdk.App();`
	
	`// Define a prefix for the role names`
	`const ROLE_NAME_PREFIX = 'dev-unicorn';`
	
	`// Instantiate the RoleNamingConventi`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	onAspect with the desired prefix
	`const roleNamingConventionAspect = new RoleNamingConventionAspect(ROLE_NAME_PREFIX);`
	3. Implante o AWS CDK aplicativo com aspectos:
	`npm run deploy:ExampleAppWithAspects`
	Para obter um exemplo de saída, consulte a seção Informações adicionais.	

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Exclua suas AWS CloudFormation pilhas.	Depois de terminar de usar esse padrão, execute o comando a seguir para limpar os recursos e evitar custos adicionais: `cdk destroy --all -f && cdk --app npx ts-node bin/app-with-aspects.ts' destroy --all -f`	AWS DevOps

Solução de problemas

Problema	Solução
Você encontra problemas ao usar AWS CDK o.	Consulte Solução de AWS CDK problemas comuns na AWS CDK documentação.

Recursos relacionados

- AWS Cloud Development Kit (AWS CDK)
- AWS CDK documentação
- AWS CDK em GitHub
- Escotilhas de escape
- Aspectos e o AWS CDK

Mais informações

Nomes de funções criados por AWS CloudFormation without aspects

```
Outputs:
ExampleStack1WithoutAspects.Function1RoleName = example-stack1-without-as-
Function1LambdaFunctionSe-y7FYTY6FXJXA
ExampleStack1WithoutAspects.Function2RoleName = example-stack1-without-as-
Function2LambdaFunctionSe-dDZV4rkWqWnI
...

Outputs:
ExampleStack2WithoutAspects.Function3RoleName = example-stack2-without-as-
Function3LambdaFunctionSe-ygMv49iTyMq0
```

Nomes de funções criados por AWS CloudFormation with aspects

```
Outputs:
ExampleStack1WithAspects.Function1RoleName = dev-unicorn-
Function1LambdaFunctionServiceRole783660DC
ExampleStack1WithAspects.Function2RoleName = dev-unicorn-
Function2LambdaFunctionServiceRole2C391181
...
```

```
Outputs:
ExampleStack2WithAspects.Function3RoleName = dev-unicorn-
Function3LambdaFunctionServiceRole4CAA721C
```

Implemente um cluster Cassandra na Amazon EC2 com estática privada IPs para evitar o reequilíbrio

Criado por Dipin Jain (AWS)

Resumo

O IP privado de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) é retido durante todo o seu ciclo de vida. No entanto, o IP privado pode mudar durante uma falha planejada ou não planejada do sistema; por exemplo, durante uma atualização da imagem de máquina da Amazon (AMI). Em alguns cenários, reter um IP estático privado pode melhorar o desempenho e o tempo de recuperação das workloads. Por exemplo, usar um IP estático para um nó inicial do Apache Cassandra evita que o cluster incorra em uma sobrecarga de rebalanceamento.

Esse padrão descreve como conectar uma interface de elastic network secundária às EC2 instâncias para manter o IP estático durante a nova hospedagem. O padrão se concentra nos clusters do Cassandra, mas você pode usar essa implementação para qualquer arquitetura que se beneficie da estática privada. IPs

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Service (AWS)

Versões do produto

- DataStax versão 5.11.1
- Sistema operacional: Ubuntu 16.04.6 LTS

Arquitetura

Arquitetura de origem

A fonte pode ser um cluster Cassandra em uma máquina virtual (VM) local ou em instâncias EC2 na nuvem da AWS. O diagrama a seguir ilustra o segundo cenário. Esse exemplo inclui quatro nós de cluster: três nós iniciais e um nó de gerenciamento. Na arquitetura de origem, cada nó tem uma única interface de rede conectada.

Arquitetura de destino

O cluster de destino é hospedado em EC2 instâncias com uma interface de rede elástica secundária conectada a cada nó, conforme ilustrado no diagrama a seguir.

Automação e escala

Você também pode automatizar a conexão de uma segunda interface de rede elástica a um grupo de Auto EC2 Scaling, conforme descrito em um vídeo do AWS Knowledge Center.

Épicos

Configurar um cluster Cassandra na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Inicie EC2 nós para hospedar um cluster Cassandra.	No EC2 console da Amazon, execute quatro EC2 instâncias para seus nós do Ubuntu em sua conta da AWS. Três nós (iniciais) são usados para o cluster Cassandra, e o quarto nó atua como um nó de gerenciamento de cluster onde você instalará o DataStax Enterprise (DSE). OpsCenter Para obter instruções, consulte a EC2 documentação da Amazon.	Engenheiro de nuvem
Confirme as comunicações do nó.	Certifique-se de que os quatro nós possam se comunicar entre si pelas portas de gerenciamento do banco de dados e do cluster.	Engenheiro de rede
Instale o DSE OpsCenter no nó de gerenciamento.	Instale o DSE OpsCenter 6.1 do pacote Debian no	DBA

Tarefa	Descrição	Habilidades necessárias
	nó de gerenciamento. Para obter instruções, consulte a DataStax documentação.	

Tarefa	Descrição	Habilidades necessárias
Criar uma interface de rede secundária.	O Cassandra gera um identificador exclusivo universal (UUID) para cada nó com base no endereço IP da EC2 instância desse nó. Esse UUID é usado para distribuir nós virtuais (vnodes) no anel. Quando o Cassandra é implantado em EC2 instâncias, os endereços IP são atribuídos automaticamente às instâncias à medida que elas são criadas. No caso de uma interrupção planejada ou não planejada, o endereço IP da nova EC2 instância muda, a distribuição de dados muda e todo o anel precisa ser rebalanceado. Isso não é desejável. Para preservar o endereço IP atribuído, use uma interface de rede elástica secundária com um endereço IP fixo. 1. No EC2 console da Amazon, escolha Interfaces de rede, Criar interface de rede. 2. Em Sub-rede, selecione a sub-rede na qual você criou a EC2 instância.	Engenheiro de nuvem

Tarefa	Descrição	Habilidades necessárias
	3. Em IPv4 Endereço privado, escolha Atribuição automática. 4. Em Grupos de segurança , selecione um grupo de segurança e, em seguida, Criar interface de rede. Para obter mais informaçõ es sobre a criação de uma interface de rede, consulte a EC2 documentação da Amazon.	
Conecte a interface de rede secundária aos nós do cluster.	1. No EC2 console da Amazon, escolha Instância s. 2. Marque a caixa de seleção da EC2 instância que você criou anteriormente. 3. Escolha Actions (Ações), Networking (Redes), Attach network interface (Associar interface de rede). 4. Marque a interface de rede criada na etapa anterior e selecione Anexar. Para obter mais informaçõ es sobre como conectar uma interface de rede, consulte a EC2 documentação da Amazon.	Engenheiro de nuvem

Tarefa	Descrição	Habilidades necessárias
Adicione rotas na Amazon EC2 para lidar com o roteamento assimétrico.	Quando você conectar a segunda interface de rede, a rede provavelmente executará um roteamento assimétrico. Para evitar isso, você pode adicionar rotas para as novas interfaces de rede. Para obter uma explicação detalhada e a remediação do roteamento assimétrico, consulte o vídeo do AWS Knowledge Center ou Superando o roteamento assimétrico em servidores multiresidenciais (artigo de Patrick no Linux Journal, 5 de abril de 2004). McManus	Engenheiro de rede
Atualize as entradas DNS para apontar para o IP da interface de rede secundária.	Aponte o nome de domínio totalmente qualificado (FQDN) do nó para o IP da interface de rede secundária.	Engenheiro de rede
Instale e configure o cluster Cassandra usando o DSE. OpsCenter	Quando os nós do cluster estiverem prontos com as interfaces de rede secundárias, você poderá instalar e configurar o cluster do Cassandra.	DBA

Recupere o cluster da falha do nó

Tarefa	Descrição	Habilidades necessárias
Crie uma AMI para o nó inicial do cluster.	Faça um backup dos nós para que você possa restaurá-los com binários do banco de dados em caso de falha do nó. Para obter instruções, consulte Criar uma AMI na EC2 documentação da Amazon.	Administrador de backup
Recupere-se da falha do nó.	Substitua o nó com falha por uma nova EC2 instância executada a partir da AMI e conecte a interface de rede secundária do nó com falha.	Administrador de backup
Verifique se o cluster do Cassandra está íntegro.	Quando o nó de substituição estiver ativo, verifique a integridade do cluster no DSE. OpsCenter	DBA

Recursos relacionados

- Instalando o DSE OpsCenter 6.1 a partir do pacote Debian (documentação) DataStax
- Como fazer uma interface de rede secundária funcionar em uma EC2 instância do Ubuntu (vídeo do AWS Knowledge Center)
- Melhores práticas para executar o Apache Cassandra na Amazon (publicação no blog EC2 da AWS)

Estenda VRFs para a AWS usando o AWS Transit Gateway Connect

Criado por Adam Till (AWS), Yashar Araghi (AWS), Vikas Dewangan (AWS) e Mohideen (AWS) HajaMohideen

Resumo

O roteamento e encaminhamento virtuais (VRF) é um atributo das redes tradicionais. Ele usa domínios de roteamento lógico isolados, na forma de tabelas de rotas, para separar o tráfego de rede dentro da mesma infraestrutura física. Você pode configurar o AWS Transit Gateway para suportar o isolamento de VRF ao conectar sua rede on-premises à AWS. Esse padrão usa uma arquitetura de exemplo para se conectar localmente VRFs a diferentes tabelas de rotas do gateway de trânsito.

Esse padrão usa interfaces virtuais de trânsito (VIFs) nos anexos do AWS Direct Connect e do Transit Gateway Connect para estender o. VRFs Uma VIF de trânsito é usada para acessar um ou mais gateways de trânsito do Amazon VPC associados aos gateways do Direct Connect. Um anexo do gateway de trânsito Connect conecta um gateway de trânsito a um dispositivo virtual de terceiros que está sendo executado em uma VPC. Um anexo do gateway de trânsito Connect oferece suporte ao protocolo de túnel Generic Routing Encapsulation (GRE) para alto desempenho e ao Protocolo de Gateway da Borda (BGP) para roteamento dinâmico.

A abordagem descrita nesse padrão tem os seguintes benefícios:

- Usando o Transit Gateway Connect, você pode anunciar até 1.000 rotas para o Transit Gateway Connect peer e receber até 5.000 rotas dele. O uso do atributo Direct Connect Transit da VIF sem o Transit Gateway Connect é limitado a 20 prefixos por gateway de trânsito.
- Você pode manter o isolamento do tráfego e usar o Transit Gateway Connect para fornecer serviços hospedados na AWS, independentemente dos esquemas de endereço IP que seus clientes estejam usando.
- O tráfego de VRF não precisa cruzar uma interface virtual pública. Isso facilita o cumprimento dos requisitos de conformidade e segurança em muitas organizações.
- Cada túnel do GRE suporta até 5 Gbps, e você pode ter até quatro túneis do GRE por anexo do gateway de trânsito Connect. Isso é mais rápido do que muitos outros tipos de conexão, como conexões AWS Site-to-Site VPN que suportam até 1,25 Gbps.

Pré-requisitos e limitações

Pré-requisitos

- As contas da AWS necessárias foram criadas (consulte a arquitetura para obter detalhes)
- Permissões para presumir um perfil do IAM no AWS Identity and Access Management (IAM) em cada conta.
- Os perfis do IAM em cada conta devem ter permissões para provisionar recursos do AWS Transit Gateway e do AWS Direct Connect. Para obter mais informações, consulte Autenticação e controle de acesso para seus gateways de trânsito e consulte Gerenciamento de identidade e acesso para o Direct Connect.
- As conexões do Direct Connect foram criadas com sucesso. Para obter mais informações, visite Criar uma conexão usando o assistente de conexão.

Limitações

- Há limites para anexos do Transit Gateway às contas VPCs de produção, controle de qualidade e desenvolvimento. Para obter mais informações, consulte Anexos do gateway de trânsito para uma VPC.
- Há limites para criação e uso de gateways Direct Connect. Para obter mais informações, consulte Cotas do AWS Direct Connect.

Arquitetura

Arquitetura de destino

O exemplo de arquitetura a seguir fornece uma solução reutilizável para implantar o transporte público VIFs com anexos do Transit Gateway Connect. Essa arquitetura fornece resiliência usando vários locais do Direct Connect. Para obter mais informações, visite Máxima resiliência na documentação do Direct Connect. A rede local tem produção, controle de qualidade e desenvolvimento VRFs que são estendidos para a AWS e isolados por meio do uso de tabelas de rotas dedicadas.

No ambiente da AWS, duas contas são dedicadas à extensão do VRFs: uma conta do Direct Connect e uma conta do hub de rede. A conta do Direct Connect contém a conexão e o trânsito VIFs de cada roteador. Você cria o trânsito a VIFs partir da conta do Direct Connect, mas o implanta na conta do hub de rede para poder associá-lo ao gateway Direct Connect na conta do hub de rede. A conta do hub de rede contém o gateway do Direct Connect e o gateway de trânsito. Os recursos da AWS estão conectados da seguinte forma:

1. O Transit VIFs conecta os roteadores nos locais do Direct Connect com o AWS Direct Connect na conta do Direct Connect.
2. Uma VIF de trânsito conecta o Direct Connect ao gateway do Direct Connect na conta do hub de rede.
3. Uma associação de gateway de trânsito conecta o gateway do Direct Connect ao gateway de trânsito na conta do hub de rede.
4. Os anexos do Transit Gateway Connect conectam o gateway de trânsito às contas de produção, controle de qualidade e desenvolvimento. VPCs

Arquitetura de VIF de trânsito

O diagrama a seguir mostra os detalhes da configuração do trânsito VIFs. Esse exemplo de arquitetura usa uma VLAN para a origem do túnel, mas você também pode usar um loopback.

A seguir estão os detalhes da configuração, como números do sistema autônomo (ASNs), para o trânsito VIFs.

Recurso	Item	Detalhes
router-01	ASN	65534
router-02	ASN	65534
router-03	ASN	65534
router-04	ASN	65534
Direct Connect gateway	ASN	64601
Transit gateway	ASN	64600
	CIDR block (Bloco CIDR)	10.100.254.0/24

Arquitetura do Transit Gateway Connect

O diagrama e as tabelas a seguir descrevem como configurar um único VRF por meio de um anexo do gateway de trânsito Connect. Além VRFs disso, atribua túneis exclusivos IDs, endereços IP GRE

do gateway de trânsito e BGP dentro dos blocos CIDR. O endereço IP do GRE de mesmo nível corresponde ao endereço IP de mesmo nível do roteador da VIF de trânsito.

A tabela a seguir contém detalhes da configuração do roteador.

Roteador	Túnel	Endereço IP	Origem	Destination (Destino)
router-01	Túnel 1	169.254.101.17	VLAN 60 169.254.100.1	10.100.254.1
router-02	Túnel 11	169.254.101.81	VLAN 61 169.254.100.5	10.100.254.11
router-03	Túnel 21	169.254.101.145	VLAN 62 169.254.100.9	10.100.254.21
router-04	Túnel 31	169.254.101.209	VLAN 63 169.254.100.13	10.100.254.31

A tabela a seguir contém detalhes da configuração do Transit Gateway.

Túnel	Endereço IP GRE do gateway de trânsito	Endereço IP GRE no mesmo nível	BGP dentro de blocos CIDR
Túnel 1	10.100.254.1	VLAN 60 169.254.100.1	169.254.101.16/29
Túnel 11	10.100.254.11	VLAN 61 169.254.100.5	169.254.101.80/29
Túnel 21	10.100.254.21	VLAN 62	169.254.101.144/29

		169.254.100.9	
Túnel 31	10.100.254.31	VLAN 63 169.254.100.13	169.254.101.208/29

Implantação

A seção Épicos descreve como implantar um exemplo de configuração para um único VRF em vários roteadores de clientes. Depois que as etapas de 1 a 5 forem concluídas, você poderá criar novos anexos do Transit Gateway Connect usando as etapas 6 a 7 para cada novo VRF que você estiver estendendo para a AWS:

1. Crie o gateway de trânsito.
2. Crie uma tabela de rotas do gateway de trânsito para cada VRF.
3. Crie as interfaces virtuais de trânsito.
4. Crie um gateway do Direct Connect.
5. Crie a interface virtual do gateway do Direct Connect e as associações de gateway com prefixos permitidos.
6. Criar um anexo do Connect do gateway de trânsito.
7. Crie pares do gateway de trânsito Connect.
8. Associe o anexo do gateway de trânsito Connect à tabela de rotas.
9. Anuncie rotas para os roteadores.

Ferramentas

Serviços da AWS

- O AWS Direct Connect conecta sua rede interna a um local do Direct Connect por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para serviços públicos da AWS, ignorando provedores de serviço da internet no caminho da sua rede.
- O AWS Transit Gateway é um hub central que conecta nuvens privadas virtuais (VPCs) e redes locais.

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Épicos

Planejar a arquitetura

Tarefa	Descrição	Habilidades necessárias
Crie diagramas de arquitetura personalizados.	1. Na seção Anexos, baixe o modelo do diagrama. 2. Abra o diagrama em anexo no Microsoft Office PowerPoint. 3. No slide Visão geral da arquitetura, personalize o diagrama da arquitetura para seu ambiente. Identifique os locais VRFs que precisam ser estendidos ao seu ambiente da AWS. 4. No slide VIF de trânsito, personalize o diagrama da arquitetura. Identifique os números AS dos roteadores, do gateway do Direct Connect e do gateway de trânsito. Identifique os endereços IP em cada extremidade da VIF de trânsito. 5. No slide do Transit Gateway Connect, personalize um diagrama de arquitetura para cada	Arquiteto de nuvem, administrador de rede

Tarefa	Descrição	Habilidades necessárias
	VRF. Identifique todos os endereços IP necessári os para configurar os roteadores e os pares do Transit Gateway Connect.	

Criar os recursos do Transit Gateway

Tarefa	Descrição	Habilidades necessárias
Crie o gateway de trânsito.	1. Faça login na conta do hub de rede. 2. Siga as instruções em Criar um gateway de trânsito. Observe o seguinte para esse padrão: • Para Amazon side Número de sistema autônomo (ASN), insira um ASN exclusivo. Para este exemplo, o ASN é `64600`. • Selecione suporte DNS. • Para esta arquitetura de amostra, não são necessários o suporte ao VPN ECMP, a associaçã o de tabela de rotas padrão, a prorrogação da tabela de rotas padrão e o suporte a multicast. • Para blocos CIDR do Transit Gateway, insira	Administrador de rede, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	os blocos IPv4 CIDR do seu Transit Gateway. Para os fins deste exemplo, o bloco CIDR é `10.100.254.0/24` .	
Criar uma tabela de rotas do gateway de trânsito.	Siga as instruções em Criar uma tabela de rotas do gateway de trânsito. Observe o seguinte para esse padrão: • Em Name tag, forneça um nome para a tabela de rotas do gateway de trânsito. Recomendamos usar um nome que corresponda ao VRF, como `routetable-dev-vrf` . • Em Transit gateway ID, escolha o gateway de trânsito que você criou anteriormente.	Arquiteto de nuvem, administrador de rede

Crie as interfaces virtuais de trânsito

Tarefa	Descrição	Habilidades necessárias
Crie as interfaces virtuais de trânsito.	1. Faça login na conta do Direct Connect. 2. Siga as instruções em Criar uma interface virtual de trânsito para o gateway Direct Connect. Observe o seguinte para esse padrão:	Arquiteto de nuvem, administrador de rede

Tarefa	Descrição	Habilidades necessárias
	• Em Nome da interface virtual, insira um nome para o VIF de trânsito. Recomendamos usar um nome que corresponda ao roteador, como `transit-vif-router01` . • Em Conexão, selecione o roteador, como`router-01` . • Para Proprietário da interface virtual, insira o ID da conta do hub de rede. Para obter instruções, consulte Visualizar o ID da sua conta da AWS. • Para o gateway do Direct Connect, não faça nenhuma seleção. Você conecta o gateway do Direct Connect em uma etapa subsequente. • Para VLAN, insira a VLAN do roteador, como `60`. • Para o BGP ASN, insira o ASN do roteador, como `65534`. • Em Additional settings (Configurações adicionais), faça o seguinte:	

Tarefa	Descrição	Habilidades necessárias
	• Selecione IPv4. • Em Seu IP do roteador, insira o endereço IP do mesmo roteador, como. `169.254.100.1` • Para IP do roteador Amazon, insira o IP do roteador Amazon, como. `169.254.100.2` • Para a chave de autenticação BGP, é necessária uma senha. Se isso for deixado em branco, a AWS cria uma chave que só pode ser acessada nessa conta. 3. Repita essas instruções para criar todo o trânsito VIFs para o VRF.	

Crie os recursos do Direct Connect

Tarefa	Descrição	Habilidades necessárias
Crie um gateway Direct Connect.	1. Faça login na conta do hub de rede. 2. Siga as instruções em Criação de um gateway do Direct Connect. Observe o seguinte para esse padrão:	Arquiteto de nuvem, administrador de rede

Tarefa	Descrição	Habilidades necessárias
	• Para ASN do lado da Amazon, insira o ASN do gateway do Direct Connect, como `64601`. • Não selecione um gateway privado virtual.	
Conecte o gateway Direct Connect ao trânsito VIFs.	1. Na conta do hub de rede, abra o console do AWS Direct Connect em https://console.aws.amazon.com/directconnect/v2/. 2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais). 3. Selecione uma nova VIF de trânsito e, em seguida, selecione Aceitar. 4. Selecione o gateway do Direct Connect que você criou. 5. Repita essas instruções para cada VIF de trânsito.	Arquiteto de nuvem, administrador de rede

Tarefa	Descrição	Habilidades necessárias
Crie as associações do gateway do Direct Connect com os prefixos permitidos.	Na conta do hub de rede, siga as instruções em Para associar um gateway de trânsito. Observe o seguinte para esse padrão: • Em Gateways, escolha o gateway de trânsito criado anteriormente. • Em Prefixos permitidos, insira o bloco CIDR atribuído ao gateway de trânsito, como `10.100.254.0/24` . A criação dessa associação cria automaticamente um anexo do gateway de trânsito que tem um tipo de recurso do Direct Connect Gateway. Esse anexo não precisa estar associado a uma tabela de rotas do gateway de trânsito.	Arquiteto de nuvem, administrador de rede

Tarefa	Descrição	Habilidades necessárias
Criar um anexo do Connect do gateway de trânsito.	1. Na conta do hub de rede, abra o console da Amazon VPC em. https://console.aws.amazon.com/vpc/ 2. No painel de navegação, selecione Anexos do gateway de trânsito. 3. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito). 4. Em Nome, insira um nome para o anexo. Recomendamos usar um nome que corresponda ao VRF, como `PROD-VRF`. 5. Em Transit gateway ID, escolha o gateway de trânsito que você criou anteriormente. 6. Em Tipo do anexo, selecione Connect. 7. Em ID do anexo de transporte, selecione o gateway do Direct Connect que você criou anteriormente. 8. Selecione Criar anexo do gateway de trânsito. 9. Repita esta etapa para cada VRF que você pretende estender.	Arquiteto de nuvem, administrador de rede

Tarefa	Descrição	Habilidades necessárias
Crie pares do gateway de trânsito Connect.	1. Na conta do hub de rede, siga as instruções em Criar um Transit Gateway Connect (túnel do GRE) no mesmo nível. Observe o seguinte para esse padrão: • Em Name tag, insira um nome para o peer do Transit Gateway Connect. Recomenda mos usar um nome que corresponda ao roteador, como `connectpeer-router01` . • Para o endereço GRE do Transit Gateway, insira o endereço IP atribuído do bloco CIDR do Transit Gateway, como`10.100.254.1` . • Em Endereço GRE no mesmo nível, insira o endereço IP atribuído à VLAN criada no roteador para a VIF de trânsito, como `169.254.100.1` . Desde que a AWS possa acessar o endereço IP, você pode usar qualquer interface, como VLAN ou Loopback, para o endereço GRE de mesmo nível.	

Tarefa	Descrição	Habilidades necessárias
	• Para BGP Inside CIDR Blocks (IPv4), insira o endereço IP do BGP dentro do bloco CIDR, como. `169.254.101.16/29` • Para ASN de mesmo nível, insira o ASN do roteador, como. `65534` 2. Repita essas instruções para criar um túnel GRE para cada roteador.	

Anuncie rotas para os roteadores

Tarefa	Descrição	Habilidades necessárias
Anuncie as rotas.	Associe o novo anexo do gateway de trânsito Connect à tabela de rotas que você criou anteriormente para esse VRF. Por exemplo, associe o anexo Connect do gateway de trânsito de produção à tabela de rotas `Production-VRF` . Crie uma rota estática para o prefixo anunciado para os roteadores. 1. Faça login na conta do hub de rede.	Administrador de rede, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	2. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. 3. No painel de navegação , em Transit Gateways, escolha Tabelas de rotas Transit Gateway. 4. Selecione a tabela de rotas do `Production-VRF` . 5. No menu Ações, escolha Criar rota estática. 6. Para CIDR, insira o bloco CIDR da rota anunciada para o anexo do gateway de trânsito na VPC de destino, como. `10.100.1.0/24` 7. Em Escolher anexo, selecione o anexo relevante do Transit Gateway Connect. 8. Selecione Criar rota estática.	

Recursos relacionados

Documentação da AWS

- Documentação do Direct Connect
  - Trabalhar com gateways Direct Connect
  - Associações de gateways de trânsito
  - Interfaces virtuais do AWS Direct Connect
- Documentação do Transit Gateway

- Trabalhar com gateways de trânsito
- Anexos do gateway de trânsito a um gateway do Direct Connect
- Anexos do Transit Gateway Connect e pares do Transit Gateway Connect
- Criar um anexo do Connect do gateway de trânsito

Publicações do blog da AWS

- Segmentação de redes híbridas com o AWS Transit Gateway Connect
- Usando o AWS Transit Gateway, conecte-se para ampliar VRFs e aumentar a publicidade do prefixo IP

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Receber notificações do Amazon SNS quando o estado de chave de uma chave do AWS KMS mudar

Criado por Shubham Harsora (AWS), Aromal Raj Jayarajan (AWS) e Navdeep Pareek (AWS)

Resumo

Os dados e metadados associados a uma chave do AWS Key Management Service (AWS KMS) são perdidos quando essa chave é excluída. A exclusão é irreversível e você não pode recuperar dados perdidos (incluindo dados criptografados). Você pode evitar a perda de dados ao configurar um sistema de notificação para alertá-lo sobre mudanças de status nos estados principais de suas chaves do AWS KMS.

Esse padrão mostra como monitorar as alterações de status nas chaves do AWS KMS usando a Amazon e o EventBridge Amazon Simple Notification Service (Amazon SNS) para emitir notificações automáticas sempre que o estado da chave do AWS KMS mudar para ou. `Disabled` `PendingDeletion` Por exemplo, se um usuário tentar desabilitar ou excluir uma chave do AWS KMS, você receberá uma notificação por e-mail com detalhes sobre a tentativa de alteração de status. Você também pode usar esse padrão para programar a exclusão das chaves do AWS KMS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa do AWS com um usuário do Identity and Access Management (IAM).
- Uma chave do AWS KMS

Arquitetura

Pilha de tecnologia

- Amazon EventBridge
- AWS Key Management Service (AWS KMS)
- Amazon Simple Notification Service (Amazon SNS)

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para criar um processo automatizado de monitoramento e notificação para detectar quaisquer alterações no estado de uma chave do AWS KMS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário desativa ou programa a exclusão de uma chave do AWS KMS.
2. Uma EventBridge regra avalia o agendado `Disabled` ou o `PendingDeletion` evento.
3. A EventBridge regra invoca o tópico do Amazon SNS.
4. O Amazon SNS envia uma mensagem de notificação por e-mail aos usuários.

> **Note**
>
> Você pode personalizar a mensagem de e-mail para atender às necessidades da sua organização. Recomendamos incluir informações sobre as entidades nas quais a chave do AWS KMS é usada. Isso pode ajudar os usuários a entenderem o impacto da exclusão da chave do AWS KMS. Você também pode agendar uma notificação de lembrete por e-mail enviada um ou dois dias antes da exclusão da chave do AWS KMS.

Automação e escala

O AWS CloudFormation stack implanta todos os recursos e serviços necessários para que esse padrão funcione. Você pode implementar o padrão de forma independente em uma única conta ou usando a AWS CloudFormation StackSets para várias contas independentes ou unidades organizacionais no AWS Organizations.

Ferramentas

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS. O CloudFormation modelo desse padrão descreve todos os recursos da AWS que você deseja e CloudFormation provisiona e configura esses recursos para você.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos e serviços da AWS e encaminha esses dados

para destinos como o AWS Lambda. EventBridge simplifica o processo de criação de arquiteturas orientadas por eventos.

- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.

Código

O código desse padrão está disponível no repositório de desativação e exclusão programada de chaves do AWS KMS do GitHub Monitor AWS KMS.

Épicos

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Clone o repositório de desativação e exclusão programada das chaves do GitHub Monitor AWS KMS em sua máquina local executando o seguinte comando: `git clone https://github.com/aws-samples/aws-kms-deletion-notification`	Administrador da AWS, arquiteto de nuvem
Atualizar os parâmetros do modelo.	Em um editor de código, abra o `Alerting-KMS-Events.yaml` CloudFormation modelo que você clonou do repositório e atualize os seguintes parâmetros:	Administrador da AWS, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	• Para `DestinationEmailAddress`, insira um endereço de e-mail ativo que você planeja usar para receber a notificação do SNS. • Para `SNSTopicName`, digite um nome para o seu tópico do SNS.	
Implante o CloudFormation modelo.	1. Faça login no Console de Gerenciamento da AWS e abra o console do CloudFormation. 2. No painel de navegação, escolha Criar pilha e, em seguida, escolha Com novos recursos (padrão). 3. Na página Identificar recursos, escolha Próximo. 4. Na página Especificar modelo, em Origem do modelo, selecione Carregar um arquivo de modelo. 5. Escolha Escolher arquivo, selecione o **`Alerting-KMS-Events.yaml`** arquivo do seu GitHub repositório clonado e escolha Avançar. 6. Em Nome da pilha, insira o nome da pilha. 7. Selecione Enviar.	Administrador da AWS, arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura de e-mail.	Depois que o CloudFormation modelo for implantado com sucesso, o Amazon SNS envia uma mensagem de confirmação da assinatura para o endereço de e-mail que você forneceu no CloudFormation modelo. Você precisa confirmar sua assinatura para começar a receber as notificações. Para obter mais informações, consulte Confirmar a assinatura no Guia do desenvolvedor do Amazon SNS.	Administrador da AWS, arquiteto de nuvem

Testar a notificação de assinatura.

Tarefa	Descrição	Habilidades necessárias
Desabilitar chaves do AWS KMS.	1. Faça login no Console de Gerenciamento da AWS e abra o Console do AWS KMS. 2. Para alterar a região, escolha o nome da região exibida atualmente e, em seguida, escolha a região para a qual você deseja alternar.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	3. No painel de navegação, escolha Chaves gerenciadas pelo cliente. 4. Marque a caixa de seleção das chaves do AWS KMS que você deseja habilitar ou desabilitar. 5. Para desabilitar a chave do AWS KMS, escolha Ações de chaves e, depois, Desabilitar.	
Validar a assinatura.	Confirme se você recebeu o e-mail de notificação do Amazon SNS.	Administrador da AWS

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Exclua a CloudFormation pilha.	1. Faça login no Console de Gerenciamento da AWS e abra o console do CloudFormation . 2. No painel de navegação, escolha Pilhas. 3. Selecione a pilha que você criou e escolha Excluir.	Administrador da AWS

Recursos relacionados

- AWS CloudFormation (documentação da AWS)

- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- Criar arquiteturas orientadas por eventos na AWS (documentação do AWS Workshop Studio)
- Práticas recomendadas do AWS Key Management Service (whitepaper da AWS)
- Práticas recomendadas de segurança para o AWS Key Management Service (AWS KMS) (Guia do desenvolvedor do AWS KMS)

Mais informações

O Amazon SNS fornece criptografia em trânsito por padrão. Para se alinhar às práticas recomendadas de segurança, você também pode habilitar a criptografia do lado do servidor para o Amazon SNS usando uma chave gerenciada pelo cliente do AWS KMS.

Preserve o espaço IP roteável em projetos de VPC com várias contas para sub-redes sem workload

Criado por Adam Spicer (AWS)

Resumo

A Amazon Web Services (AWS) publicou as melhores práticas que recomendam o uso de sub-redes dedicadas em uma nuvem privada virtual (VPC) para anexos do gateway de trânsito e endpoints do Gateway Load Balancer (para oferecer suporte ao AWS Network Firewall ou dispositivos de terceiros). Essas sub-redes são usadas para conter interfaces de rede elásticas para esses serviços. Se você usa o AWS Transit Gateway e um balanceador de carga do gateway, duas sub-redes são criadas em cada zona de disponibilidade da VPC. Devido à forma como VPCs são projetadas, essas sub-redes extras não podem ser menores que uma máscara /28 e podem consumir um precioso espaço IP roteável que, de outra forma, poderia ser usado para cargas de trabalho roteáveis. Esse padrão demonstra como você pode usar um intervalo de Encaminhamento Entre Domínios Sem Classificação (CIDR) secundário, não roteável para essas sub-redes dedicadas para ajudar a preservar o espaço IP roteável.

Pré-requisitos e limitações

Pré-requisitos

- Estratégia de várias VPCs para espaço IP roteável
- Um intervalo CIDR não roteável para os serviços que você está usando (anexos de gateway de trânsito e balanceador de carga do gateway ou endpoints do Network Firewall)

Arquitetura

Arquitetura de destino

Esse padrão inclui duas arquiteturas de referência: uma arquitetura tem sub-redes para anexos do Transit Gateway (TGW) e um endpoint do Gateway Load Balancer (GWLBe), e a segunda arquitetura tem sub-redes somente para anexos TGW.

Arquitetura 1 – VPC conectada ao TGW com roteamento de entrada para um dispositivo

O diagrama a seguir representa uma arquitetura de referência para uma VPC que abrange duas zonas de disponibilidade. Na entrada, a VPC usa um padrão de roteamento de entrada para

direcionar o tráfego destinado à sub-rede pública para um dispositivo para inspeção do firewall. bump-in-the-wire Um anexo TGW suporta a saída das sub-redes privadas para uma VPC separada.

Esse padrão usa um intervalo CIDR não roteável para a sub-rede do anexo TGW e a sub-rede. GWLBe Na tabela de rotas do TGW, esse CIDR não roteável é configurado com uma rota de buraco negro (estática) usando um conjunto de rotas mais específicas. Se as rotas fossem propagadas para a tabela de rotas do TGW, essas rotas de buraco negro mais específicas se aplicariam.

Neste exemplo, o CIDR roteável /23 é dividido e totalmente alocado às sub-redes roteáveis.

Arquitetura 2 – VPC conectada ao TGW

O diagrama a seguir representa outra arquitetura de referência para uma VPC que abrange duas zonas de disponibilidade. Um anexo TGW oferece suporte ao tráfego de saída (egress) das sub-redes privadas para uma VPC separada. Ele usa um intervalo CIDR não roteável somente para a sub-rede de anexos do TGW. Na tabela de rotas TGW, esse CIDR não roteável é configurado com uma rota blackhole usando um conjunto de rotas mais específicas. Se as rotas fossem propagadas para a tabela de rotas do TGW, essas rotas de buraco negro mais específicas se aplicariam.

Neste exemplo, o CIDR roteável /23 é dividido e totalmente alocado às sub-redes roteáveis.

Ferramentas

Serviços e recursos da AWS

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS. Nesse padrão, a VPC secundária CIDRs é usada para preservar o espaço IP roteável na carga de trabalho. CIDRs
- O roteamento de entrada do gateway da Internet (associações de borda) pode ser usado junto com os endpoints do balanceador de carga do gateway para sub-redes dedicadas não roteáveis.
- O AWS Transit Gateway é um hub central que conecta VPCs redes locais. Nesse padrão, VPCs são conectados centralmente a um gateway de trânsito, e os anexos do gateway de trânsito estão em uma sub-rede dedicada não roteável.
- Os balanceadores de carga do gateway ajudam você a implantar, escalar e gerenciar dispositivos virtuais, como firewalls, sistemas de detecção e prevenção de intrusões e sistemas de inspeção

profunda de pacotes. O gateway atua como um único ponto de entrada e saída para todo o tráfego. Nesse padrão, os endpoints de um balanceador de carga do gateway podem ser usados em uma sub-rede dedicada não roteável.

- O AWS Network Firewall é um serviço gerenciado e monitorado de firewall de rede e detecção e prevenção de intrusões VPCs na nuvem da AWS. Nesse padrão, os endpoints de um firewall podem ser usados em uma sub-rede não roteável dedicada.

Repositório de código

Um runbook e CloudFormation modelos da AWS para esse padrão estão disponíveis no repositório de padrões CIDR secundários GitHub não roteáveis. Você pode usar os arquivos de amostra para configurar um laboratório de trabalho em seu ambiente.

Práticas recomendadas

AWS Transit Gateway

- Use uma sub-rede separada para cada anexo da VPC do gateway.
- Aloque uma sub-rede /28 do intervalo CIDR secundário não roteável para as sub-redes do anexo do gateway de trânsito.
- Em cada tabela de rotas do Transit Gateway, adicione uma rota estática e mais específica para o intervalo CIDR não roteável como um buraco negro.

Balanceador de carga do gateway e roteamento de entrada

- Use o roteamento de entrada para direcionar o tráfego da Internet para os endpoints do balanceador de carga do gateway.
- Use uma sub-rede separada para cada endpoint do balanceador de carga do gateway.
- Aloque uma sub-rede /28 do intervalo CIDR secundário não roteável para as sub-redes de endpoint do balanceador de carga do gateway.

Épicos

Criar VPCs

Tarefa	Descrição	Habilidades necessárias
Determine o intervalo CIDR não roteável.	Determine um intervalo CIDR não roteável que será usado para a sub-rede de anexo do gateway de trânsito e (opcionalmente) para qualquer sub-rede de endpoint do balanceador de carga do gateway ou do Network Firewall. Esse intervalo de CIDR será usado como CIDR secundário para a VPC. Ele não deve ser roteável a partir do intervalo CIDR primário da VPC ou de uma rede maior.	Arquiteto de nuvem
Determine os intervalos de CIDR roteáveis para. VPCs	Determine um conjunto de intervalos CIDR roteáveis que serão usados para o seu. VPCs Esse intervalo de CIDR será usado como o CIDR primário para o seu. VPCs	Arquiteto de nuvem
Criar VPCs.	Crie o seu VPCs e conecte-o ao gateway de trânsito. Cada VPC deve ter um intervalo CIDR primário que seja roteável e um intervalo CIDR secundário que não seja roteável, com base nos intervalos que você determinou nas duas etapas anteriores.	Arquiteto de nuvem

Configurar rotas de blackhole do Transit Gateway

Tarefa	Descrição	Habilidades necessárias
Crie buracos negros não roteáveis CIDRs mais específicos.	Cada tabela de roteamento do gateway de trânsito precisa ter um conjunto de rotas blackhole criadas para as não roteáveis. CIDRs Eles são configurados para garantir que qualquer tráfego do CIDR VPC secundário permaneça não roteável e não vaze para a rede maior. Essas rotas devem ser mais específicas do que o CIDR não roteável definido como CIDR secundário na VPC. Por exemplo, se o CIDR secundário não roteável for 100.64.0.0/26, as rotas do blackhole na tabela de rotas do Transit Gateway deverão ser 100.64.0.0/27 e 100.64.0.32/27.	Arquiteto de nuvem

Recursos relacionados

- Melhores práticas para implantar o balanceador de carga do gateway
- Arquiteturas de inspeção distribuídas com Gateway Load Balancer
- Dia de imersão em redes – – Lab de Internet para o Firewall da VPC
- Melhores práticas de design do gateway de trânsito

Mais informações

O intervalo CIDR secundário não roteável também pode ser útil ao trabalhar com implantações de contêineres em maior escala que exigem um grande conjunto de endereços IP. Você pode usar esse padrão com um gateway NAT privado para usar uma sub-rede não roteável para hospedar suas implantações de contêineres. Para obter mais informações, consulte a postagem de blog Como resolver o esgotamento de IP privado com a solução de NAT privado.

Provisione um produto Terraform AWS Service Catalog usando um repositório de código

Criado pelo Dr. Rahul Sharad Gaikwad (AWS) e Tamilselvan P (AWS)

Resumo

AWS Service Catalog oferece suporte ao provisionamento de autoatendimento com governança para suas HashiCorp configurações do Terraform. Se você usa o Terraform, pode usar o Service Catalog como a única ferramenta para organizar, controlar e distribuir suas configurações do Terraform em grande escala. AWS Você pode acessar os principais recursos do Service Catalog, incluindo catalogação de modelos padronizados e pré-aprovados de infraestrutura como código (IaC), controle de acesso, provisionamento de recursos em nuvem com acesso de privilégios mínimos, controle de versão, compartilhamento com milhares de pessoas e marcação. Contas da AWS Usuários finais, como engenheiros, administradores de banco de dados e cientistas de dados, veem uma lista de produtos e versões aos quais têm acesso e podem implantá-los por meio de uma única ação.

Esse padrão ajuda você a implantar AWS recursos usando o código do Terraform. O código do Terraform no GitHub repositório é acessado por meio do Service Catalog. Usando essa abordagem, você integra os produtos aos seus fluxos de trabalho existentes do Terraform. Os administradores podem criar portfólios do Service Catalog e adicionar AWS Launch Wizard produtos a eles usando o Terraform.

A seguir estão os benefícios dessa solução:

- Devido ao recurso de reversão no Service Catalog, se ocorrer algum problema durante a implantação, você poderá reverter o produto para uma versão anterior.
- Você pode identificar facilmente as diferenças entre as versões do produto. Isso ajuda você a resolver problemas durante a implantação.
- Você pode configurar uma conexão de repositório no Service Catalog, como para GitHub ou GitLab. Você pode fazer alterações no produto diretamente por meio do repositório.

Para obter informações sobre os benefícios gerais do AWS Service Catalog, consulte O que é Service Catalog.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Um GitHub, BitBucket, ou outro repositório que contenha arquivos de configuração do Terraform no formato ZIP.
- AWS Serverless Application Model Interface de linha de comando (AWS SAM CLI), instalada.
- AWS Command Line Interface (AWS CLI), instalado e configurado.
- Vá, instalado.
- Python versão 3.9, instalado. AWS SAM A CLI requer essa versão do Python.
- Permissões para escrever e executar AWS Lambda funções e permissões para acessar e gerenciar produtos e portfólios do Service Catalog.

Arquitetura

O diagrama mostra o seguinte fluxo de trabalho:

1. Quando uma configuração do Terraform está pronta, um desenvolvedor cria um arquivo.zip que contém todo o código do Terraform. O desenvolvedor carrega o arquivo.zip no repositório de código conectado ao Service Catalog.
2. Um administrador associa o produto Terraform a um portfólio no Service Catalog. O administrador também cria uma restrição de lançamento que permite que os usuários finais provisionem o produto.
3. No Service Catalog, os usuários finais iniciam AWS recursos usando a configuração do Terraform. Eles podem escolher a versão do produto a ser implantada.

Ferramentas

Serviços da AWS

- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Service Catalogajuda você a gerenciar centralmente catálogos de serviços de TI aprovados. AWS Os usuários finais podem implantar rapidamente somente os serviços de TI aprovados de que precisam, seguindo as restrições definidas pela organização.

Outros serviços

- Go é uma linguagem de programação de código aberto compatível com o Google.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

Se você precisar de exemplos de configurações do Terraform que você possa implantar por meio do Service Catalog, você pode usar as configurações no repositório GitHub Amazon Macie Organization Setup Using Terraform. O uso das amostras de código neste repositório não é obrigatório.

Práticas recomendadas

- Em vez de fornecer os valores das variáveis no arquivo de configuração do Terraform (`terraform.tfvars`), configure os valores das variáveis ao iniciar o produto por meio do Service Catalog.
- Conceda acesso ao portfólio somente para usuários ou administradores específicos.
- Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Conceder privilégios mínimos e melhores práticas de segurança na documentação AWS Identity and Access Management (IAM).

Épicos

Configure sua estação de trabalho local.

Tarefa	Descrição	Habilidades necessárias
(Opcional) Instale o Docker.	Se você quiser executar as AWS Lambda funções em seu ambiente de desenvolvimento, instale o Docker. Para obter mais informações, consulte Install Docker Engine (Instalar mecanismo do Docker) na documentação do Docker.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Instale o AWS Service Catalog motor para o Terraform.	1. Digite o comando a seguir para clonar o repositór io AWS Service Catalog Engine for Terraform.
	`git clone https://g ithub.com/aws-samp les/service-catalo g-engine-for-terra form-os.git`
	2. Navegue até o diretório raiz do repositório clonado.
	3. Insira o comando da a seguir. Isso instala o motor.
	`run ./bin/bash/ deploy-tre.sh -r`
	O Região da AWS conjunto em seu perfil padrão não é usado durante a instalaçã o automatizada. Em vez disso, você fornece a Região ao executar esse comando.
		DevOps engenheiro, administr ador da AWS

Conecte o GitHub repositório

Tarefa	Descrição	Habilidades necessárias
Crie uma conexão com o GitHub repositório.	1. Faça login no e AWS Management Console, em seguida, abra o console do Developer Tools. Você	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	pode acessar o console do Developer Tools escolhendo um serviço como AWS CodePipeline ou AWS CodeDeploy. 2. No painel de navegação esquerdo, escolha Configurações e, em seguida, escolha Conexões. 3. Escolha Criar conexão. 4. Selecione o repositório em que você mantém o código-fonte do Terraform. Por exemplo, você pode escolher Bitbucket ou GitHub Enterprise Server. GitHub 5. Insira um nome para a conexão e escolha Connect. 6. Quando solicitado, autentique o repositório. Após a conclusão da autenticação, a conexão é criada e o status muda para ativo.	

Crie um produto Terraform no Service Catalog

Tarefa	Descrição	Habilidades necessárias
Crie o produto Service Catalog.	1. Abra o console de AWS Service Catalog. 2. Navegue até a seção Administração e escolha Lista de produtos. 3. Escolha Criar produto. 4. Na página Criar produto, na seção Detalhes do produto, escolha o tipo de produto externo. O Service Catalog usa esse tipo de produto para oferecer suporte aos produtos Terraform Community Edition. 5. Insira um nome e um proprietário para o produto Service Catalog. 6. Selecione Especificar seu repositório de código usando um CodeStar provedor. 7. Insira as seguintes informações para o seu repositório: • Conecte-se ao seu provedor usando Conexões de código da AWS — Selecione a conexão que você criou anteriormente.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	• Repositório — Selecione o repositório. • Filial — Selecione a ramificação. • Caminho do arquivo de modelo — Escolha o caminho em que o arquivo de modelo de código está armazenado. O nome do arquivo deve terminar com `tar.gz`. 8. Em Nome e descrição da versão, forneça informaçõ es sobre a versão do produto. 9. Escolha Criar produto.	

Tarefa	Descrição	Habilidades necessárias
Crie um portfólio.	1. Abra o console de AWS Service Catalog. 2. Navegue até a seção Administração e, em seguida, escolha Portfólios. 3. Escolha Criar portfólio. 4. Insira os seguintes valores: • Portfolio name – `Sample terraform` • Descrição do portfólio – `Sample portfolio for Terraform configurations` • Proprietário — Suas informações de contato, como um endereço de e-mail 5. Escolha Criar.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Adicione o produto Terraform ao portfólio.	1. Abra o console de AWS Service Catalog. 2. Navegue até a seção Administração e escolha Lista de produtos. 3. Selecione o produto Terraform que você criou anteriormente. 4. Escolha Ações e, em seguida, escolha Adicionar produto ao portfólio. 5. Escolha o `Sample terraform` portfólio. 6. Escolha Adicionar produto ao portfólio.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Crie a política de acesso.	1. Abra o console AWS Identity and Access Management (IAM). 2. No painel de navegação, selecione Políticas. 3. No painel de conteúdo, escolha Criar política. 4. Escolha a opção JSON. 5. Insira o exemplo de política JSON em Política de acesso na seção Informações adicionais desse padrão. 6. Escolha Próximo. 7. Na página Revisar e criar, na caixa Nome da política, digite `TerraformResourceCreationAndArtifactAccessPolicy` . 8. Selecione Criar política.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Crie uma política de confiança personalizada.	1. Abra o console do IAM. 2. No painel de navegação, selecione Perfis. 3. Escolha Criar Perfil. 4. Em Tipo de entidade confiável, escolha Política de confiança personalizada. 5. No editor de políticas JSON, insira o exemplo de política JSON em Política de confiança na seção Informações adicionais desse padrão. 6. Escolha Próximo. 7. Em Políticas de permissões, escolha as `TerraformResourceCreationAndArtifactAccessPolicy` que você criou anteriormente. 8. Escolha Próximo. 9. Em Detalhes da função, na caixa Nome da função, insira `SCLaunch-product` . **Important** O nome da função deve começar com `SCLaunch`. 10. Selecione Criar perfil.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Adicione uma restrição de lançamento ao produto Service Catalog.	1. Faça login no AWS Management Console como usuário com permissões administrativas. 2. Abra o console de AWS Service Catalog. 3. No painel de navegação, escolha Portfólios. 4. Escolha o portfólio que você criou anteriormente. 5. Na página Detalhes do portfólio, escolha a guia Restrições e escolha Criar restrição. 6. Em Produto, selecione o produto Terraform que você criou anteriormente. 7. Em Restrição de inicializ ação, em Método, escolha Inserir nome da função. 8. Na caixa Nome da função, insira`SCLaunch-product` . 9. Escolha Criar.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Conceda acesso ao produto.	1. Abra o console de AWS Service Catalog. 2. No painel de navegação, escolha Portfólios. 3. Escolha o portfólio que você criou anteriormente. 4. Escolha a guia Acesso e, em seguida, escolha Conceder acesso. 5. Escolha a guia Funções e, em seguida, selecione a função que deve ter acesso para implantar esse produto. 6. Escolha Conceder acesso.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Lance o produto.	1. Faça login no AWS Management Console como usuário com permissões para implantar o produto Service Catalog. 2. Abra o console de AWS Service Catalog. 3. No painel de navegação, escolha Produtos. 4. Escolha o produto que você criou anteriormente e, em seguida, escolha Lançar produto. 5. Insira o nome do produto e defina os parâmetros necessários. 6. Escolha Lançar produto.	DevOps engenheiro

Verificar a implantação

Tarefa	Descrição	Habilidades necessárias
Valide a implantação.	Há duas máquinas de AWS Step Functions estado para o fluxo de trabalho de provision amento do Service Catalog: • `ManageProvisionedProductStateMachine` — O Service Catalog invoca essa máquina de estado ao provisionar um novo produto Terraform e	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ao atualizar um produto provisionado existente do Terraform. • `TerminateProvisionedProductStateMachine` — O Service Catalog invoca essa máquina de estado ao encerrar um produto provisionado existente do Terraform. Você verifica os registros da máquina de `ManageProvisionedProductStateMachine` estado para confirmar se o produto foi provisionado. 1. Faça login no e AWS Management Console, em seguida, abra o AWS Step Functions console. 2. No painel de navegação esquerdo, escolha Máquinas estaduais. 3. Escolha`ManageProvisionedProductStateMachine` . 4. Na lista Execuções, insira a ID do produto provisionado para localizar a execução.	

Tarefa	Descrição	Habilidades necessárias
	Note Os nomes dos buckets de back-end do arquivo de estado começam com `sc-terraform-engine-state-`. 5. Valide se todos os recursos necessários foram criados na conta.	

Limpe a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Exclua produtos provisionados.	1. Faça login no AWS Management Console como usuário com permissões para implantar o produto Service Catalog. 2. Abra o console de AWS Service Catalog. 3. No painel de navegação à esquerda, escolha Produtos provisionados. 4. Selecione o produto que você criou. 5. Na lista Ações, escolha Encerrar.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	6. Na caixa de texto de confirmação, insira `eterminate` , em seguida, escolha Encerrar produto provisionado. 7. Repita essas etapas para encerrar todos os produtos provisionados.	

Tarefa	Descrição	Habilidades necessárias
Remova o AWS Service Catalog motor do Terraform.	1. Faça login no AWS Management Console como usuário com permissões administrativas. 2. Abra o console do Amazon Simple Storage Service (Amazon S3). 3. No painel de navegação, escolha Buckets. 4. Selecione o `sc-terraform-engine-logging-XXXX` bucket. 5. Escolha Vazio. 6. Repita as etapas de 4 a 5 para os seguintes buckets: • `sc-terraform-engine-state-XXXX` • `terraform-engine-bootstrap-XXXX` 7. Abra o AWS CloudFormation console e, em seguida, confirme que você está no correto Região da AWS. 8. No painel de navegação à esquerda, escolha Pilhas. 9. Selecione e`SAM-TRE`, em seguida, escolha Excluir. Espere até que a pilha seja excluída. 10. Selecione e`Bootstrap-TRE`, em seguida, escolha	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Excluir. Espere até que a pilha seja excluída.	

Recursos relacionados

AWS documentação

- Começando com um produto Terraform

Documentação do Terraform

- Instalação do Terraform
- Configuração de back-end do Terraform
- Documentação do Terraform AWS Provider

Mais informações

Política de acesso

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        },
        {
            "Action": [
                "s3:CreateBucket*",
                "s3:DeleteBucket*",
```

```
                "s3:Get*",
                "s3:List*",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Política de confiança

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GivePermissionsToServiceCatalog",
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
```

```
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account_id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
TerraformExecutionRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogExternalParameterParserRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogTerraformOSParameterParserRole*"
                    ]
                }
            }
        }
    ]
}
```

Registrar várias contas da AWS com um único endereço de e-mail usando o Amazon SES

Criado por Joe Wozniak (AWS) e Shubhangi Vishwakarma (AWS)

Resumo

Esse padrão descreve como você pode dissociar endereços de e-mail reais do endereço de e-mail associado a um Conta da AWS. Contas da AWS exija que um endereço de e-mail exclusivo seja fornecido no momento da criação da conta. Em algumas organizações, a equipe que gerencia Contas da AWS deve assumir a responsabilidade de gerenciar vários endereços de e-mail exclusivos com sua equipe de mensagens. Isso pode ser difícil para grandes organizações que gerenciam muitas Contas da AWS. Além disso, se seu sistema de e-mail não permitir endereçamento adicional ou subendereçamento, conforme definido em Filtragem de e-mail do Sieve: extensão de subendereço (RFC 5233) — adicionando um sinal de adição (+) e um identificador ao final da parte local do endereço de e-mail, como `admin+123456789123@example.com` —esse padrão pode ajudar a superar essa limitação.

Esse padrão fornece uma solução exclusiva de venda automática de endereços de e-mail que permite que Conta da AWS os proprietários associem um endereço de e-mail a vários Contas da AWS. Os endereços de e-mail reais dos Conta da AWS proprietários são então associados a esses endereços de e-mail gerados em uma tabela. A solução lida com todos os e-mails recebidos para as contas de e-mail exclusivas, pesquisa o proprietário de cada conta e, em seguida, encaminha todas as mensagens recebidas para o proprietário.

Pré-requisitos e limitações

Pré-requisitos

- Acesso administrativo a um Conta da AWS.
- Acesso a um ambiente de desenvolvimento.
- (Opcional) A familiaridade com AWS Cloud Development Kit (AWS CDK) os fluxos de trabalho e com a linguagem de programação Python ajudará você a solucionar quaisquer problemas ou fazer modificações.

Limitações

- O tamanho geral do endereço de e-mail vendido é de 64 caracteres. Para obter detalhes, consulte CreateAccounta referência AWS Organizations da API.

Versões do produto

- Node.js versão 12.7.0 ou superior
- Python 3.9 ou superior
- Pacotes Python pip e virtualenv
- AWS CDK versão 2.23.0 ou posterior
- Docker 20.10.x ou superior

Arquitetura

Pilha de tecnologias de destino

- AWS CloudFormation pilha
- AWS Lambda funções
- Regra e conjunto de regras do Amazon Simple Email Service (Amazon SES)
- AWS Identity and Access Management Funções e políticas (IAM)
- O bucket do Amazon Simple Storage Service (Amazon S3) e política de bucket.
- AWS Key Management Service (AWS KMS) chave e política chave
- Tópico e política de tópico do Amazon Simple Notification Service (Amazon SNS)
- Tabela do Amazon DynamoDB

Arquitetura de destino

Esse diagrama mostra dois fluxos:

- Fluxo de venda automática de endereços de e-mail: no diagrama, o fluxo de venda automática de endereços de e-mail (seção inferior) geralmente inicia com uma solução de venda automática de contas ou automação externa, ou é invocado manualmente. Na solicitação, uma função do Lambda é chamada com uma carga que contém os metadados necessários. A função usa essas informações para gerar um nome de conta e endereço de e-mail exclusivos, armazenar em um

banco de dados do DynamoDB e retornar os valores ao chamador. Esses valores podem então ser usados para criar um novo Conta da AWS (normalmente usando AWS Organizations).

- Fluxo de encaminhamento de e-mail: esse fluxo é ilustrado na seção superior do diagrama anterior. Quando um Conta da AWS é criado usando o e-mail da conta gerado a partir do fluxo de venda automática de endereços de e-mail, AWS envia vários e-mails, como confirmação do registro da conta e notificações periódicas, para esse endereço de e-mail. Seguindo as etapas desse padrão, você configura seu Conta da AWS com o Amazon SES para receber e-mails de todo o domínio. Essa solução configura regras de encaminhamento que permitem ao Lambda processar todos os e-mails recebidos, verificar se o endereço T0 está na tabela do DynamoDB e encaminhar a mensagem para o endereço de e-mail do proprietário da conta. O uso desse processo dá aos proprietários da conta a capacidade de associar várias contas a um endereço de e-mail.

Automação e escala

Esse padrão usa o AWS CDK para automatizar totalmente a implantação. A solução usa serviços AWS gerenciados que serão (ou podem ser configurados para) escalar automaticamente para atender às suas necessidades. As funções do Lambda podem exigir configuração adicional para atender às suas necessidades de escalabilidade. Para obter mais informações, consulte Entendendo a escalabilidade da função Lambda na documentação do Lambda.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir com os serviços da AWS por meio de comandos em seu shell de linha de comando.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.

- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- Amazon Simple Email Service (Amazon SES): ajuda você a enviar e receber e-mails usando seus próprios endereços de e-mail e domínios.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Ferramentas necessárias para implantação

- Ambiente de desenvolvimento com acesso AWS CLI e IAM ao seu Conta da AWS. Para obter detalhes, consulte os links na seção Recursos relacionados.
- Em seu sistema de desenvolvimento, instale o seguinte:
  - Ferramenta de linha de comando do Git, disponível no site de downloads do Git.
  - O AWS CLI para configurar as credenciais de acesso para o. AWS CDK Para obter mais informações, consulte a documentação do AWS CLI.
  - Python versão 3.9 ou posterior, disponível no site de downloads do Python.
  - Pacotes Python pip e virtualenv. Para obter instruções de instalação, consulte a documentação do pip e a documentação do virtualenv.
  - Node.js versão 12.7.0 ou posterior. Para obter instruções de instalação, consulte a documentação do Node.js.
  - AWS CDK versão 2.23.0 ou posterior. Para obter instruções de instalação, consulte a AWS CDK documentação.
  - Docker versão 20.10.x ou posterior. Para obter instruções de instalação, consulte a documentação do Docker.

Código

O código desse padrão está disponível no repositório de e-mail de GitHub Conta da AWS fábrica.

Épicos

Aloque um ambiente de implantação de destino

Tarefa	Descrição	Habilidades necessárias
Identifique ou crie um Conta da AWS.	Identifique um existente ou novo Conta da AWS ao qual você tenha acesso administrativo total para implantar a solução de e-mail.	Administrador da AWS, administrador de nuvem
Configurar um ambiente de implantação.	Configure um ambiente de implantação fácil de usar e configure dependências seguindo estas etapas: 1. Configure seu ambiente de desenvolvimento com as ferramentas listadas na seção Ferramentas. 2. Clone a base de código do repositório de e-mail de GitHub Conta da AWS fábrica em seu ambiente de desenvolvimento usando o comando: `git clone https://github.com/aws-samples/aws-account-factory-email` 3. No `requirements.txt` arquivo (na raiz do repositório), atualize a linha que começa com `aws-cdk-lib==` para corresponder	AWS DevOps, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	à versão da AWS CDK que está sendo executada em seu ambiente. Para identificar a versão, use o `cdk --version` comando.	

Configurar um domínio verificado

Tarefa	Descrição	Habilidades necessárias
Identifique e aloque um domínio.	A funcionalidade de encaminhamento de e-mail requer um domínio dedicado. Identifique e aloque um domínio ou subdomínio que você possa verificar com o Amazon SES. Esse domínio deve estar disponível para receber e-mails recebidos no local em Conta da AWS que a solução de encaminhamento de e-mail está implantada. Requisitos de domínio: • O domínio deve ser um domínio ou subdomínio padrão. • O domínio deve ser solucionável externamente por DNS, pois será usado para receber e-mails de fora da organização.	Administrador de nuvem, administrador de rede, administrador de DNS

Tarefa	Descrição	Habilidades necessárias
Verificar o domínio.	Verifique se o domínio identificado pode ser usado para aceitar e-mails recebidos. Complete as instruções em Como verificar seu domínio para recebimento de e-mails do Amazon SES na documentação do Amazon SES. Isso exigirá coordenação com a pessoa ou equipe responsável pelos registros DNS do domínio.	Desenvolvedor de aplicativos, AWS DevOps
Configurar registros MX.	Configure seu domínio com registros MX que apontam para os endpoints do Amazon SES em sua região Conta da AWS . Para obter mais informações, consulte Publicação de um registro MX para recebimento de e-mails do Amazon SES na documentação do Amazon SES.	Administrador de nuvem, administrador de rede, administrador de DNS

Implemente a solução de venda e encaminhamento de e-mails

Tarefa	Descrição	Habilidades necessárias
Modifique os valores padrão em`cdk.json`.	Edite alguns dos valores padrão no arquivo `cdk.json` (na raiz do repositório) para que a solução funcione	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	corretamente após a implantação. 1. Modifique o valor `SES_DOMAIN_NAME` para corresponder ao nome de domínio que você verificou anteriormente. 2. Modifique o valor `ADDRESS_FROM` para incluir o mesmo domínio que está em `SES_DOMAIN_NAME`. A parte local do endereço deve ser determinada pela sua equipe de nuvem. Esse endereço se torna o endereço `FROM` de cada e-mail encaminhado pela solução. 3. Modifique o valor `ADDRESS_ADMIN` para corresponder ao endereço de e-mail para o qual todas as mensagens recebidas que não correspondam serão encaminhadas. Esse valor deve ser um endereço de e-mail válido e operacional.	

Tarefa	Descrição	Habilidades necessárias

Implante a solução de venda e encaminhamento de e-mails.	1. Crie um ambiente virtual Python.
	`python -m venv .venv`
	2. Ative o ambiente virtual Python:
	`source .venv/bin/activate`
	Ou, na plataforma Windows, use:
	`% .venv\Scripts\activate.bat`
	3. Instale todos os requisitos do Python sem erros:
	`pip install -r requirements.txt`
	4. Sintetize o CloudFormation modelo:
	`cdk synth`
	Confirme se não há erros e se o CloudFormation modelo completo contém a saída esperada.
	5. (Opcional) Se você estiver implantando o AWS CDK código na região atual Conta da AWS ou na região
		Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	pela primeira vez, inicializ e o ambiente. Para obter mais informações, consulte AWS CDK Bootstrapping na documentação. AWS CDK
	`cdk bootstrap aws://AWS-ACCOUNT-NUMBER/REGION`
	Substitua `AWS-ACCOUNT-NUMBER` e `REGION` por valores reais.
	6. Implantar a solução.
	`cdk bootstrap`
	`cdk deploy`
	Os comandos de compilaçã o deve ser concluídos sem erros.	

Tarefa	Descrição	Habilidades necessárias
Verificar se a solução foi implantada.	Verificar se a solução foi implantada com sucesso antes de começar o teste: 1. Abra o AWS CloudFormation console e procure uma CloudFormation pilha que contenha o nome `AwsMailFwdStack` . 2. Confirmar se essa pilha `AwsMailFwdStack` tem os seguintes recursos: • Funções do Lambda • Regra e conjunto de regras do Amazon SES • Perfis e políticas do IAM • Bucket do Amazon S3 e política de bucket • AWS KMS chave e política chave • Tópico e política de tópicos do Amazon SNS • Tabela do DynamoDB	Desenvolvedor de aplicativos, AWS DevOps

Verificar se a venda e o encaminhamento de e-mails funcionam conforme o esperado

Tarefa	Descrição	Habilidades necessárias
Verificar se a API está trabalhando.	Nesta etapa, você enviará dados de teste para a API da solução e confirma se a solução produz a saída esperada e se as operações	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	de backend foram executadas conforme o esperado. Execute manualmente a função do Lambda Vend Email usando a entrada de teste. (Para ver um exemplo, consulte o arquivo sample_vend_request.json.) Use um endereço de e-mail válido para `OwnerAddress` . A API deve retornar o nome da conta e o e-mail da conta com os valores esperados.	

Tarefa	Descrição	Habilidades necessárias
Verificar se o e-mail está sendo encaminhado.	Nesta etapa, você enviará um e-mail de teste pelo sistema e verifica se o e-mail foi encaminhado para o destinatário esperado. 1. Obtenha o e-mail da conta na última etapa. 2. Enviar um e-mail para esse endereço com o assunto do teste e o corpo do texto. 3. Confirmar se você recebeu o e-mail no endereço de e-mail do proprietário da conta. 4. Confirmar se o e-mail que você recebeu tem um `FROM` endereço que corresponde à `ADDRESS_FROM` configuração em `cdk.json`. 5. Confirmar se o assunto e o corpo do e-mail recebido são iguais aos da mensagem original enviada.	Desenvolvedor de aplicativos, AWS DevOps

Solução de problemas

Problema	Solução
O sistema não encaminha e-mails conforme o esperado.	Verificar se sua configuração está correta:

Problema	Solução
	1. Você deve ter concluído o processo de verificação do Amazon SES para seu domínio. 2. Seu domínio deve ser configurado corretamente com registros MX apontando para os endpoints do Amazon SES em sua região Conta da AWS . Para obter mais informações, consulte Publicação de um registro MX para recebimento de e-mails do Amazon SES na documentação do Amazon SES. Depois de verificar a configuração do domínio, siga estas etapas: 1. Abra o CloudWatch console da Amazon para a conta e a região em que você implantou a solução e navegue até os grupos de CloudWatch log no painel de navegação. 2. Pesquise na lista de grupos de logs por`SesMailForwardLogGroup` . 3. Investigue os logs desse grupo para ver se algum erro foi gerado durante o processo de venda e encaminhamento de e-mails.

Problema	Solução
Ao tentar implantar a AWS CDK pilha, você recebe um erro semelhante a: “Erro no formato do modelo: tipos de recursos não reconhecidos”	Na maioria das instâncias, essa mensagem de erro significa que a região que você está segmentando não tem todos os serviços da AWS disponíveis. Se você estiver usando uma EC2 instância da Amazon para implantar a solução, você pode ter como alvo uma região diferente da região em que a instância está sendo executada. **Note** Por padrão, o é AWS CDK implantad o na região e na conta que você configurou no AWS CLI. Soluções possíveis: 1. Analise os serviços da AWS por região para investigar se todos os serviços necessários para essa solução (consulte a seção Target technology stack mais abaixo neste padrão) estão no Região da AWS que você está almejando. 2. Se você estiver usando uma EC2 instância e segmentando uma região diferente da região em que sua instância está sendo executada, certifique-se de definir a variável de `AWS_DEFAULT_REGION` ambiente ou definir uma região com a AWS CLI antes de implantar a solução. Para obter mais informações, consulte Configuração de variáveis de ambiente AWS CLI na AWS CLI documentação. Como alternativa, você pode modificar o `app.py` arquivo na raiz

Problema	Solução
	do repositório para incluir uma ID de conta e uma região codificadas seguindo as instruções na documentação dos ambientes .AWS CDK
Ao implementar a solução, você recebe a mensagem de erro: “Falha na implantação: Erro AwsMailFwdStack: SSM parameter /cdk-bootstrap/hnb659fds/version não encontrado. O ambiente foi inicializado? Por favor, execute 'cdk bootstrap'”	Se você nunca implantou nenhum AWS CDK recurso na região que está almejando, primeiro precisará executar o `cdk bootstrap` comando conforme o erro indica. Conta da AWS Se você continuar recebendo esse erro depois de executar o comando bootstrapping, talvez esteja tentando implantar a solução em uma região diferente da região em que seu ambiente de desenvolvimento está sendo executado. Para resolver esse problema, defina a variável de `AWS_DEFAULT_REGION` ambiente ou defina uma região com o AWS CLI antes de implantar a solução. Como alternativa, você pode modificar o `app.py` arquivo na raiz do repositório para incluir uma ID de conta e uma região codificadas seguindo as instruções na documentação dos ambientes.AWS CDK

Recursos relacionados

- Para obter ajuda na instalação do AWS CLI, consulte Instalando ou atualizando para a versão mais recente do AWS CLI.
- Para obter ajuda na configuração do AWS CLI com credenciais de acesso do IAM, consulte Como configurar as configurações do. AWS CLI
- Para obter ajuda com o AWS CDK, consulte Introdução ao AWS CDK.

Mais informações

Custos

Quando você implanta essa solução, o Conta da AWS detentor pode incorrer em custos associados ao uso dos seguintes serviços. É importante entender como esses serviços são cobrados para estar ciente de quaisquer possíveis cobranças. Para obter mais informações sobre definição de preço, veja as seguintes páginas:

- Definição de preços do Amazon SES
- Definição de preços do Amazon S3
- AWS KMS preços
- AWS Lambda preços
- Preços do Amazon DynamoDB

Configure a resolução de DNS para redes híbridas em um ambiente de conta única da AWS

Criado por Abdullahi Olaoye (AWS)

Resumo

Esse padrão descreve como configurar uma arquitetura de Sistema de Nomes de Domínio (DNS) totalmente híbrida que permite a resolução de end-to-end DNS de recursos locais, recursos da AWS e consultas de DNS na Internet, sem sobrecarga administrativa. O padrão descreve como configurar as regras de encaminhamento do Amazon Route 53 Resolver que determinam para onde uma consulta ao DNS originada da AWS deve ser enviada, com base no nome do domínio. As consultas ao DNS para recursos on-premises são encaminhadas para solucionadores de DNS on-premises. As consultas ao DNS para recursos da AWS e consultas ao DNS da Internet são resolvidas pelo Route 53 Resolver.

Esse padrão cobre a resolução de DNS híbrido em um ambiente de conta única da AWS. Para obter informações sobre como configurar consultas ao DNS de saída em um ambiente de várias contas da AWS, consulte o padrão Configurar a resolução de DNS para redes híbridas em um ambiente da AWS com várias contas.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da AWS
- Uma nuvem privada virtual (VPC) na conta da AWS.
- Uma conexão de rede entre o ambiente on-premises e a sua VPC, por meio da AWS Virtual Private Network (AWS VPN) ou do AWS Direct Connect
- Endereços IP dos seus solucionadores de DNS on-premises (acessíveis a partir da sua VPC)
- Nome de domínio/subdomínio a ser encaminhado aos solucionadores on-premises (por exemplo, onprem.mydc.com)
- Nome de domínio/subdomínio para a zona hospedada privada da AWS (por exemplo, myvpc.cloud.com)

Arquitetura

Pilha de tecnologias de destino

- Zona hospedada privada do Amazon Route 53
- Amazon Route 53 Resolver
- Amazon VPC
- AWS VPN ou Direct Connect

Arquitetura de destino

Ferramentas

- O Amazon Route 53 Resolver facilita a nuvem híbrida para clientes corporativos ao permitir uma resolução perfeita de consultas ao DNS em toda a sua nuvem híbrida. Você pode criar endpoints de DNS e regras de encaminhamento condicional para resolver namespaces DNS entre seu data center local e seu. VPCs
- A zona hospedada privada do Amazon Route 53 é um contêiner que contém informações sobre como você deseja que o Route 53 responda às consultas de DNS para um domínio e seus subdomínios em um ou mais VPCs que você cria com o serviço Amazon VPC.

Épicos

Configurar uma zona hospedada privada

Tarefa	Descrição	Habilidades necessárias
Crie uma zona hospedada privada do Route 53 para um nome de domínio reservado da AWS, como myvpc.cloud.com.	Essa zona contém os registros DNS dos recursos da AWS que devem ser resolvidos no ambiente on-premises. Para obter instruções, consulte Como criar uma zona hospedada privada na documentação do Route 53.	Admin de rede, admin do sistema
Associe a zona hospedada privada à sua VPC.	Para permitir que os recursos em sua VPC resolvam registros DNS nessa zona	Admin de rede, admin do sistema

Tarefa	Descrição	Habilidades necessárias
	hospedada privada, você deve associar sua VPC à zona hospedada. Para obter instruções, consulte Como criar uma zona hospedada privada na documentação do Route 53.	

Configurar endpoints do Route 53 Resolver

Tarefa	Descrição	Habilidades necessárias
Criar um endpoint de entrada.	O Route 53 Resolver usa o endpoint de entrada para receber consultas ao DNS de solucionadores DNS on-premises. Para obter instruções, consulte Encaminhando consultas de DNS de entrada para você na documentação do VPCs Route 53. Anote o endereço IP do endpoint de entrada.	Admin de rede, admin do sistema
Crie um endpoint de saída	O Route 53 Resolver usa o endpoint de saída para enviar consultas ao DNS para solucionadores DNS on-premises. Para obter instruções, consulte Como encaminhar consultas ao DNS de saída para sua rede na documentação do Route 53. Anote o ID do endpoint de saída.	Admin de rede, admin do sistema

Configure uma regra de encaminhamento e associe à sua VPC

Tarefa	Descrição	Habilidades necessárias
Crie uma regra para o domínio no on-premises	Essa regra instruirá o Route 53 Resolver a encaminhar qualquer consulta ao DNS para domínios on-premises (como onprem.mydc.com) para solucionadores de DNS on-premises. Para criar essa regra, você precisará dos endereços IP dos soluciona dores de DNS on-premises e do ID do endpoint de saída do Route 53 Resolver. Para obter instruções, consulte Como gerenciar regras de encaminhamento na documentação do Route 53.	Admin de rede, admin do sistema
Associe a regra de encaminha mento à sua VPC.	Para que a regra de encaminhamento entre em vigor, você deve associar a regra à sua VPC. O Route 53 Resolver então leva a regra em consideração ao resolver um domínio. Para obter instruções, consulte Como gerenciar regras de encaminhamento na documentação do Route 53.	Admin de rede, admin do sistema

Configurar solucionadores de DNS on-premises

Tarefa	Descrição	Habilidades necessárias
Configure o encaminhamento condicional nos soluciona dores de DNS on-premises.	Para que as consultas ao DNS sejam enviadas para a zona hospedada privada do Route 53 a partir do ambiente on-premises, você deve configurar o encaminhamento condicional nos soluciona dores de DNS on-premis es. Isso instrui os soluciona dores de DNS a encaminha r todas as consultas ao DNS para o domínio da AWS (por exemplo, para myvpc.clo ud.com) para o endereço IP do endpoint de entrada do Route 53 Resolver.	Admin de rede, admin do sistema

Teste a end-to-end resolução do DNS

Tarefa	Descrição	Habilidades necessárias
Teste a resolução de DNS da AWS para o ambiente on-premises.	Em um servidor na VPC, execute uma consulta ao DNS para um domínio on-premis es (como server1.onprem.myd c.com).	Admin de rede, admin do sistema
Teste a resolução de DNS para o ambiente on-premises.	Em um servidor on-premises, execute a resolução de DNS para um domínio da AWS (como server1.myvpc.clou d.com).	Admin de rede, admin do sistema

Recursos relacionados

- Gerenciamento de DNS centralizado da nuvem híbrida com o Amazon Route 53 e o AWS Transit Gateway (blog de redes e entrega de conteúdo da AWS)
- Simplifique o gerenciamento de DNS em um ambiente de várias contas com o Route 53 Resolver (blog de segurança da AWS)
- Trabalhando com zonas hospedadas privadas (documentação do Route 53)
- Conceitos básicos do Route 53 Resolver (documentação do Route 53 Resolver)

Configure bots de UiPath RPA automaticamente na Amazon EC2 usando a AWS CloudFormation

Criado pelo Dr. Rahul Sharad Gaikwad (AWS) e Tamilselvan P (AWS)

Resumo

Esse padrão explica como você pode implantar bots de automação robótica de processos (RPA) em instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Ele usa um pipeline do EC2 Image Builder para criar uma Amazon Machine Image (AMI) personalizada. Uma AMI é uma imagem de máquina virtual (VM) pré-configurada que contém o sistema operacional (OS) e o software pré-instalado para implantar instâncias. EC2 Esse padrão usa CloudFormation modelos da AWS para instalar a edição UiPath Studio Community na AMI personalizada. UiPath é uma ferramenta de RPA que ajuda você a configurar robôs para automatizar suas tarefas.

Como parte dessa solução, as instâncias EC2 do Windows são iniciadas usando a AMI básica e o aplicativo UiPath Studio é instalado nas instâncias. O padrão usa a ferramenta Microsoft System Preparation (Sysprep) para duplicar uma instalação personalizada do Windows. Depois disso, ele remove as informações do host e cria uma AMI final da instância. Em seguida, você pode executar as instâncias sob demanda usando a AMI final com suas próprias convenções de nomenclatura e configuração de monitoramento.

> **Note**
>
> Esse padrão não fornece nenhuma informação sobre o uso de bots de RPA. Para obter essas informações, consulte a UiPath documentação. Você também pode usar esse padrão para configurar outros aplicativos de bot RPA personalizando as etapas de instalação com base em seus requisitos.

Esse padrão fornece as seguintes automações e benefícios:

- Implantação e compartilhamento de aplicativos: você pode criar a Amazon EC2 AMIs para implantação de aplicativos e compartilhá-los em várias contas por meio de um pipeline do EC2 Image Builder, que usa CloudFormation modelos da AWS como scripts de infraestrutura como código (IaC).

- EC2 Provisionamento e escalabilidade da Amazon: os modelos de CloudFormation IaC fornecem sequências personalizadas de nomes de computadores e automação de junção do Active Directory.
- Observabilidade e monitoramento: o padrão configura os CloudWatch painéis da Amazon para ajudar você a monitorar as EC2 métricas da Amazon (como uso de CPU e disco).
- Benefícios da RPA para sua empresa: a RPA melhora a precisão porque os robôs podem realizar tarefas atribuídas de forma automática e consistente. A RPA também aumenta a velocidade e a produtividade porque remove operações que não agregam valor e lida com atividades repetitivas.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões do AWS Identity and Access Management (IAM) para implantação de modelos CloudFormation
- Políticas do IAM para configurar a distribuição de AMI entre contas com o EC2 Image Builder

Arquitetura

1. O administrador fornece a AMI básica do Windows no `ec2-image-builder.yaml` arquivo e implanta a pilha no CloudFormation console.
2. A CloudFormation pilha implanta o pipeline do EC2 Image Builder, que inclui os seguintes recursos:
   - `Ec2ImageInfraConfiguration`
   - `Ec2ImageComponent`
   - `Ec2ImageRecipe`
   - `Ec2AMI`
3. O pipeline do EC2 Image Builder inicia uma EC2 instância temporária do Windows usando a AMI básica e instala os componentes necessários (nesse caso, o UiPath Studio).
4. O EC2 Image Builder remove todas as informações do host e cria uma AMI do Windows Server.
5. Você atualiza o `ec2-provisioning yaml` arquivo com a AMI personalizada e executa várias EC2 instâncias com base em seus requisitos.

6. Você implanta a macro Count usando um CloudFormation modelo. Essa macro fornece uma propriedade Count para CloudFormation recursos para que você possa especificar facilmente vários recursos do mesmo tipo.
7. Você atualiza o nome da macro no CloudFormation `ec2-provisioning.yaml` arquivo e implanta a pilha.
8. O administrador atualiza o arquivo `ec2-provisioning.yaml` com base nos requisitos e inicia a pilha.
9. O modelo implanta EC2 instâncias com o aplicativo UiPath Studio.

Ferramentas

Serviços da AWS

- CloudFormationA AWS ajuda você a modelar e gerenciar recursos de infraestrutura de forma automatizada e segura.
- CloudWatchA Amazon ajuda você a observar e monitorar recursos e aplicativos na AWS, no local e em outras nuvens.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade computacional segura e redimensionável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- EC2 O Image Builder simplifica a criação, o teste e a implantação de máquinas virtuais e imagens de contêineres para uso na AWS ou localmente.
- EventBridgeA Amazon ajuda você a criar aplicativos orientados por eventos em grande escala na AWS, em sistemas existentes ou em aplicativos de software como serviço (SaaS).
- O AWS Identity and Access Management (IAM) ajuda você a controlar de modo seguro o acesso a recursos da AWS. Com o IAM, é possível gerenciar, de maneira centralizada, permissões que controlam quais recursos da AWS os usuários poderão acessar. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.
- O AWS Lambda é um serviço computacional com tecnologia sem servidor e orientado a eventos que permite executar o código em praticamente qualquer tipo de aplicativo ou serviço de backend sem o provisionamento ou gerenciamento de servidores. Você chama as funções do Lambda a partir de mais de 200 serviços da AWS e aplicativos de SaaS e pagar somente pelo que usar.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

- O AWS Systems Manager Agent (SSM Agent) ajuda o Systems Manager a atualizar, gerenciar e configurar EC2 instâncias, dispositivos periféricos, servidores locais e máquinas virtuais ()VMs.

Repositórios de códigos

O código desse padrão está disponível na configuração do bot GitHub UiPath RPA usando o CloudFormation repositório. O padrão também usa uma macro que está disponível no repositório de CloudFormation macros da AWS.

Práticas recomendadas

- A AWS lança um novo Windows AMIs todo mês. Elas contêm os drivers, agentes de execução e patches do SO mais recentes. Recomendamos utilizar o AMI mais recente ao executar novas instâncias ou ao criar suas próprias imagens personalizadas.
- Aplique todos os patches de segurança disponíveis para Windows ou Linux durante a criação de imagens.

Épicos

Implementar um pipeline de imagens para a imagem base

Tarefa	Descrição	Habilidades necessárias
Configure um pipeline do EC2 Image Builder.	1. Clone a configuração do bot UiPath RPA usando o CloudFormation repositório ou baixe o `ec2-image-builder.yaml` modelo do repositório. 2. Faça login no Console de Gerenciamento da AWS e abra o CloudFormation console da AWS. 3. Selecione Criar pilha. 4. Na seção Specify template (Especificar modelo)	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	escolha Upload a template file (Fazer upload de um arquivo de modelo). 5. Localize e carregue o modelo `ec2-image-builder.yaml` do seu computador e escolha Próximo. 6. Forneça os parâmetros de entrada para a pilha ou aceite os valores padrão. Escolha Próximo. **Note** O número e os valores dos parâmetros podem variar dependendo dos valores de entrada. 7. Opcionalmente, configure as opções de pilha e escolha Próximo. 8. Revise os detalhes da sua pilha. 9. No final da tela, marque a caixa de seleção para reconhecer os recursos e, em seguida, escolha Enviar. 10. Monitore o progresso da pilha. Quando o status	

Tarefa	Descrição	Habilidades necessárias
	estiver `CREATE_COMPLETE`, a implantação estará pronta.	
Veja as configurações do EC2 Image Builder.	As configurações do EC2 Image Builder incluem configuração de infraestrutura, configurações de distribuição e configurações de verificação de segurança. Para ver as configurações: 1. Abra o console do EC2 Image Builder. 2. No painel de navegação, navegue até várias configurações do Image Builder. **Note** Como prática recomendada, você deve fazer qualquer atualização no EC2 Image Builder somente por meio do CloudFormation modelo.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Visualize o pipeline de imagens.	Para ver o pipeline de imagens implantado: 1. No console do EC2 Image Builder, escolha Image pipelines no painel de navegação. 2. Selecione o pipeline de imagens que você criou. 3. Veja os detalhes de configuração das imagens de saída, da receita da imagem, da configura ção da infraestrutura, das configurações de distribuição, EventBridge das regras e das tags da Amazon.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Veja os logs do Image Builder.	EC2 Os registros do Image Builder são agregados em grupos de CloudWatch registros. Para ver os logins CloudWatch: 1. Abra o console de CloudWatch . 2. No painel de navegação, selecione Logs, Grupos de log. 3. Escolha o nome do grupo de registros. EC2 Os registros do Image Builder são agregados no grupo `/aws/imagebuilder/XXX` de registros. 4. Verifique os logs mais recentes no respectivo fluxo de logs para ver se há erros encontrados ao executar o pipeline de imagens. EC2 Os registros do Image Builder também são armazenados em um bucket do S3. Para visualizar os logs no bucket: 1. Abra o console Amazon S3. 2. Na lista Buckets (Buckets), escolha o nome do bucket. Os logs são agregados no	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	bucket do S3 `<stack-name>-XXXXXX` .	
Faça upload do UiPath arquivo em um bucket do S3.	1. Baixe o `.msi` arquivo para o UiPath Studio no local https://download.uipath.com/UiPathStudioCommunity/.msi. 2. Faça upload do arquivo em um bucket do S3. 3. Atualize o nome do bucket e a chave do arquivo no modelo `ec2-image-builder.yaml` , na seção de dados do usuário, linha número 310.	AWS DevOps

Implantar e testar a macro Count

Tarefa	Descrição	Habilidades necessárias
Implantar a macro Count.	1. Clone ou baixe a CloudFormation macro Count. 2. Navegue para a pasta `Count`. 3. Você precisará de um bucket S3 para armazenar os CloudFormation artefatos. Se você ainda não tiver um bucket do S3, crie um com o nome `aws s3 mb s3://<bucket name>`.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	4. Empacote o modelo de macro Count. O modelo usa o AWS Serverless Application Model (SAM), portanto, ele deve ser transformado antes que você possa implantá-lo.
	
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket <your bucket name here> \ --output-template-file packaged.yaml`
	
	Por exemplo:
	
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket count-macro-ec2 \ --output-template-file packaged.yaml`
	
	5. Implante o modelo empacotado para criar uma CloudFormation pilha.
	
	`aws cloudformation deploy \ --stack-name Count-macro \`	

Tarefa	Descrição	Habilidades necessárias
	`--template-file packaged.yaml \ --capabilities CAPABILITY_IAM` Se você quiser usar o console, siga as instruções no épico anterior ou na CloudFormation documentação.	
Testar a macro Count.	Para testar os recursos da macro, tente iniciar o modelo de exemplo fornecido com a macro. `aws cloudformation deploy \ --stack-name Count-test \ --template-file test.yaml \ --capabilities CAPABILITY_IAM`	DevOps engenheiro

Implante a CloudFormation pilha para provisionar instâncias com a imagem personalizada

Tarefa	Descrição	Habilidades necessárias
Implante o modelo de EC2 provisionamento da Amazon.	Para implantar o EC2 Image Pipeline usando CloudFormation: 1. Baixe o `ec2-provisioning.yaml` modelo do GitHub repositório ou localize-o em seu	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	computador se você clonou o repositório. 2. Abra o console de CloudFormation . 3. Repita as etapas do primeiro épico (ou siga as instruções na CloudFormation documentação) para implantar `ec2-provisioning.yaml` .	
Veja as EC2 configurações da Amazon.	As EC2 configurações da Amazon incluem configurações de segurança, rede, armazenamento, verificações de status, monitoramento e tags. Para ver essas configurações: 1. Abra o EC2 console da Amazon. 2. No painel de navegação, escolha Instâncias e, em seguida, selecione a EC2 instância que foi criada pelo modelo de EC2 provisionamento da Amazon. 3. No resumo da instância , selecione as guias para ver as EC2 configurações correspondentes da Amazon.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Veja o CloudWatch painel.	1. Abra o console de CloudWatch . 2. No painel de navegação, escolha Painéis. 3. Escolha o painel que tem o nome da sua pilha. **Note** Depois de provisionar a pilha, leva tempo para preencher o painel com métricas. O painel fornece essas métricas:`CPUUtilization` , `DiskUtilization` , `MemoryUtilization` , `NetworkIn` , `NetworkOut` , `StatusCheckFailed` .	AWS DevOps
Visualizar métricas personalizadas para uso de memória e disco.	1. No CloudWatch console, escolha Painéis. 2. No painel de navegação, escolha Métricas, Todas as métricas. 3. Escolha namespaces personalizados,. CWAgent	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Visualizar os alarmes para uso da memória e do disco.	1. No CloudWatch console, no painel de navegação, escolha Painéis. 2. Escolha Todos os alarmes.	AWS DevOps
Verificar a regra do ciclo de vida do snapshot.	1. Abra o EC2 console da Amazon. 2. No painel de navegação , escolha Gerenciador de ciclo de vida. 3. Verifique as configurações do ciclo de vida da AMI.	AWS DevOps

Excluir o ambiente (opcional)

Tarefa	Descrição	Habilidades necessárias
Exclua as pilhas.	Quando seu PoC ou projeto piloto estiver concluído, recomendamos que você exclua as pilhas criadas para garantir que não seja cobrado por esses recursos. 1. Abra o CloudFormation console da AWS. 2. No painel de navegação, escolha Pilhas e selecione uma ou as duas pilhas que você criou anteriormente e que deseja excluir. A pilha deve estar em execução no momento.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	3. No painel de detalhes da pilha, escolha Excluir. 4. Quando solicitado, escolha Excluir pilha. **Important** A operação de exclusão da pilha não pode ser interrompida após o início. A pilha continua para o estado `DELETE_IN_PROGRESS` . Se houver falha ao excluir, a pilha estará no estado `DELETE_FAILED` . Para obter soluções, consulte Excluir falhas na pilha na documentação de solução de CloudFormation problemas da AWS. Para obter informações sobre como proteger pilhas de serem excluídas acidentalmente, consulte Como proteger uma pilha de ser excluída na documentação da AWS. CloudFormation	

Solução de problemas

Problema	Solução
Ao implantar o modelo de EC2 provision amento da Amazon, você recebe o erro: Received malformed response from transform 123xxxx: :Count.	Esse é um problema conhecido. (Veja a solução personalizada e o PR no repositório de CloudFormation macros da AWS.) Para corrigir esse problema, abra o console do AWS Lambda e atualize `index.py` com o conteúdo do GitHub repositório.

Recursos relacionados

GitHub repositórios

- UiPath Configuração do bot RPA usando CloudFormation
- CloudFormation Macro de contagem

Referências da AWS

- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação)
- Solução de problemas CloudFormation (CloudFormation documentação)
- Monitore métricas de memória e disco para EC2 instâncias da Amazon (EC2 documentação da Amazon)
- Como posso usar o CloudWatch agente para visualizar métricas do Monitor de Desempenho em um servidor Windows? (Artigo do AWS ref:Post)

Referências adicionais

- UiPath documentação
- Definindo o nome do host em uma SysPreped AMI (postagem no blog de Brian Beach)
- Como faço para que o Cloudformation reprocesse um modelo usando uma macro quando os parâmetros mudam? (Estouro de pilha)

Configure uma PeopleSoft arquitetura altamente disponível na AWS

Criado por Ramanathan Muralidhar (AWS)

Resumo

Quando você migra suas PeopleSoft cargas de trabalho para a AWS, a resiliência é um objetivo importante. Ele garante que seu PeopleSoft aplicativo esteja sempre altamente disponível e seja capaz de se recuperar rapidamente de falhas.

Esse padrão fornece uma arquitetura para seus PeopleSoft aplicativos na AWS para garantir alta disponibilidade (HA) nos níveis de rede, aplicativo e banco de dados. Ele usa um banco de dados Amazon Relational Database Service (Amazon RDS) para Oracle ou Amazon RDS para SQL Server para a camada de banco de dados. Essa arquitetura também inclui serviços da AWS, como Amazon Route 53, instâncias Linux do Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Storage (Amazon EBS), Amazon Elastic File System (Amazon EFS) e um Application Load Balancer, além de ser escalável.

PeopleSoftA Oracle fornece um conjunto de ferramentas e aplicativos para gerenciamento da força de trabalho e outras operações comerciais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um PeopleSoft ambiente com as licenças necessárias para configurá-lo na AWS
- Uma nuvem privada virtual (VPC) configurada em sua conta da AWS com os seguintes recursos:
  - Selecione pelo menos duas Zonas de disponibilidade.
  - Uma sub-rede pública e três sub-redes privadas em cada zona de disponibilidade
  - Um gateway NAT e um gateway da Internet
  - Tabelas de rotas para cada sub-rede para rotear o tráfego
  - Listas de controle de acesso à rede (rede ACLs) e grupos de segurança definidos para ajudar a garantir a segurança do PeopleSoft aplicativo de acordo com os padrões da sua organização

Limitações

- Esse padrão fornece uma solução de alta disponibilidade (HA). Ele não oferece suporte a cenários de recuperação de desastres (DR). Na rara ocorrência de toda a região da AWS para a implementação de HA cair, o aplicativo ficará indisponível.

Versões do produto

- PeopleSoft aplicativos executando PeopleTools 8.52 e versões posteriores

Arquitetura

Arquitetura de destino

O tempo de inatividade ou interrupção de seu aplicativo de PeopleSoft produção afeta a disponibilidade do aplicativo e causa grandes interrupções em seus negócios.

Recomendamos que você projete seu aplicativo de PeopleSoft produção para que ele esteja sempre altamente disponível. Você pode conseguir isso eliminando pontos únicos de falha, adicionando pontos confiáveis de cruzamento ou failover e detectando falhas. O diagrama a seguir ilustra uma arquitetura de HA para PeopleSoft a AWS.

Essa implantação de arquitetura usa o Amazon RDS for Oracle como PeopleSoft banco de dados EC2 e instâncias que estão sendo executadas no Red Hat Enterprise Linux (RHEL). Você também pode usar o Amazon RDS para SQL Server como banco de dados Peoplesoft.

Essa arquitetura inclui os seguintes componentes:

- O Amazon Route 53 é usado como servidor de nomes de domínio (DNS) para rotear solicitações da Internet para o PeopleSoft aplicativo.
- O AWS WAF ajuda você a se proteger contra exploits comuns da web e bots que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos. O AWS Shield Avançado (não ilustrado) oferece uma proteção muito mais ampla.
- Um Application Load Balancer equilibra a carga do tráfego HTTP e HTTPS com roteamento avançado de solicitações direcionado aos servidores da web.
- Os servidores web, servidores de aplicativos, servidores de agendamento de processos e servidores Elasticsearch que oferecem suporte ao PeopleSoft aplicativo são executados em várias zonas de disponibilidade e usam o Amazon Auto EC2 Scaling.

- O banco de dados usado pelo PeopleSoft aplicativo é executado no Amazon RDS em uma configuração Multi-AZ.
- O compartilhamento de arquivos usado pelo PeopleSoft aplicativo é configurado no Amazon EFS e é usado para acessar arquivos entre instâncias.
- As Amazon Machine Images (AMI s) são usadas pelo Amazon EC2 Auto Scaling para garantir que PeopleSoft os componentes sejam clonados rapidamente quando necessário.
- O gateway NAT conecta as instâncias em uma sub-rede privada a serviços fora da VPC, e tgarantir que externos não iniciem uma conexão com essas instâncias.
- Um gateway da Internet é um componente da VPC horizontalmente dimensionado, redundante e altamente disponível que permite a comunicação entre a VPC e a Internet.
- Os bastion hosts na sub-rede pública fornecem acesso aos servidores na sub-rede privada a partir de uma rede externa, como a Internet ou a rede on-premises. Os bastion hosts fornecem acesso controlado e seguro aos servidores nas sub-redes privadas.

Detalhes de arquitetura

O PeopleSoft banco de dados está alojado em um banco de dados Amazon RDS for Oracle (ou Amazon RDS for SQL Server) em uma configuração Multi-AZ. O atributo Multi-AZ do Amazon RDS replica as atualizações de bancos de dados em duas zonas de disponibilidade para aumentar a durabilidade e a disponibilidade. O Amazon RDS passará automaticamente para o modo de standby para manutenção planejada e interrupções não planejadas.

A PeopleSoft web e a camada intermediária são instaladas nas EC2 instâncias. Essas instâncias estão espalhadas por várias zonas de disponibilidade e vinculadas por um grupo do Auto Scaling. Isso garante que esses componentes estejam sempre altamente disponíveis. Um número mínimo de instâncias necessárias é mantido para garantir que o aplicativo esteja sempre disponível e possa ser escalado quando necessário.

Recomendamos que você use um tipo de EC2 instância da geração atual para as EC2 instâncias OEM. Os tipos de instância da geração atual, como instâncias criadas no AWS Nitro System, oferecem suporte a máquinas virtuais de hardware (HVMs). É necessário que o HVM aproveite AMIs as vantagens da rede aprimorada e também ofereça maior segurança. As EC2 instâncias que fazem parte de cada grupo do Auto Scaling usam sua própria AMI ao substituir ou ampliar as instâncias. Recomendamos que você selecione os tipos de EC2 instância com base na carga que você deseja que seu PeopleSoft aplicativo manipule e nos valores mínimos recomendados pela Oracle para seu PeopleSoft aplicativo e sua PeopleTools versão. Para obter mais informações sobre os requisitos de hardware e software, consulte o site de suporte da Oracle.

A PeopleSoft web e o nível intermediário compartilham uma montagem do Amazon EFS para compartilhar relatórios, arquivos de dados e (se necessário) o `PS_HOME` diretório. O Amazon EFS é configurado com destinos de montagem em cada zona de disponibilidade por motivos de desempenho e custo.

Um Application Load Balancer é provisionado para suportar o tráfego que acessa o PeopleSoft aplicativo e balanceia a carga do tráfego entre os servidores web em diferentes zonas de disponibilidade. Um Application Load Balancer é um dispositivo de rede que fornece HA em pelo menos duas zonas de disponibilidade. Os servidores web distribuem o tráfego para diferentes servidores de aplicativos usando uma configuração de balanceamento de carga. O balanceamento de carga entre o servidor web e o servidor de aplicativos garante que a carga seja distribuída uniformemente entre as instâncias e ajuda a evitar gargalos e interrupções no serviço devido a instâncias sobrecarregadas.

O Amazon Route 53 é usado como serviço de DNS para rotear o tráfego da Internet para o Application Load Balancer. O Amazon Route 53 é um web service DNS altamente disponível e dimensionável.

Detalhes do HA

- Bancos de dados: o atributo Multi-AZ do Amazon RDS opera dois bancos de dados em várias zonas de disponibilidade com replicação síncrona. Isso cria um ambiente altamente disponível com failover automático. O Amazon RDS tem detecção de eventos de failover e inicia um failover automático quando esses eventos ocorrem. Você também pode iniciar o failover manual por meio da API do Amazon RDS. Para obter uma explicação detalhada, consulte a postagem do blog Amazon RDS Under The Hood: Multi-AZ. O failover é contínuo e o aplicativo se reconecta automaticamente ao banco de dados quando isso acontece. No entanto, qualquer trabalho do agendador de processos durante o failover gera erros e precisa ser reenviado.
- PeopleSoft servidores de aplicativos: os servidores de aplicativos estão espalhados por várias zonas de disponibilidade e têm um grupo de Auto Scaling definido para eles. Se uma instância falhar, o grupo do Auto Scaling a substituirá imediatamente por uma instância íntegra que é clonada da AMI do modelo do servidor de aplicativos. Especificamente, o jolt pooling está ativado. Portanto, quando uma instância do servidor de aplicativos fica inativa, as sessões são transferidas automaticamente para outro servidor de aplicativos, e o grupo do Auto Scaling automaticamente cria outra instância, abre o servidor do aplicativo e o registra na montagem do Amazon EFS. O servidor de aplicativos recém-criado é adicionado automaticamente aos servidores web usando o `PSSTRSETUP.SH` script nos servidores web. Isso garante que o servidor de aplicativos esteja sempre altamente disponível e se recupere rapidamente de falhas.

- Agendadores de processos: os servidores dos agendadores de processos estão espalhados por várias zonas de disponibilidade e têm um grupo do Auto Scaling definido para eles. Se uma instância falhar, o grupo do Auto Scaling a substituirá imediatamente por uma instância íntegra que é clonada da AMI do modelo do servidor de processos. Especificamente, quando uma instância do agendador de processos fica inativa, o grupo do Auto Scaling ativa automaticamente outra instância e ativa o agendador de processos. Todos os trabalhos que estavam em execução quando a instância falhou devem ser reenviados. Isso garante que o agendador de processos esteja sempre altamente disponível e se recupere rapidamente de falhas.
- Servidores Elasticsearch: os servidores Elasticsearch têm um grupo do Auto Scaling definido para eles. Se uma instância falhar, o grupo do Auto Scaling a substituirá imediatamente por uma instância íntegra que é clonada da AMI do modelo do servidor Elasticsearch. Especificamente, quando uma instância do Elasticsearch fica inativa, o Application Load Balancer que atende às solicitações detecta a falha e para de enviar tráfego para ela. O grupo do Auto Scaling ativa automaticamente outra instância e ativa a instância do Elasticsearch. Quando a instância do Elasticsearch é reativada, o Application Load Balancer detecta que ela está íntegra e começa a enviar solicitações para ela novamente. Isso garante que o servidor Elasticsearch esteja sempre altamente disponível e se recupere rapidamente de falhas.
- Servidores web: os servidores web têm um grupo do Auto Scaling definido para eles. Se uma instância falhar, o grupo do Auto Scaling a substituirá imediatamente por uma instância íntegra que é clonada da AMI do modelo de servidor web. Especificamente, quando uma instância do servidor web fica inativa, o Application Load Balancer que atende às solicitações detecta a falha e para de enviar tráfego para ela. O grupo do Auto Scaling ativa automaticamente outra instância e ativa a instância do servidor web. Quando a instância do web server é reativada, o Application Load Balancer detecta que ela está íntegra e começa a enviar solicitações para ela novamente. Isso garante que o servidor web esteja sempre altamente disponível e se recupere rapidamente de falhas.

Ferramentas

Serviços da AWS

- Os Application Load Balancers distribuem o tráfego de entrada do aplicativo em vários destinos, como EC2 instâncias, em várias zonas de disponibilidade.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (Amazon). EC2

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.

Práticas recomendadas

Melhores práticas operacionais

- Quando você executa PeopleSoft na AWS, use o Route 53 para rotear o tráfego da Internet e localmente. Use a opção de failover para redirecionar o tráfego para o site de recuperação de desastres (DR) se a instância de banco de dados primária não estiver disponível.
- Sempre use um Application Load Balancer na frente do PeopleSoft ambiente. Isso garante que a carga do tráfego seja balanceada para os servidores da web de forma segura.
- Nas configurações do grupo-alvo do Application Load Balancer, verifique se a aderência está ativada com um cookie gerado pelo balanceador de carga.

> **Note**
>
> Talvez seja necessário usar um cookie baseado em aplicativo se você usar login único (SSO) externo. Isso garante que as conexões sejam consistentes entre os servidores web e os servidores de aplicativos.

- Para um aplicativo PeopleSoft de produção, o tempo limite de inatividade do Application Load Balancer deve corresponder ao que está definido no perfil da web que você usa. Isso evita que as sessões do usuário expirem na camada do balanceador de carga.
- Para um aplicativo PeopleSoft de produção, defina a contagem de reciclagem do servidor de aplicativos para um valor que minimize os vazamentos de memória.
- Se você estiver usando um banco de dados do Amazon RDS para seu aplicativo de PeopleSoft produção, conforme descrito neste padrão, execute-o no formato Multi-AZ para obter alta disponibilidade.

- Se seu banco de dados estiver sendo executado em uma EC2 instância para seu aplicativo PeopleSoft de produção, certifique-se de que um banco de dados em espera esteja sendo executado em outra zona de disponibilidade para alta disponibilidade.
- Para DR, certifique-se de que seu banco de dados ou EC2 instância do Amazon RDS tenha um modo de espera configurado em uma região da AWS separada do banco de dados de produção. Isso garante que, em caso de desastre na região, você possa mudar o aplicativo para outra região.
- Para DR, usar o Amazon Elastic Disaster Recovery para configurar componentes no nível do aplicativo em uma região separada dos componentes de produção. Isso garante que, em caso de desastre na região, você possa mudar o aplicativo para outra região.
- Use o Amazon EFS (para requisitos moderados de E/S) ou o Amazon FSx (para requisitos altos de E/S) para armazenar seus PeopleSoft relatórios, anexos e arquivos de dados. Isso garante que o conteúdo seja armazenado em um local central e seja acessado de qualquer lugar dentro da infraestrutura.
- Use a Amazon CloudWatch (básica e detalhada) para monitorar os recursos da Nuvem AWS que seu PeopleSoft aplicativo está usando quase em tempo real. Isso garante que você receba alertas sobre problemas instantaneamente e possa resolvê-los rapidamente antes que afetem a disponibilidade do ambiente.
- Se você estiver usando um banco de dados do Amazon RDS como banco de dados, use o PeopleSoft Enhanced Monitoring. Esse atributo fornece acesso a mais de 50 métricas, incluindo CPU, memória, E/S do sistema de arquivos e E/S de disco.
- Use CloudTrail a AWS para monitorar chamadas de API nos recursos da AWS que seu PeopleSoft aplicativo está usando. Isso ajuda você a realizar análises de segurança, rastreamento de alterações de recursos e auditoria de conformidade.

Práticas recomendadas de segurança

- Para proteger seu PeopleSoft aplicativo contra explorações comuns, como injeção de SQL ou cross-site scripting (XSS), use o AWS WAF. Considere usar o AWS Shield Avançado para serviços personalizados de detecção e mitigação.
- Adicione uma regra ao Application Load Balancer para redirecionar automaticamente o tráfego de HTTP para HTTPS e ajudar a proteger seu aplicativo. PeopleSoft
- Configure um grupo de segurança separado para o Application Load Balancer. Esse grupo de segurança deve permitir somente tráfego de entrada HTTPS/HTTP e nenhum tráfego de saída. Isso garante que somente o tráfego pretendido seja permitido e ajuda a proteger seu aplicativo.

- Use sub-redes privadas para os servidores de aplicativos, servidores web e banco de dados, e use gateways NAT para tráfego de saída da Internet. Isso garante que os servidores que oferecem suporte ao aplicativo não possam ser acessados publicamente, ao mesmo tempo em que fornece acesso público somente aos servidores que precisam dele.
- Use diferentes VPCs para executar seus ambientes PeopleSoft de produção e não produção. Use o AWS Transit Gateway, o emparelhamento de VPC ACLs, a rede e os grupos de segurança para controlar o fluxo de tráfego entre as VPCs e, se necessário, seu datacenter local.
- Seguir o princípio do privilégio mínimo Conceda acesso aos recursos da AWS usados pelo PeopleSoft aplicativo somente para usuários que realmente precisam deles. Conceder somente os privilégios mínimos necessários para executar uma tarefa. Para obter mais informações, consulte o pilar Segurança do AWS Well-Architected Framework.
- Sempre que possível, use o AWS Systems Manager para acessar as EC2 instâncias que o PeopleSoft aplicativo usa.

Práticas recomendadas de confiabilidade

- Ao usar um Application Load Balancer, registre um único destino para cada zona de disponibilidade ativada. Isso torna o balanceador de carga mais eficaz.
- Recomendamos que você tenha três endereços distintos URLs para cada ambiente de PeopleSoft produção: um URL para acessar o aplicativo, um para servir ao agente de integração e outro para visualizar relatórios. Se possível, cada URL deve ter seus próprios servidores web e servidores de aplicativos dedicados. Esse design ajuda a tornar seu PeopleSoft aplicativo mais seguro, pois cada URL tem uma funcionalidade distinta e acesso controlado. Também minimiza o escopo do impacto se os serviços subjacentes falharem.
- Recomendamos que você configure verificações de integridade nos grupos-alvo do balanceador de carga do seu PeopleSoft aplicativo. As verificações de saúde devem ser realizadas nos servidores da Web em vez das EC2 instâncias que executam esses servidores. Isso garante que, se o servidor web falhar ou a EC2 instância que hospeda o servidor web cair, o Application Load Balancer reflita essas informações com precisão.
- Para um aplicativo PeopleSoft de produção, recomendamos que você distribua os servidores web em pelo menos três zonas de disponibilidade. Isso garante que o PeopleSoft aplicativo esteja sempre altamente disponível, mesmo que uma das zonas de disponibilidade fique inativa.
- Para um aplicativo PeopleSoft de produção, habilite jolt pooling (). `joltPooling=true` Isso garante que seu aplicativo passe para outro servidor de aplicativos se um servidor estiver inativo para fins de correção ou devido a uma falha na VM.

- Para um aplicativo PeopleSoft de produção, `DynamicConfigReload` defina como 1. Essa configuração é suportada na PeopleTools versão 8.52 e posterior. Ele adiciona novos servidores de aplicativos ao servidor web dinamicamente, sem reiniciar os servidores.
- Para minimizar o tempo de inatividade ao aplicar PeopleTools patches, use o método de implantação azul/verde para suas configurações de inicialização de grupo do Auto Scaling para servidores web e de aplicativos. Para obter mais informações, consulte a visão geral das opções de implantação no whitepaper da AWS.
- Use o AWS Backup para fazer backup do seu PeopleSoft aplicativo na AWS. O AWS Backup é um serviço econômico, totalmente gerenciado e baseado em políticas que simplifica a proteção de dados em grande escala.

Práticas recomendadas de desempenho

- Encerre o SSL no Application Load Balancer para obter o desempenho ideal do ambiente, PeopleSoft a menos que sua empresa exija tráfego criptografado em todo o ambiente.
- Crie endpoints VPC de interface para serviços da AWS, como o Amazon Simple Notification Service (Amazon SNS) CloudWatch, para que o tráfego seja sempre interno. Isso é econômico e ajuda a manter seu aplicativo seguro.

Melhores práticas de otimização de custos

- Marque todos os recursos usados pelo seu PeopleSoft ambiente e ative as tags de alocação de custos. Essas tags ajudam você a visualizar e gerenciar seus custos de recursos.
- Para um aplicativo PeopleSoft de produção, configure grupos de Auto Scaling para os servidores web e os servidores de aplicativos. Isso mantém um número mínimo de servidores web e de aplicativos para dar suporte ao seu aplicativo. Você pode usar as políticas de grupo do Auto Scaling para aumentar e reduzir os servidores conforme necessário.
- Use alarmes de cobrança para receber alertas quando os custos excederem um limite de orçamento especificado por você.

Melhores práticas de sustentabilidade

- Use a infraestrutura como código (IaC) para manter seus PeopleSoft ambientes. Isso ajuda você a criar ambientes consistentes e manter o controle de mudanças.

Épicos

Migre seu PeopleSoft banco de dados para o Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de sub-redes de banco de dados.	No console do Amazon RDS, no painel de navegação, escolha Grupos de sub-redes e, em seguida, crie um grupo de sub-redes de banco de dados do Amazon RDS com sub-redes em várias zonas de disponibilidade. Isso é necessário para o banco de dados do Amazon RDS ser executado em uma configuração Multi-AZ.	Administrador de nuvem
Criar o banco de dados do Amazon RDS	Crie um banco de dados do Amazon RDS em uma zona de disponibilidade da região da AWS que você selecionou para o ambiente de PeopleSoft HA. Ao criar o banco de dados do Amazon RDS, certifique-se de selecionar a opção Multi-AZ (Criar uma instância em espera) e o grupo de sub-rede do banco de dados que você criou na etapa anterior. Para obter mais informações, consulte a documentação do Amazon RDS.	Administrador de nuvem, administrador de banco de dados Oracle

Tarefa	Descrição	Habilidades necessárias
Migre seu PeopleSoft banco de dados para o Amazon RDS.	Migre seu PeopleSoft banco de dados existente para o banco de dados do Amazon RDS usando o AWS Database Migration Service (AWS DMS). Para obter mais informações sobre , consulte documentação de AWS DMS o post do blog da AWS Migrar bancos de dados do Oracle com tempo de inatividade quase zero usando o DMS.	Administrador de nuvem, PeopleSoft DBA

Configure o sistema de arquivos do Amazon EFS

Tarefa	Descrição	Habilidades necessárias
Crie um sistema de arquivos.	No console do Amazon EFS, crie um sistema de arquivos e monte destinos para cada zona de disponibilidade. Para obter instruções, consulte a Documentação do Amazon EFS. Quando o sistema de arquivos tiver sido criado, anote o nome DNS. Você usará essas informações ao montar o sistema de arquivos.	Administrador de nuvem

Configure seu PeopleSoft aplicativo e sistema de arquivos

Tarefa	Descrição	Habilidades necessárias
Execute uma EC2 instância.	Execute uma EC2 instância para seu PeopleSoft aplicativo. Para obter instruções, consulte a EC2 documentação da Amazon. • Em Nome, digite `APP_TEMPLATE` . • Para ter imagens do sistema operacional, escolha Red Hat. • Em Tipo de instância, escolha o tipo de instância apropriado para seu PeopleSoft aplicativo. Para obter mais informações, consulte Detalhes da arquitetura na seção Arquitetura.	Administrador de nuvem, PeopleSoft administrador
Instale PeopleSoft na instância.	Instale seu PeopleSoft aplicativo e PeopleTools na EC2 instância que você criou. Para obter instruções, consulte a documentação do Oracle.	Administrador de nuvem, PeopleSoft administrador
Criar o servidor de aplicativos.	Crie o servidor do aplicativo para o modelo AMI e certifique-se de que ele se conecte com sucesso ao banco de dados do Amazon RDS.	Administrador de nuvem, PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias

Monte o sistema de arquivos do Amazon EFS.	Faça login na EC2 instância como usuário root e execute os seguintes comandos para montar o sistema de arquivos do Amazon EFS em uma pasta chamada `PSFTMNT` no servidor.
	`sudo su -`
	`mkdir /psftmnt`
	`cat /etc/fstab`
	Adicione a linha a seguir ao arquivo `/etc/fstab` . Use o nome DNS que você anotou ao criar o sistema de arquivos.
	`fs-09e064308f11453 88.efs.us-east-1.a mazonaws.com:/ / psftmnt nfs4 nfsvers=4 .1,rsize=1048576,w size=1048576,hard, timeo=600,retrans= 2,noresvport,_netdev 0 0`
	`mount -a`
		Administrador de nuvem, PeopleSoft administrador

Verificar permissões	Certifique-se de que a `PSFTMNT` pasta tenha as permissões adequadas para que o PeopleSoft usuário possa acessá-la adequadam ente.	Administrador de nuvem, PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias
Criar instâncias adicionais.	Repita as etapas anteriores neste épico para criar instâncias de modelo para o agendador de processos, o servidor web e o servidor Elasticsearch. Nomeie essas instâncias `PRCS_TEMPLATE` `WEB_TEMPLATE` , `SRCH_TEMPLATE` e. Para o servidor web, `joltPooling=true` defina `DynamicConfigReload=1` e.	Administrador de nuvem, PeopleSoft administrador

Crie scripts para configurar servidores

Tarefa	Descrição	Habilidades necessárias

Crie um script para instalar o servidor do aplicativo.	Na EC2 `APP_TEMPLATE` instância da Amazon, como PeopleSoft usuário, crie o seguinte script. Nomeie `appstart.sh` e coloque no `PS_HOME` diretório. Você usará esse script para abrir o servidor do aplicativo e também registrar o nome do servidor na montagem do Amazon EFS.
	`#!/bin/ksh`
	`. /usr/homes/hcmdemo/.profile.`
	`psadmin -c configure -d HCMDEMO`
		PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias
	`psadmin -c parallelb oot -d HCMDEMO touch /psftmnt/`echo $HOSTNAME`	
Crie um script para instalar o servidor do agendador de processos.	Na EC2 PRCS_TEMPLATE instância da Amazon, como PeopleSoft usuário, crie o seguinte script. Nomeie `prcsstart.sh` e coloque no PS_HOME diretório. Você usará esse script para abrir o servidor do agendador de processos. `#!/bin/ksh . /usr/homes/hcmdemo/. profile /* The following line ensures that the process scheduler always has a unique name during replaceme nt or scaling activity. */ sed -i "s/.*Prcs ServerName.*/`host name -I | awk -F. '{print "PrcsServ erName=PSUNX"$3$4} '`/" $HOME/appserv/ prcs/*/psprcs.cfg psadmin -p configure -d HCMDEMO psadmin -p start -d HCMDEMO`	PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias

Crie um script para instalar o servidor Elasticsearch.	Na EC2 `SRCH_TEMPLATE` instância da Amazon, como usuário do Elasticsearch, crie o seguinte script. Nomeie `srchstart.sh` e coloque no `HOME` diretório.
	`#!/bin/ksh`
	`/* The following line ensures that the correct IP is indicated in the elasticsearch.yaml file. */`
	`sed -i "s/.*network.host.*/`hostname -I
		awk '{print "host:"$0}'`/" $ES_HOME_DIR/config/elasticsearch.yaml`
		`nohup $ES_HOME_DIR/bin/elasticsearch &`
			PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias
Criar um script para instalar o servidor web.	Na EC2 `WEB_TEMPLATE` instância da Amazon, como usuário do servidor web, crie os seguintes scripts no `HOME` diretório. `renip.sh`: esse script garante que o servidor web tenha o IP correto quando clonado da AMI. `#!/bin/ksh` `hn=`hostname`` `/* On the following` ` line, change the IP` ` with the hostname with` ` the hostname of the web` ` template. */` `for text_file in `find` ` * -type f -exec grep` ` -l '<hostname-of-the-` `web-template>' {} \;` `do` `sed -e 's/<hostn` `ame-of-the-web-tem` `plate>/'$hn'/g'` ` $text_file > temp` `mv -f temp $text_file` `done`  `psstrsetup.sh` : esse script garante que o servidor web use o servidor de aplicativos correto IPs que está sendo executado no momento. Ele tenta se conectar a cada servidor de aplicativos na	PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias
	porta de choque e o adiciona ao arquivo de configuração. `#!/bin/ksh` `c2=""` `for ctr in `ls -1 /psftmnt/*.internal`` `do` `c1=`echo $ctr | awk -F "/" '{print $3}'`` `/* In the following lines, 9000 is the jolt port. Change it if necessary. */` `if nc -z $c1 9000 2> /dev/null; then` `if [[ $c2 = "" ]]; then` `c2="psserver="`echo $c1`":9000"` `else` `c2=`echo $c2`","`echo $c1`":9000"` `fi` `fi` `done` `webstart.sh` : esse script executa os dois scripts anteriores e inicia os servidores web. `#!/bin/ksh` `/* Change the path in the following if necessary. */` `cd /usr/homes/hcmdemo` `./renip.sh` `./psstrsetup.sh`	

Tarefa	Descrição	Habilidades necessárias
	`webserv/peoplesoft/bin/startPIA.sh`	
Adicione uma entrada crontab.	Na EC2 `WEB_TEMPLATE` instância da Amazon, como usuário do servidor web, adicione a seguinte linha ao crontab. Mude o tempo e o caminho para refletir os valores de que você precisa. Essa entrada garante que o servidor web sempre tenha as entradas corretas do servidor de aplicativos no `configuration.properties` arquivo. `* * * * * /usr/homes/hcmdemo/psstrsetup.sh`	PeopleSoft administrador

Crie modelos AMIs de grupos com Auto Scaling

Tarefa	Descrição	Habilidades necessárias
Crie uma AMI para o modelo do servidor de aplicativos.	No EC2 console da Amazon, crie uma imagem AMI da EC2 `APP_TEMPLATE` instância da Amazon. Dê um nome à AMI`PSAPPSRV-SCG-VER1`. Para obter instruções, consulte a EC2 documentação da Amazon.	Administrador de nuvem, PeopleSoft administrador
Crie AMIs para os outros servidores.	Repita a etapa anterior para criar AMIs para o agendador	Administrador de nuvem, PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias
	de processos, o servidor Elasticsearch e o servidor web.	

Criar um modelo de execução para um grupo do Auto Scaling do servidor do aplicativo	Criar um modelo de execução para um grupo do Auto Scaling do servidor do aplicativo Nomear o modelo `PSAPPSRV_TEMPLATE.` No modelo, escolha a AMI que você criou para a `APP_TEMPLATE` instância. Para obter instruções, consulte a EC2 documentação da Amazon.
	• No modelo de execução, selecione o tipo de instância com base nos seus requisitos.
	• No campo Dados do usuário da seção Detalhes avançados, adicione as seguintes entradas. Verifique se o caminho e as informações do usuário estão corretos. Teste o objeto do `appstart.sh` que você criou na etapa anterior.
	`#! /bin/ksh`
	`su -c “/usr/homes/hcmdemo/appstart.sh” - hcmdemo`
		Administrador de nuvem, PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias

Criar um modelo de execução para o grupo do Auto Scaling do servidor do agendador de processos.	Repetir a etapa anterior para criar um modelo de execução para o grupo do Auto Scaling do servidor do agendador de processos. Nomear o modelo `PSPRCS_TEMPLATE` . No modelo, escolha a AMI que você criou para o agendador de processos.
	• No campo Dados do usuário da seção Detalhes avançados, adicione as seguintes entradas. Verifique se o caminho e as informações do usuário estão corretos. Teste o objeto do `prcsstart.sh` que você criou na etapa anterior.
	`#! /bin/ksh`
	`su -c “/usr/hom`
	`es/hcmdemo/prcssta`
	`rt.sh” - hcmdemo`
		Administrador de nuvem, PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias

Criar um modelo de execução para o grupo do Auto Scaling do servidor Elasticsearch.	Repetir as etapas anteriores para criar um modelo de execução para o grupo do Auto Scaling do servidor Elasticsearch. Nomear o modelo `SRCH_TEMPLATE` . No modelo, escolha a AMI que você criou para o servidor de pesquisa.
	• No campo Dados do usuário da seção Detalhes avançados, adicione as seguintes entradas. Verifique se o caminho e as informações do usuário estão corretos. Teste o objeto do `srchstart.sh` que você criou na etapa anterior.
	`#! /bin/ksh`
	`su -c “/usr/hom`
	`es/essearch/srchst`
	`art.sh” - essearch`
		Administrador de nuvem, PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias

Criar um modelo de execução para um grupo do Auto Scaling do servidor web	Repetir as etapas anteriores para criar um modelo de execução para o grupo do Auto Scaling do servidor web. Nomear o modelo `WEB_TEMPLATE` . No modelo, escolha a AMI que você criou para o servidor web.
	• No campo Dados do usuário da seção Detalhes avançados, adicione as seguintes entradas. Verifique se o caminho e as informações do usuário estão corretos. Teste o objeto do `webstart.sh` que você criou na etapa anterior.
	`#! /bin/ksh`
	`su -c “/usr/homes/hcmdemo/webstart.sh” - hcmdemo`
		Administrador de nuvem, PeopleSoft administrador

Criar grupos do Auto Scaling

Tarefa	Descrição	Habilidades necessárias
Criar um grupo do Auto Scaling para o servidor de aplicativos.	No EC2 console da Amazon, crie um grupo de Auto Scaling chamado `PSAPPSRV_ASG` para o servidor do aplicativo usando o `PSAPPSRV_`	Administrador de nuvem, PeopleSoft administrador

Tarefa	Descrição	Habilidades necessárias
	`TEMPLATE` modelo. Para obter instruções, consulte a EC2 documentação da Amazon. • Na página Escolher opções de execução da instância, selecione a VPC correta e, em seguida, selecione várias sub-redes de diferentes zonas de disponibilidade. • Na página Configurar opções avançadas, não selecione um balanceador de carga. • Na página Configura r tamanho do grupo e políticas de escalabilidade, escolha as configurações dependendo da carga para a qual você deseja arquitetar seu sistema e se deseja usar uma política de escalabilidade. Recomenda mos que você defina a capacidade desejada e mínima como 2, no mínimo, para que pelo menos uma instância esteja disponíve l para atender ao tráfego a qualquer momento. Para obter mais informaçõ es sobre as políticas do Auto Scaling, consulte a	

Tarefa	Descrição	Habilidades necessárias
	documentação da Amazon EC2 .	
Criar um grupo do Auto Scaling para os outros servidores.	Repita a etapa anterior para criar grupos do Auto Scaling para o agendador de processos, o servidor Elasticsearch e o servidor web.	Administrador de nuvem, PeopleSoft administrador

Criar e configurar grupos de destino

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de destino para o servidor web.	No EC2 console da Amazon, crie um grupo-alvo para o servidor web. Para obter instruções, consulte a documentação do Elastic Load Balancing. Configure a porta como a porta em que o servidor web está realizando a recepção.	Administrador de nuvem
Configurar verificações de integridade	Confirme se as verificação de integridade têm os valores corretos para refletir suas necessidades comerciais. Para obter mais informações, consulte a documentação do Elastic Load Balancing.	Administrador de nuvem
Criar um grupo de destino para o servidor Elasticsearch.	Repita as etapas anteriore s para criar um grupo-alvo chamado PSFTSRCH para o	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	servidor Elasticsearch e defina a porta correta do Elasticsearch.	
Adicionar grupos de destino aos grupos do Auto Scaling	Abra o grupo do Auto Scaling do servidor web chamado `PSPIA_ASG` criado por você anteriormente. Na guia Load balancing, escolha Editar e adicione o grupo de `PSFTWEB` destino ao grupo do Auto Scaling. Repita essa etapa para que o grupo do Auto Scaling do Elasticsearch `PSSRCH_ASG` para adicionar o grupo de destino`PSFTSRCH` que você criou anteriormente.	Administrador de nuvem
Defina a aderência da sessão.	No grupo-alvo`PSFTWEB`, escolha a guia Atributos, escolha Editar e defina a aderência da sessão. Para o tipo de aderência, escolha Cookie gerado pelo balanceador de carga e defina a duração como 1. Para mais informações, consulte a documentação do Elastic Load Balancing. Repita as etapas para o grupo de destino `PSFTSRCH`.	Administrador de nuvem

Criar e configurar Application Load Balancers

Tarefa	Descrição	Habilidades necessárias
Crie um balanceador de carga para os servidores web.	Crie um Application Load Balancer chamado `PSFTLB` para balancear a carga do tráfego para os servidores web. Para obter instruções, consulte a documentação do Elastic Load Balancing. • Forneça o nome do balanceador de carga. • Para Esquema, escolha Voltado para a internet. • Na seção Mapeamento de rede, selecione a VPC correta e pelo menos duas sub-redes públicas de diferentes zonas de disponibilidade. • Na seção Receptores e roteamento, selecione o grupo de destino `PSFTWEB` e especifique o protocolo e o número da porta corretos.	Administrador de nuvem
Criar um balanceador de carga para os servidores Elasticsearch.	Crie um Application Load Balancer chamado `PSFTSCH` para balancear a carga do tráfego para os servidores Elasticsearch. • Forneça o nome do balanceador de carga.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	• Em Esquema, escolha Interno. • Na seção Mapeamento de rede, selecione a VPC e as sub-redes privadas corretas. • Na seção Receptores e roteamento, selecione o grupo de destino `PSFTSRCH` e especifique o protocolo e o número da porta corretos.	
Configure o Route 53	No console do Amazon Route 53, crie um registro na zona hospedada que atenderá o PeopleSoft aplicativo. Para obter instruções, consulte a Documentação do Amazon Route 53. Isso garante que todo o tráfego passe pelo balanceador de `PSFTLB` carga.	Administrador de nuvem

Recursos relacionados

- PeopleSoft Site da Oracle
- Documentação da AWS

Configure a recuperação de desastres para o Oracle JD Edwards com o EnterpriseOne AWS Elastic Disaster Recovery

Criado por Thanigaivel Thirumalai (AWS)

Resumo

Desastres desencadeados por catástrofes naturais, falhas de aplicativos ou interrupção de serviços prejudicam a receita e causam tempo de inatividade para aplicativos corporativos. Para reduzir as repercussões de tais eventos, o planejamento da recuperação de desastres (DR) é fundamental para empresas que adotam os sistemas de planejamento de recursos EnterpriseOne corporativos (ERP) da JD Edwards e outros softwares de missão crítica e de negócios.

Esse padrão explica como as empresas podem usar o AWS Elastic Disaster Recovery como uma opção de DR para seus aplicativos JD Edwards EnterpriseOne . Também descreve as etapas para usar o failover e o failback do Elastic Disaster Recovery para criar uma estratégia de DR entre regiões para bancos de dados hospedados em uma instância do Amazon Elastic Compute Cloud (EC2Amazon) na Nuvem AWS.

> **Note**
>
> Esse padrão exige que as regiões primária e secundária da implementação de DR entre regiões sejam hospedadas na AWS.

O Oracle JD Edwards EnterpriseOne é uma solução de software ERP integrada para empresas de médio a grande porte em uma ampla variedade de setores.

O AWS Elastic Disaster Recovery minimiza o tempo de inatividade e a perda de dados com a recuperação rápida e confiável de aplicativos locais e baseados na nuvem usando armazenamento acessível, computação e recuperação mínimas. point-in-time

A AWS fornece quatro padrões principais de arquitetura de DR. Este documento se concentra na instalação, configuração e otimização usando a estratégia de piloto leve. Essa estratégia ajuda você a criar um ambiente de DR de baixo custo em que provisiona inicialmente um servidor de replicação para replicar dados do banco de dados de origem e provisiona o servidor de banco de dados real somente quando inicia uma simulação e uma recuperação de DR. Essa estratégia elimina as despesas de manutenção de um servidor de banco de dados na região de DR. Em vez disso, você paga por uma EC2 instância menor que serve como servidor de replicação.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um EnterpriseOne aplicativo JD Edwards executado no Oracle Database ou no Microsoft SQL Server com um banco de dados compatível em um estado de execução em uma instância gerenciada EC2 . Esse aplicativo deve incluir todos os componentes EnterpriseOne básicos do JD Edwards (Enterprise Server, HTML Server e Database Server) instalados em uma região da AWS.
- Um perfil do (IAM) para AWS Identity and Access Management para configurar o serviço do Elastic Disaster Recovery.
- A rede para executar o Elastic Disaster Recovery configurada de acordo com as configurações de conectividade necessárias.

Limitações

- Você pode usar esse padrão para replicar todos os níveis, a menos que o banco de dados esteja hospedado no Amazon Relational Database Service (Amazon RDS). Nesse caso, recomendamos que você use a funcionalidade de cópia entre regiões do Amazon RDS.
- O Elastic Disaster Recovery não é compatível com o CloudEndure Disaster Recovery, mas você pode fazer o upgrade do CloudEndure Disaster Recovery. Para obter mais informações, consulte as Perguntas frequentes na documentação do Elastic Disaster Recovery.
- O Amazon Elastic Block Store (Amazon EBS) limita a taxa na qual você pode tirar snapshots. Você pode replicar um número máximo de 300 servidores em uma única conta da AWS usando o Elastic Disaster Recovery. Para replicar mais servidores, você pode usar várias contas da AWS ou várias regiões da AWS de destino. (Você precisará configurar o Elastic Disaster Recovery separadamente para cada conta e região.) Para obter mais informações, consulte Práticas recomendadas na documentação do Elastic Disaster Recovery.
- As cargas de trabalho de origem (o EnterpriseOne aplicativo e o banco de dados do JD Edwards) devem ser hospedadas nas instâncias. EC2 Esse padrão não é compatível com workloads on-premises ou em outros ambientes de nuvem.
- Esse padrão se concentra nos componentes do JD Edwards EnterpriseOne . Um plano completo de DR e continuidade de negócios (BCP) deve incluir outros serviços essenciais, incluindo:
  - Rede (nuvem privada virtual, sub-redes e grupos de segurança)
  - Active Directory

- Amazon WorkSpaces
- Elastic Load Balancing
- Um serviço de banco de dados gerenciado, como Amazon Relational Database Service (Amazon RDS)

Para obter informações adicionais sobre pré-requisitos, configurações e limitações, consulte a documentação do Elastic Disaster Recovery.

Versões do produto

- Oracle JD Edwards EnterpriseOne (versões compatíveis com Oracle e SQL Server com base nos requisitos técnicos mínimos da Oracle)

Arquitetura

Pilha de tecnologias de destino

- Uma única região e uma única nuvem privada virtual (VPC) para produção e não produção, e uma segunda região para DR
- Zonas de disponibilidade únicas para garantir baixa latência entre servidores
- Um Application Load Balancer que distribui o tráfego de rede para melhorar a escalabilidade e a disponibilidade de seus aplicativos em várias zonas de disponibilidade
- Amazon Route 53 fornecerá a configuração do Sistema de Nomes de Domínio (DNS)
- Amazon fornecerá WorkSpaces aos usuários uma experiência de desktop na nuvem
- Use o Amazon Simple Storage Service (Amazon S3) para armazenar backups, arquivos e objetos
- Amazon CloudWatch para registro, monitoramento e alarmes de aplicativos
- Amazon Elastic Disaster Recovery para recuperação de desastres

Arquitetura de destino

O diagrama a seguir mostra a arquitetura de recuperação de desastres entre regiões para a JD Edwards EnterpriseOne usando o Elastic Disaster Recovery.

Procedimento

Aqui está uma análise de alto nível do processo. Consulte a seção Épicos para obter detalhes.

- A replicação do Elastic Disaster Recovery começa com uma sincronização inicial. Durante a sincronização inicial, o AWS Replication Agent replica todos os dados dos discos de origem para o recurso apropriado na sub-rede da área de armazenamento.
- A replicação contínua continua indefinidamente após a conclusão da sincronização inicial.
- Você revisa os parâmetros de lançamento, que incluem configurações específicas do serviço e um modelo de EC2 lançamento da Amazon, após a instalação do agente e o início da replicação. Quando o servidor de origem é indicado como pronto para recuperação, você pode iniciar as instâncias.
- Quando o Elastic Disaster Recovery emite uma série de chamadas de API para iniciar a operação de lançamento, a instância de recuperação é iniciada imediatamente na AWS de acordo com suas configurações de execução. O serviço ativa automaticamente um servidor de conversão durante a inicialização.
- A nova instância é ativada na AWS após a conclusão da conversão e está pronta para uso. O estado do servidor de origem no momento da execução é representado pelos volumes associados à instância executada. O processo de conversão envolve alterações nos drivers, na rede e na licença do sistema operacional para garantir que a instância seja inicializada de forma nativa na AWS.
- Após o lançamento, os volumes recém-criados não são mais mantidos em sincronia com os servidores de origem. O AWS Replication Agent continua replicando rotineiramente as alterações feitas em seus servidores de origem para os volumes da área de armazenamento, mas as instâncias lançadas não refletem essas alterações.
- Quando você inicia uma nova instância de simulação ou recuperação, os dados são sempre refletidos no estado mais recente que foi replicado do servidor de origem para a sub-rede da área de simulação.
- Quando o servidor de origem é marcado como sendo preparado para recuperação, você pode iniciar instâncias.

> **Note**
>
> O processo funciona nos dois sentidos: para failover de uma região primária da AWS para uma região de DR e para retornar ao site primário, quando ele for recuperado. Você pode se

preparar para o failback revertendo a direção da replicação de dados da máquina de destino para a máquina de origem de uma forma totalmente orquestrada.

Os benefícios desse processo descritos nesse padrão incluem:

- Flexibilidade: os servidores de replicação aumentam e reduzem de escala horizontalmente, com base no conjunto de dados e no tempo de replicação, para que você possa realizar testes de DR sem interromper os workload de origem ou a replicação.
- Confiabilidade: a replicação é robusta, sem interrupções e contínua.
- Automação: essa solução fornece um processo unificado e automatizado para teste, recuperação e failback.
- Otimização de custos: você pode replicar somente os volumes necessários e pagar por eles, e pagar pelos recursos computacionais no local de DR somente quando esses recursos forem ativados. Você pode usar uma instância de replicação com custo otimizado (recomendamos que você use um tipo de instância otimizado para computação) para várias fontes ou uma única fonte com um grande volume do EBS.

Automação e escala

Quando você executa a recuperação de desastres em grande escala, os EnterpriseOne servidores JD Edwards terão dependências de outros servidores no ambiente. Por exemplo:

- Os servidores de EnterpriseOne aplicativos JD Edwards que se conectam a um banco de dados EnterpriseOne compatível com o JD Edwards na inicialização têm dependências desse banco de dados.
- EnterpriseOne Os servidores JD Edwards que exigem autenticação e precisam se conectar a um controlador de domínio na inicialização para iniciar os serviços têm dependências do controlador de domínio.

Por esse motivo, recomendamos que você automatize as tarefas de failover. Por exemplo, você pode usar o AWS Lambda ou o AWS Step Functions para automatizar os scripts de EnterpriseOne inicialização e as alterações do balanceador de carga do JD Edwards para automatizar o processo de failover. end-to-end Para obter mais informações, consulte a publicação Criação de um plano de recuperação de desastres escalável com o AWS Elastic Disaster Recovery no blog.

Ferramentas

Serviços da AWS

- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias. EC2
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Elastic Disaster Recovery minimiza o tempo de inatividade e a perda de dados com a recuperação rápida e confiável de aplicativos locais e baseados na nuvem usando armazenamento acessível, computação e recuperação mínimas. point-in-time
- A Amazon Virtual Private Cloud (Amazon VPC) oferece controle total sobre seu ambiente de rede virtual, incluindo posicionamento de recursos, conectividade e segurança.

Práticas recomendadas

Práticas recomendadas gerais

- Tenha um plano escrito sobre o que fazer no caso de um evento real de recuperação.
- Depois de configurar o Elastic Disaster Recovery corretamente, crie um CloudFormation modelo da AWS que possa criar a configuração sob demanda, caso seja necessário. Determine a ordem na qual os servidores e aplicativos devem ser iniciados e registre isso no plano de recuperação.
- Faça um exercício regular (aplicam-se EC2 as tarifas padrão da Amazon).
- Monitore a integridade da replicação contínua usando o console do Elastic Disaster Recovery ou programaticamente.
- Proteja os point-in-time instantâneos e confirme antes de encerrar as instâncias.
- Crie um perfil do IAM para a instalação do AWS Replication Agent.
- Habilite a proteção contra encerramento para instâncias de recuperação em um cenário real de DR.
- Não use a ação Disconnect from AWS (Desconectar da AWS) no console do Elastic Disaster Recovery para servidores para os quais você lançou instâncias de recuperação, mesmo no caso de um evento real de recuperação. Executar uma desconexão encerra todos os recursos de replicação relacionados a esses servidores de origem, incluindo seus pontos de recuperação point-in-time (PIT).

- Altere a política do PIT para alterar o número de dias para retenção de instantâneos.
- Edite o modelo de lançamento nas configurações de execução do Elastic Disaster Recovery para definir a sub-rede, o grupo de segurança e o tipo de instância corretos para seu servidor de destino.
- Automatize o processo de end-to-end failover usando o Lambda ou o Step Functions para automatizar os scripts de inicialização e as alterações do balanceador de carga do JD Edwards EnterpriseOne .

EnterpriseOne Otimização e considerações do JD Edwards

- Vá PrintQueuepara o banco de dados.
- Vá MediaObjectspara o banco de dados.
- Exclua os registros em log e a pasta temporária dos servidores lógicos e de lote.
- Exclua a pasta temporária do Oracle WebLogic.
- Crie scripts para inicialização após o failover.
- Exclua o tempdb para o SQL Server.
- Exclua o arquivo temporário do Oracle.

Épicos

Execute tarefas e configurações iniciais

Tarefa	Descrição	Habilidades necessárias
Configure a rede de replicaçã o.	Implemente seu Enterpris eOne sistema JD Edwards na região principal da AWS e identifique a região da AWS para DR. Siga as etapas na seção Requisitos de rede de replicação da documentação do Elastic Disaster Recovery para planejar e configurar sua rede de replicação e DR.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Determine o RPO e o RTO.	Identifique o objetivo de tempo de recuperação (RTO) e o objetivo de ponto de recuperação (RPO) para seus servidores de aplicativos e seu banco de dados.	Arquiteto de nuvem, arquiteto de DR
Ative a replicação para o Amazon EFS.	Se aplicável, habilite a replicação da região primária da AWS para a região de DR para sistemas de arquivos compartilhados, como o Amazon Elastic File System (Amazon EFS), usando AWS DataSync, rsync ou outra ferramenta apropriada.	Administrador de nuvem
Gerencie o DNS em caso de DR.	Identifique o processo para atualizar o Sistema de Nomes de Domínio (DNS) durante a simulação de DR ou uma DR real.	Administrador de nuvem
Crie uma perfil do IAM para configuração.	Siga as instruções na seção Elastic Disaster Recovery initialization and permissions (inicialização e permissões do Elastic Disaster Recovery) da documentação do Elastic Disaster Recovery para criar um perfil do IAM para inicializar e gerenciar o serviço da AWS.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Configurar o emparelhamento de VPC.	Certifique-se de que a origem e o destino VPCs estejam emparelhados e acessíveis um ao outro. Para obter instruções de configuração, consulte a documentação do Amazon VPC.	Administrador da AWS

Defina as configurações de replicação do Elastic Disaster Recovery

Tarefa	Descrição	Habilidades necessárias
Inicializar o Elastic Disaster Recovery.	Abra o console do Elastic Disaster Recovery, selecione a região de destino da AWS (onde você replicará dados e iniciará instâncias de recuperação) e, em seguida, selecione Definir configurações de replicação padrão.	Administrador da AWS
Configure os servidores de replicação.	1. No painel Set up replication servers (Configurar servidores de replicação), insira a sub-rede da área de armazenamento e o tipo de instância do servidor de replicação. O tipo de instância `t3.small` é selecionado por padrão. Defina essa configuração com base em seus requisitos e lembre-se de considerar os preços das instâncias.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es, consulte os EC2 preços da Amazon. 2. Na seção Acesso ao serviço, selecione Exibir detalhes para revisar o perfil vinculado ao serviço e as políticas adicionais criadas durante a inicializ ação do serviço. 3. Escolha Próximo.	
Configure volumes e grupos de segurança.	1. No painel Volumes e grupos de segurança, selecione o tipo de volume do EBS para o servidor de replicação e defina a criptografia do Amazon EBS como Padrão. 2. Selecione Always use AWS Elastic Disaster Recovery security group (Sempre use o grupo de segurança do AWS Elastic Disaster Recovery) para que o Elastic Disaster Recovery anexe e monitore automaticamente o grupo de segurança padrão. 3. Escolha Próximo.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Defina configurações adicionais.	1. No painel Additional settings (Configurações adicionais), configure o roteamento e controle de utilização de dados, a política PIT e as tags. • O roteamento e o controle de utilização de dados controlam como os dados fluem do servidor externo para os servidores de replicação. Selecione Use private IP for data replication (Usar IP privado para replicação de dados). Caso contrário, os servidores de replicação receberão automaticamente um IP público e os dados fluirão pela Internet pública. • Na seção Política para um ponto no tempo (PIT), configure uma política de retenção que determine a duração após a qual os instantâneos não são necessários. O período de retenção padrão é de sete dias. • Na seção Tags, adicione tags personalizadas aos recursos criados pelo	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Elastic Disaster Recovery na sua conta da AWS. 2. Selecione Next (Próximo), analise as configurações no próximo painel e selecione Create default (Criar padrão) para criar o modelo padrão.	

Instale o AWS Replication Agent

Tarefa	Descrição	Habilidades necessárias
Criar um perfil do IAM.	Crie um perfil do IAM que contenha a política `AWSElasticDisasterRecoveryAgentInstallationPolicy`. Na seção Select AWS access type (Selecionar tipo de acesso da AWS), habilite o acesso programático. Anote o ID de chave de acesso e a chave de acesso secreta. Você precisará dessas informações durante a instalação do AWS Replication Agent.	Administrador da AWS
Verifique os requisitos.	Verifique e preencha os pré-requisitos na documentação do Elastic Disaster Recovery para instalar o AWS Replication Agent.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Instale o AWS Replication Agent.	Siga as instruções de instalação do seu sistema operacional e instale o AWS Replication Agent.
	• Para Microsoft Windows: baixe os arquivos de instalação e execute o arquivo .exe como administrador. Responda às solicitações para concluir a instalação.
	• Para Linux: copie os comandos a seguir (na ordem apresentada) e cole-os na sua sessão do Secure Shell (SSH). O primeiro comando baixa o instalador e o segundo comando o executa.
	`wget -O ./aws-replication-installer-init.py https://aws-elastic-disaster-recovery-us-west-2.s3.amazonaws.com/latest/linux/aws-replication-installer-init.py`
	`sudo python3 aws-replication-installer-init.py`
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Responda às solicitações para concluir a instalação. **Note** Altere o URL para refletir sua região. Repita essas etapas para o servidor restante.	
Monitore a replicação.	Retorne ao painel Source servers (Servidores de origem) do Elastic Disaster Recovery para monitorar o status da replicação. A sincronização inicial levará algum tempo, dependendo do tamanho da transferência de dados. Quando o servidor de origem estiver totalmente sincroniz ado, o status do servidor será atualizado para Ready (Pronto). Isso significa que um servidor de replicação foi criado na área de armazenam ento e os volumes do EBS foram replicados do servidor de origem para a área de armazenamento.	Administrador da AWS

Definir as configurações de lançamento

Tarefa	Descrição	Habilidades necessárias
Edite as configurações de lançamento.	Para atualizar as configurações de inicialização das instâncias de simulação e recuperação, no console do Elastic Disaster Recovery, selecione o servidor de origem e, em seguida, selecione Actions (Ações), Edit launch settings (Editar configurações de lançamento). Ou você pode escolher suas máquinas de origem de replicação na página Source servers (Servidores de origem) e, em seguida, escolher a guia Launch Settings (Configurações de inicialização). Essa guia tem duas seções: Configurações gerais de lançamento e modelo de EC2 lançamento.	Administrador da AWS
Defina as configurações gerais de lançamento.	Revise as configurações gerais de inicialização de acordo com seus requisitos. • Dimensionamento correto do tipo de instância: se você escolher Básico, o Elastic Disaster Recovery ignora o tipo de instância seleciona do no modelo de EC2 lançamento da Amazon e	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	escolhe automaticamente o tipo de instância com base no sistema operacional, na CPU e na RAM do servidor de origem. • Copiar IP privado: selecione se você deseja que o Elastic Disaster Recovery garanta que o IP privado usado pela simulação ou pela instância de recuperação corresponda ao IP privado usado pelo servidor de origem. Se você escolher Sim, certifique-se de que o intervalo de IP da sub-rede que você definiu no modelo de EC2 lançamento da Amazon inclua o endereço IP privado. Para obter mais informaçõ es, consulte Configurações gerais de lançamento na documentação do Elastic Disaster Recovery.	

Tarefa	Descrição	Habilidades necessárias
Configure o modelo de EC2 lançamento da Amazon.	O Elastic Disaster Recovery usa modelos de EC2 lançamento da Amazon para iniciar instâncias de detalhamento e recuperação para cada servidor de origem. O modelo de lançamento é criado automaticamente para cada servidor de origem que você adiciona ao Elastic Disaster Recovery depois de instalar o AWS Replication Agent. Você deve definir o modelo de EC2 lançamento da Amazon como o modelo de lançamento padrão se quiser usá-lo com o Elastic Disaster Recovery. Para obter mais informações, consulte EC2 Launch Template na documentação do Elastic Disaster Recovery.	Administrador da AWS

Inicie a simulação de recuperação de desastres e o failover

Tarefa	Descrição	Habilidades necessárias
Iniciar simulação	1. No console do Elastic Disaster Recovery, abra a página Source servers (Servidores de origem) e verifique se o status do servidor de origem está como Ready (Pronto).	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	2. Selecione todos os servidores de origem para os quais você deseja realizar a simulação de DR. 3. No menu Iniciar tarefa de recuperação, escolha Iniciar simulação e selecione o instantâneo apropriado point-in-time. Isso inicia um trabalho de recuperaç ão para os servidores de origem selecionados. Você pode monitorar o status do trabalho na guia Recovery job history (Histórico do trabalho de recuperação). A instância de simulação lançada também aparece na página Recovery instances (Instâncias de recuperação). **Note** Outras alteraçõe s no servidor de origem serão sincronizadas com o servidor de replicação, não com a instância de detalhamento.	

Tarefa	Descrição	Habilidades necessárias
	4. Teste e verifique a instância de simulação de DR. 5. Na página Recovery instances (Instâncias de recuperação), selecione a instância de simulação e, em seguida, selecione Actions (Ações), Disconnect from AWS (Desconectar da AWS). Isso exclui o AWS Replication Agent da instância de recuperação e remove todos os recursos associados à instância de recuperação do Elastic Disaster Recovery. 6. Selecione Delete recovery instances (Excluir instâncias de recuperação). Isso exclui a representação da instância do console do Elastic Disaster Recovery e dissocia completamente a instância do serviço Elastic Disaster Recovery. Ela não exclui a EC2 instância subjacente. 7. Encerre a instância do DR Drill a partir do EC2 console da Amazon. Para obter mais informações, consulte Preparação para um	

Tarefa	Descrição	Habilidades necessárias
	failover na documentação do Elastic Disaster Recovery.	
Validar a simulação.	Na etapa anterior, você lançou novas instâncias de destino na região de DR. As instâncias de destino são réplicas dos servidores de origem com base no instantâneo obtido quando você iniciou o lançamento. Neste procedimento, você se conecta às máquinas de EC2 destino da Amazon para confirmar se elas estão funcionando conforme o esperado. 1. Abra o EC2 console da Amazon. 2. Selecione Instâncias (execução). 3. Selecione a instância de destino e anote seu IPv4 endereço privado. 4. Certifique-se de que você possa se conectar à EC2 instância e de que o JD Edwards EnterpriseOne e os componentes relacionados sejam replicados conforme o esperado.	

Tarefa	Descrição	Habilidades necessárias
Iniciar um failover.	Um failover é o redirecionamento do tráfego de um sistema primário para um sistema secundário. O Elastic Disaster Recovery ajuda você a realizar um failover lançando instâncias de recuperação na AWS. Quando as instâncias de recuperação são iniciadas, você redireciona o tráfego dos seus sistemas primários para essas instâncias. 1. No console do Elastic Disaster Recovery, abra a página Source servers (Servidores de origem) e verifique se a coluna Ready for recovery (Pronto para recuperação) do servidor de origem mostra Ready (Pronto), e a coluna Data replication status (Status de replicação de dados) mostra Healthy (Saudável). 2. Selecione o servidor de origem. No menu Initiate recovery job (Iniciar tarefa de recuperação), selecione Initiate recovery (Iniciar recuperação). 3. Selecione o point-in-time snapshot a partir do qual iniciar a instância de	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	recuperação e, em seguida, escolha Iniciar recuperação. Isso inicia um trabalho de recuperação. Você pode monitorar o status do trabalho na página Recovery instances (Instâncias de recuperação). 4. Teste e verifique a instância de recuperação. Se necessário, ajuste a configuração do DNS e conecte seu EnterpriseOne aplicativo JD Edwards ao banco de dados. 5. Agora você pode desconectar e descomissionar o EnterpriseOne servidor JD Edwards de origem, porque todas as alterações foram gravadas na nova instância de recuperação. 6. Registre a instância de recuperação como servidor de origem na região de DR seguindo o processo descrito no épico Install the AWS Replication Agent (Instale o agente de replicação AWS).	

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es, consulte Execução de um failover na documentação do Elastic Disaster Recovery.	

Tarefa	Descrição	Habilidades necessárias
Inicie um failback.	O processo para iniciar um failback é semelhante ao processo para iniciar o failover. 1. Abra o console do Elastic Disaster Recovery na região primária. Navegue até a página Recovery instances (Instâncias de recuperação), selecione a instância de simulação e, em seguida, selecione Actions (Ações), Disconnect from AWS (Desconectar da AWS), Delete recovery instances (Excluir instâncias de recuperação). 2. Abra o console do Elastic Disaster Recovery na região de DR. Registre seu novo servidor JD Edwards como EnterpriseOne servidor de origem na região de DR instalando o AWS Replication Agent. Os dados serão sincronizados com um novo servidor de replicação provisionado na nova sub-rede de teste. **Note** Quando o novo servidor JD	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Edwards é registrado como EnterpriseOne servidor de origem, você pode ver dois servidores de origem no console do Elastic Disaster Recovery: um servidor criado a partir da EC2 instância primária e o novo servidor criado a partir da instância de recuperação. Recomendamos que você marque os servidores corretamente para evitar confusão e, de preferência, adicione o novo servidor ao modelo de execução. 3. Para reiniciar a replicação de DR da região primária, desassocie a instância de recuperação iniciada do console do Elastic Disaster Recovery na região de DR e registre o host como servidor de origem na região primária.	

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es, consulte Execução de um failback na documentação do Elastic Disaster Recovery.	

Tarefa	Descrição	Habilidades necessárias
Inicie os componentes do JD Edwards. EnterpriseOne	1. Inicie o EnterpriseOne banco de dados do JD Edwards fazendo login no servidor do banco de dados. 2. Quando o banco de dados estiver em execução, inicie a EnterpriseOne lógica e os servidores em lote do JD Edwards. 3. Inicie WebLogic nos servidores web e inicie uma instância JAS nos servidore s JAS. 4. Comece WebLogic no servidor de provisão e no servidor do console SM. 5. Inicie o SM Agent nos servidores. 6. Confirme se o login no JD Edwards EnterpriseOne funciona corretamente. Você precisará incorporar as alterações no Route 53 e no Application Load Balancer para que o link do JD Edwards funcione EnterpriseOne . Você pode automatizar essas etapas usando Lambda, Step Functions e Systems Manager (Run Command).	JD Edwards EnterpriseOne CNC

Tarefa	Descrição	Habilidades necessárias
	Note O Elastic Disaster Recovery executa a replicação em nível de bloco dos volumes do EBS da EC2 instância de origem que hospedam o sistema operacional e os sistemas de arquivos. Os sistemas de arquivos compartilhados que foram criados usando o Amazon EFS não fazem parte dessa replicação. Você pode replicar sistemas de arquivos compartilhados para a região de DR usando a AWS DataSync, conforme observado no primeiro épico, e depois montar esses sistemas de arquivos replicados no sistema de DR.	

Solução de problemas

Problema	Solução
O status de replicação de dados do servidor de origem está Paralisado e a replicação está atrasada. Se você verificar os detalhes, o status da replicação de dados exibirá Agent not seen (Agente indisponível).	Verifique se o servidor de origem paralisado está em execução. **Note** Se o servidor de origem ficar inativo, o servidor de replicação será encerrado automaticamente. Para obter mais informações sobre problemas de atraso, consulte Problemas de atraso de replicação na documentação do Elastic Disaster Recovery.
A instalação do AWS Replication Agent na EC2 instância de origem falha no RHEL 8.2 após a digitalização dos discos. `aws_replication_agent_installer.log` revela que faltam cabeçalhos do kernel.	Antes de instalar o AWS Replication Agent no RHEL 8, CentOS 8 ou Oracle Linux 8, execute: `sudo yum install elfutils-libelf-devel` Para obter mais informações, consulte os requisitos de instalação do Linux na documentação do Elastic Disaster Recovery.
No console do Elastic Disaster Recovery, você vê o servidor de origem como Ready (Pronto), com um atraso e o status de replicação de dados como Stalled (Parado). Dependendo de quanto tempo o AWS Replication Agent estiver indisponível, o status pode indicar um alto atraso, mas o problema continua o mesmo.	Use um comando do sistema operacional para confirmar se o AWS Replication Agent está sendo executado na EC2 instância de origem ou confirme se a instância está em execução. Depois de corrigir qualquer problema, o Elastic Disaster Recovery reiniciará o escaneamento. Espere até que todos os dados tenham sido sincronizados e o status da replicação

Problema	Solução
	seja Healthy (Saudável) antes de iniciar um simulação de recuperação de desastres.
Replicação inicial com alto atraso. No console do Elastic Disaster Recovery, você pode ver que o status de sincronização inicial é extremamente lento para um servidor de origem.	Verifique os problemas de atraso de replicaçã o documentados na seção Replication lag issues (Problemas de atraso de replicação) na documentação do Elastic Disaster Recovery. O servidor de replicação pode não conseguir lidar com a carga devido às operações computacionais intrínsecas. Nesse caso, tente atualizar o tipo de instância depois de consultar a equipe do Suporte técnico da AWS.

Recursos relacionados

- Guia do usuário do AWS Elastic Disaster Recovery
- Criação de um plano escalável de recuperação de desastres com o AWS Elastic Disaster Recovery (publicação no blog da AWS)
- AWS Elastic Disaster Recovery – Uma introdução técnica (curso AWS Skill Builder; requer login)
- Guia de início rápido do AWS Elastic Disaster Recovery

Configure a detecção de AWS CloudFormation desvios em uma organização multirregional e com várias contas

Criado por Ram Kandaswamy (AWS)

Resumo

Os usuários do Amazon Web Services (AWS) geralmente procuram uma maneira eficiente de detectar incompatibilidades na configuração de recursos, incluindo a variação nas AWS CloudFormation pilhas, e corrigi-las o mais rápido possível. Esse é especialmente o caso quando AWS Control Tower é usado.

Esse padrão fornece uma solução prescritiva que resolve o problema de forma eficiente usando alterações consolidadas na configuração de recursos e agindo de acordo com essas alterações para gerar resultados. A solução foi projetada para cenários em que há várias AWS CloudFormation pilhas criadas em mais de uma Região da AWS, ou em mais de uma conta, ou uma combinação de ambas. Os objetivos da solução são os seguintes:

- Simplifique o processo de detecção de desvios
- Configurar notificação e alerta
- Configurar relatórios consolidados

Pré-requisitos e limitações

Pré-requisitos

- AWS Config ativado em todas as regiões e contas que devem ser monitoradas

Limitações

- O relatório gerado suporta somente os formatos de saída JSON e valores separados por vírgula (CSV).

Arquitetura

O diagrama a seguir mostra a AWS Organizations configuração com várias contas. AWS Config as regras se comunicam entre as contas.

O fluxo de trabalho inclui as seguintes etapas:

1. A AWS Config regra detecta desvios.
2. Os resultados da detecção de desvios encontrados em outras contas são enviados para a conta de gerenciamento.
3. A CloudWatch regra da Amazon chama uma AWS Lambda função.
4. A função Lambda consulta a AWS Config regra para obter resultados agregados.
5. A função Lambda notifica o Amazon Simple Notification Service (Amazon SNS), que envia uma notificação por e-mail sobre o desvio.

Automação e escala

A solução apresentada aqui pode ser dimensionada para regiões e contas adicionais.

Ferramentas

Serviços da AWS

- AWS Configfornece uma visão detalhada da configuração dos AWS recursos em seu Conta da AWS. Isso inclui como os recursos estão relacionados um com o outro e como eles foram configurados no passado, de modo que você possa ver como os relacionamentos e as configurações foram alterados ao longo do tempo.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.

Épicos

Automatize a detecção de desvios para AWS CloudFormation

Tarefa	Descrição	Habilidades necessárias
Crie o agregador.	1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config. 2. Crie um agregador na conta de gerenciamento. 3. Certifique-se de que a replicação de dados esteja ativada para que AWS Config possa buscar dados das contas de origem. 4. Selecione todas as regiões e contas aplicáveis. Você pode selecionar contas com base em AWS Organizations. Recomendamos essa abordagem porque as novas contas na organização são automaticamente parte do agregador.	Arquiteto de nuvem
Crie uma regra AWS gerenciada.	Adicione a regra `cloudformation-stack-drift-detection-check` AWS gerenciada. A regra precisa de um valor de parâmetro: `cloudformationArn` . Insira o nome do recurso da Amazon (ARN) do perfil do	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	IAM que tem permissões para detectar desvio de pilha. A função deve ter uma política de confiança que AWS Config permita assumir a função.	
Crie a seção de consulta avançada do agregador.	Para buscar pilhas derivadas de várias fontes, crie a seguinte consulta: `SELECT resourceId, configuration.driftInformation.stackDriftStatus WHERE resourceType = 'AWS::CloudFormation::Stack' AND configuration.driftInformation.stackDriftStatus IN ('DRIFTED')`	Arquiteto de nuvem, desenvolvedor
Automatize a execução da consulta e publique.	1. Crie uma função Lambda usando o código anexado. O Lambda publicará os resultados em um tópico do SNS que é fornecido como uma variável de ambiente na função Lambda. 2. Para receber alertas, crie uma assinatura de e-mail para o tópico do SNS.	Arquiteto de nuvem, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Crie uma CloudWatch regra.	Crie uma CloudWatch regra baseada em agendamento para chamar a função Lambda, que é responsável pelos alertas.	Arquiteto de nuvem

Recursos relacionados

Recursos

- O que é AWS Config?
- Agregação de dados de várias regiões e várias contas
- Detectar alterações de configuração não gerenciadas em pilhas e recursos
- IAM: passe uma função do IAM para uma função específica AWS service (Serviço da AWS)
- O que é o Amazon SNS?

Mais informações

Considerações

Recomendamos usar a solução apresentada nesse padrão em vez de usar soluções personalizadas que envolvam chamadas de API em intervalos específicos para iniciar a detecção de desvios em cada pilha ou conjunto de CloudFormation pilhas. Soluções personalizadas que usam chamadas de API em intervalos específicos podem levar a um grande número de chamadas de API e afetar o desempenho. Devido ao número de chamadas de API, a limitação pode ocorrer. Outro problema potencial é um atraso na detecção se as alterações de recursos forem identificadas com base somente no cronograma.

Como os conjuntos de pilhas são feitos de pilhas, você pode usar essa solução. Os detalhes da instância de pilhas também estão disponíveis como parte da solução.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Importe com sucesso um bucket do S3 como uma pilha da AWS CloudFormation

Criado por Ram Kandaswamy (AWS)

Resumo

Se você usa recursos da Amazon Web Services (AWS), como buckets do Amazon Simple Storage Service (Amazon S3), e quer usar uma abordagem de infraestrutura como código (IaC), você pode importar seus recursos para a CloudFormation AWS e gerenciá-los como uma pilha.

Esse padrão fornece etapas para importar com sucesso um bucket do S3 como uma CloudFormation pilha da AWS. Ao usar essa abordagem padrão, você pode evitar possíveis erros que possam ocorrer se você importar seu bucket do S3 em uma única ação.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket S3 existente e uma política de bucket S3. Para obter mais informações sobre isso, consulte Qual política de bucket do S3 devo usar para cumprir a regra s3- do AWS Config bucket-ssl-requests-only no Centro de Conhecimento da AWS.
- Uma chave do AWS Key Management Service (AWS KMS) existente e seu alias. Para obter mais informações sobre isso, consulte Trabalho com aliases na documentação do AWS KMS.
- O CloudFormation modelo de amostra `CloudFormation-template-S3-bucket` da AWS (anexado), baixado para seu computador local.

Arquitetura

O diagrama mostra o seguinte fluxo de trabalho:

1. O usuário cria um modelo da AWS em formato JSON ou YAML. CloudFormation
2. O modelo cria uma CloudFormation pilha da AWS para importar o bucket do S3.
3. O AWS CloudFormation stack gerencia o bucket S3 que você especificou no modelo.

Pilha de tecnologia

- AWS CloudFormation
- AWS Identity and Access Management (IAM)
- AWS KMS
- Amazon S3

Ferramentas

- AWS CloudFormation — CloudFormation A AWS ajuda você a criar e provisionar implantações de infraestrutura da AWS de forma previsível e repetida.
- AWS Identity and Access Management (IAM): o IAM é um serviço web para controlar, com segurança, o acesso a serviços da AWS.
- AWS KMS: o AWS Key Management Service (AWS KMS) é um serviço de criptografia e gerenciamento de chave com escalabilidade para a nuvem.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet.

Épicos

Importe um bucket S3 com criptografia AWS KMS key baseada como uma pilha da AWS CloudFormation

Tarefa	Descrição	Habilidades necessárias

Crie um modelo para importar o bucket do S3 e a chave KMS.	Em seu computador local, crie um modelo para importar seu bucket do S3 e a chave KMS usando o seguinte modelo de exemplo:
	`AWSTemplateFormatVersion: 2010-09-09`
	
	`Parameters:`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre> bucketName:
	
	    Type: String
	
	Resources:
	
	  S3Bucket:
	
	    Type: 'AWS::S3:
	:Bucket'
	
	    DeletionPolicy:
	 Retain
	
	    Properties:
	
	      BucketName: !Ref
	 bucketName
	
	      BucketEncryption:
	
	        ServerSid
	eEncryptionConfigu
	ration:
	
	          - ServerSid
	eEncryptionByDefault:
	
	              SSEAlgori
	thm: 'aws:kms'
	
	              KMSMaster
	KeyID: !GetAtt
	
	                -
	 KMSS3Encryption
	
	                - Arn
	
	  KMSS3Encryption:</pre>	

Tarefa	Descrição	Habilidades necessárias

	<pre> Type: 'AWS::KMS
	::Key'
	
	    DeletionPolicy:
	 Retain
	
	    Properties:
	
	      Enabled: true
	
	      KeyPolicy: !Sub
	 |-
	
	        {
	
	            "Id": "key-
	consolepolicy-3",
	
	            "Version":
	 "2012-10-17",
	
	            "Statemen
	t": [
	
	                {
	
	 "Sid": "Enable IAM User
	 Permissions",
	
	 "Effect": "Allow",
	
	 "Principal": {
	
	 "AWS": ["arn:aws:iam::
	${AWS::AccountId}:roo
	t"]
	
	                    },</pre>	

Tarefa	Descrição	Habilidades necessárias

	<pre>"Action": "kms:*",
	
	"Resource": "*"
	}
	}
	]
	}
	
	EnableKey Rotation: true</pre>	

Tarefa	Descrição	Habilidades necessárias
Crie a pilha.	1. Faça login no Console de Gerenciamento da AWS, abra o CloudFormation console da AWS, escolha Exibir pilha, escolha Criar pilha e, em seguida, escolha Com recursos existentes (recursos de importação). 2. Escolha Carregar um arquivo de modelo e, em seguida, carregue o arquivo de modelo que você criou anteriormente. 3. Insira um nome para sua pilha e configure as opções restantes de acordo com seus requisitos. 4. Escolha Criar pilha e aguarde até que o status da pilha mude para. `IMPORT_COMPLETE`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Crie o alias da chave KMS.	1. No CloudFormation console da AWS, escolha Stacks, escolha o nome da pilha que você criou anteriorm ente, escolha o painel Template e, em seguida, escolha View in Designer.
	2. Adicione o seguinte trecho à seção de recursos `Resource` do modelo e, em seguida, escolha Criar pilha e conclua o assistent e:
	
	`KMSS3EncryptionAlias:`
	
	`  Type: 'AWS::KMS ::Alias'`
	
	`  DeletionPolicy: Retain`
	
	`  Properties:`
	
	`  AliasName: alias/ S3BucketKey`
	
	`  TargetKeyId: !Ref KMSS3Encryption`
	
	Para obter mais informaçõ es sobre isso, consulte as atualizações do AWS CloudFormation Stack na
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	CloudFormation documentação da AWS.	

Tarefa	Descrição	Habilidades necessárias

Atualize a pilha para incluir a política de bucket do S3.	1. No CloudFormation console da AWS, escolha Stacks, escolha o nome da pilha que você criou anteriorm ente, escolha o painel Template e, em seguida, escolha View in Designer.
	2. Adicione o seguinte trecho à seção `Resource` do seu modelo e, em seguida, escolha Criar pilha e conclua o assistente:
	
	`S3BucketPolicy:`
	
	`  Type: 'AWS::S3:`
	`:BucketPolicy'`
	
	`  Properties:`
	
	`    Bucket: !Ref`
	` S3Bucket`
	
	`    PolicyDocument: !`
	`Sub |-`
	
	`      {`
	
	` "Version": "2008-10-`
	`17",`
	
	`                  "Id":`
	` "restricthttp",`
	
	` "Statement": [`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	{
	
	"Sid": "denyhttp",
	
	"Effect": "Deny",
	
	"Principal": {
	
	"AWS": "*"
	
	},
	
	"Action": "s3:*",
	
	"Resource": ["arn:aws:s3:::${S3Bucket}","arn:aws:s3:::${S3Bucket}/*"],
	
	"Condition": {
	
	"Bool": {
	
	"aws:SecureTransport": "false"
	
	}
	
	}	

Tarefa	Descrição	Habilidades necessárias
	}] } **Note** Essa política de bucket do S3 tem uma declaração de negação que restringe as chamadas de API que não são seguras.	

Tarefa	Descrição	Habilidades necessárias
Atualize a política de chaves.	1. No CloudFormation console da AWS, escolha Stacks, escolha o nome da pilha que você criou anteriorm ente, escolha o painel Template e, em seguida, escolha View in Designer. 2. Modifique o recurso KMS do modelo para incluir a política de chaves que permite aos administr adores administrar a chave KMS. 3. Escolha Criar pilha, escolha Avançar e, em seguida, conclua o assistente de acordo com seus requisitos. Para obter mais informações, consulte Políticas principais AWS KMS na documentação do AWS KMS.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Adicione tags em nível de recurso.	1. No CloudFormation console da AWS, escolha Stacks, escolha o nome da pilha que você criou anteriorm ente, escolha o painel Template e, em seguida, escolha View in Designer.
	2. Adicione o seguinte trecho à seção de recursos `Properties` do Amazon S3 do modelo e, em seguida, escolha Create stack e conclua o assistent e:
	
	`Tags:`
	
	`- Key: createdBy`
	
	`Value: Cloudform ation`
		AWS DevOps

Recursos relacionados

- Trazendo os recursos existentes para o CloudFormation gerenciamento da AWS
- AWS re:Invent 2017: aprofundamento na AWS CloudFormation (vídeo)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Sincronize dados entre sistemas de arquivos Amazon EFS em diferentes regiões da AWS usando a AWS DataSync

Criado por Sarat Chandra Pothula (AWS) e Aditya Ambati (AWS)

Resumo

Essa solução fornece uma estrutura robusta para sincronização de dados eficiente e segura entre instâncias do Amazon Elastic File System (Amazon EFS) em diferentes regiões da AWS. Essa abordagem é escalável e fornece replicação de dados controlada entre regiões. Essa solução pode aprimorar suas estratégias de recuperação de desastres e redundância de dados.

Ao usar o AWS Cloud Development Kit (AWS CDK), esse padrão é usado como uma abordagem de infraestrutura como código (IaC) para implantar os recursos da solução. O aplicativo AWS CDK implanta os recursos essenciais da AWS, DataSync Amazon EFS, Amazon Virtual Private Cloud (Amazon VPC) e Amazon Elastic Compute Cloud (Amazon). EC2 Esse IaC fornece um processo de implantação repetível e controlado por versão que está totalmente alinhado às melhores práticas da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) versão 2.9.11 ou posterior, instalada e configurada
- AWS CDK versão 2.114.1 ou posterior, instalado e inicializado
- NodeJS versão 20.8.0 ou posterior, instalado

Limitações

- A solução herda limitações do DataSync Amazon EFS, como taxas de transferência de dados, limitações de tamanho e disponibilidade regional. Para obter mais informações, consulte Cotas da AWS e DataSync cotas do Amazon EFS.
- Essa solução é compatível somente com o Amazon EFS. DataSync oferece suporte a outros serviços da AWS, como Amazon Simple Storage Service (Amazon S3) e FSx Amazon for Lustre. No entanto, essa solução requer modificações para sincronizar dados com esses outros serviços.

Arquitetura

Essa solução implanta as seguintes pilhas de CDK da AWS:

- Pilha Amazon VPC — Essa pilha configura recursos de nuvem privada virtual (VPC), incluindo sub-redes, um gateway de internet e um gateway NAT nas regiões primária e secundária da AWS.
- Pilha Amazon EFS — Essa pilha implanta sistemas de arquivos Amazon EFS nas regiões primária e secundária e os conecta às suas respectivas regiões. VPCs
- Amazon EC2 stack — Essa pilha inicia EC2 instâncias nas regiões primária e secundária. Essas instâncias são configuradas para montar o sistema de arquivos Amazon EFS, o que lhes permite acessar o armazenamento compartilhado.
- DataSync pilha de localização — Essa pilha usa uma construção personalizada chamada `DataSyncLocationConstruct` para criar recursos de DataSync localização nas regiões primária e secundária. Esses recursos definem endpoints para sincronização de dados.
- DataSync pilha de tarefas — Essa pilha usa uma construção personalizada chamada `DataSyncTaskConstruct` para criar uma DataSync tarefa na região primária. Essa tarefa está configurada para sincronizar dados entre as regiões primária e secundária usando os locais de DataSync origem e destino.

Ferramentas

Serviços da AWS

- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- DataSyncA AWS é um serviço on-line de transferência e descoberta de dados que ajuda você a mover arquivos ou dados de objetos de, para e entre os serviços de armazenamento da AWS.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Repositório de código

O código desse padrão está disponível no repositório do GitHub Amazon EFS Cross-Region DataSync Project.

Práticas recomendadas

Siga as melhores práticas descritas em Melhores práticas para usar o AWS CDK TypeScript para criar projetos de IaC.

Épicos

Implante o aplicativo AWS CDK

Tarefa	Descrição	Habilidades necessárias
Clone o repositório do projeto.	Insira o comando a seguir para clonar o repositório do Amazon EFS Cross-Region DataSync Project. `git clone https://github.com/aws-samples/aws-efs-cross-region-datasync.git`	AWS DevOps
Instale as dependências do npm.	Insira o comando da a seguir. `npm ci`	AWS DevOps
Escolha as regiões primária e secundária.	No repositório clonado, navegue até o `src/infra` diretório. No `Launcher.ts` arquivo, `PRIMARY_AWS_REGION` atualize os `SECONDARY_AWS_REGION` valores e. Use os códigos de região correspondentes.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`const primaryRegion = { account: account, region: '<PRIMARY_AWS_REGION>' }; const secondaryRegion = { account: account, region: '<SECONDARY_AWS_REGION>' };`	
Faça o bootstrap do ambiente.	Digite o comando a seguir para inicializar a conta da AWS e a região da AWS que você deseja usar. `cdk bootstrap <aws_account>/<aws_region>` Para obter mais informações, consulte Inicialização na documentação do AWS CDK.	AWS DevOps
Liste as pilhas do AWS CDK.	Digite o comando a seguir para ver uma lista das pilhas de CDK da AWS no aplicativo. `cdk ls`	AWS DevOps
Sintetize as pilhas de CDK da AWS.	Insira o comando a seguir para produzir um CloudFormation modelo da AWS para cada pilha definida no aplicativo AWS CDK. `cdk synth`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Implante o aplicativo AWS CDK.	Insira o comando a seguir para implantar todas as pilhas em sua conta da AWS, sem exigir aprovação manual para nenhuma alteração. `cdk deploy --all --require-approval never`	AWS DevOps

Valide a implantação

Tarefa	Descrição	Habilidades necessárias
Faça login na EC2 instância na região principal.	1. Usando o Session Manager, um recurso do AWS Systems Manager, faça login na EC2 instância na região principal. Para obter instruções, consulte Conecte-se à sua instância Linux com o AWS Systems Manager Session Manager. 2. Altere os diretórios para o caminho de montagem do Amazon EFS. `cd /mnt/efs`	AWS DevOps
Crie um arquivo temporário.	Insira o comando a seguir para criar um arquivo temporário no caminho de montagem do Amazon EFS. `sudo dd if=/dev/zero \`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`of=tmptst.dat \`
	`bs=1G \`
	`seek=5 \`
	`count=0`
	
	`ls -lrt tmptst.dat`	

Inicie a DataSync tarefa.	Insira o comando a seguir para replicar o arquivo temporário da região primária para a região secundária, onde `<ARN-task>` está o Amazon Resource Name (ARN) da DataSync sua tarefa.
	
	`aws datasync start-task-execution \`
	`--task-arn <ARN-task>`
	
	O comando retorna o ARN da execução da tarefa no formato a seguir.
	
	`arn:aws:datasync:<region>:<account-ID>:task/task-execution/<exec-ID>`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Verifique o status da transferência de dados.	Digite o comando a seguir para descrever a tarefa de DataSync execução, onde `<ARN-task-execution>` está o ARN da execução da tarefa. `aws datasync describe-task-execution \ --task-execution-arn <ARN-task-execution>` A DataSync tarefa é concluída quando `PrepareStatus` , `TransferStatus` , e `VerifyStatus` todas têm o valor `SUCCESS`.	AWS DevOps
Faça login na EC2 instância na região secundária.	1. Usando o Session Manager, um recurso do AWS Systems Manager, faça login na EC2 instância na região secundária. Para obter instruções, consulte Conecte-se à sua instância Linux com o AWS Systems Manager Session Manager. 2. Altere os diretórios para o caminho de montagem do Amazon EFS. `cd /mnt/efs`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Valide a replicação.	Insira o comando a seguir para verificar se o arquivo temporário existe no sistema de arquivos do Amazon EFS. `ls -lrt tmptst.dat`	AWS DevOps

Recursos relacionados

Documentação da AWS

- Referência da API AWS CDK
- Configurando DataSync transferências da AWS com o Amazon EFS
- Solução de problemas com DataSync transferências da AWS

Outros recursos da AWS

- AWS DataSync FAQs

Teste a AWS infraestrutura usando LocalStack e Terraform Tests

Criado por Ivan Girardi (AWS) e Ioannis Kalyvas (AWS)

Resumo

Esse padrão ajuda você a testar localmente a infraestrutura como código (IaC) AWS no Terraform sem a necessidade de provisionar a infraestrutura em seu AWS ambiente. Ele integra a estrutura do Terraform Tests com. LocalStack O contêiner LocalStack Docker fornece um ambiente de desenvolvimento local que emula vários. Serviços da AWS Isso ajuda você a testar e iterar implantações de infraestrutura sem incorrer em custos no. Nuvem AWS

Essa solução oferece os seguintes benefícios:

- Otimização de custos — a execução de testes LocalStack elimina a necessidade de uso Serviços da AWS. Isso evita que você incorra em custos associados à criação, operação e modificação desses AWS recursos.
- Velocidade e eficiência — Testar localmente também é normalmente mais rápido do que implantar os AWS recursos. Esse ciclo de feedback rápido acelera o desenvolvimento e a depuração. Como LocalStack é executado localmente, você pode desenvolver e testar seus arquivos de configuração do Terraform sem uma conexão com a Internet. Você pode depurar os arquivos de configuração do Terraform localmente e receber feedback imediato, o que simplifica o processo de desenvolvimento.
- Consistência e reprodutibilidade — LocalStack fornece um ambiente consistente para testes. Essa consistência ajuda a garantir que os testes produzam os mesmos resultados, independentemente de AWS alterações externas ou problemas de rede.
- Isolamento — Testar com LocalStack evita que você acidentalmente afete AWS recursos ativos ou ambientes de produção. Esse isolamento torna seguro experimentar e testar várias configurações.
- Automação — A integração com um pipeline de integração contínua e entrega contínua (CI/CD) ajuda você a testar automaticamente os arquivos de configuração do Terraform. O pipeline testa minuciosamente o IaC antes da implantação.
- Flexibilidade — você pode simular configurações diferentes Regiões da AWS e de serviço para se adequar melhor aos seus ambientes de produção. Contas da AWS

Pré-requisitos e limitações

Pré-requisitos

- Instalar o Docker
- Habilite o acesso ao soquete Docker padrão ()`/var/run/docker.sock`. Para obter mais informações, consulte a documentação do LocalStack .
- Instale o Docker Compose
- Instale o Terraform versão 1.6.0 ou posterior
- Instale o Terraform CLI
- Configurar o provedor Terraform AWS
- (Opcional) Instale e configure o AWS Command Line Interface (AWS CLI). Para ver um exemplo de como usar o AWS CLI with LocalStack, consulte o repositório GitHub Test AWS infrastructure using LocalStack and Terraform Tests.

Limitações

- Esse padrão fornece exemplos explícitos para testar os recursos do Amazon Simple Storage Service (Amazon S3),, AWS Lambda e AWS Step Functions do Amazon DynamoDB. No entanto, você pode estender essa solução para incluir AWS recursos adicionais.
- Esse padrão fornece instruções para executar testes do Terraform localmente, mas você pode integrar os testes em qualquer pipeline de CI/CD.
- Esse padrão fornece instruções para usar a imagem LocalStack da comunidade. Se você estiver usando a imagem LocalStack Pro, consulte a documentação do LocalStack Pro.
- LocalStack fornece serviços de emulação para diferentes. AWS APIs Para obter uma lista completa, consulte Cobertura AWS de recursos de serviço. Alguns recursos avançados podem exigir uma assinatura do LocalStack Pro.

Arquitetura

O diagrama a seguir mostra a arquitetura dessa solução. Os componentes principais são um repositório de código-fonte, um pipeline de CI/CD e um LocalStack contêiner Docker. O LocalStack Docker Container hospeda o seguinte Serviços da AWS localmente:

- Um bucket Amazon S3 para armazenar arquivos
- Amazon CloudWatch para monitoramento e registro
- Uma AWS Lambda função para executar código sem servidor
- Uma máquina de AWS Step Functions estado para orquestrar fluxos de trabalho em várias etapas

- Uma tabela do Amazon DynamoDB para armazenar dados NoSQL

O diagrama mostra o seguinte fluxo de trabalho:

1. Você adiciona e confirma um arquivo de configuração do Terraform no repositório do código-fonte.
2. O pipeline de CI/CD detecta as alterações e inicia um processo de construção para análise estática do código do Terraform. O pipeline cria e executa o contêiner LocalStack Docker. Em seguida, o pipeline inicia o processo de teste.
3. O pipeline carrega um objeto em um bucket do Amazon S3 que está hospedado no contêiner LocalStack do Docker.
4. O upload do objeto invoca uma função. AWS Lambda
5. A função Lambda armazena a notificação de eventos do Amazon S3 em um log. CloudWatch
6. A função Lambda inicia uma máquina de AWS Step Functions estado.
7. A máquina de estado grava o nome do objeto Amazon S3 em uma tabela do DynamoDB.
8. O processo de teste no pipeline de CI/CD verifica se o nome do objeto carregado corresponde à entrada na tabela do DynamoDB. Também verifica se o bucket do S3 foi implantado com o nome especificado e se a AWS Lambda função foi implantada com sucesso.

Ferramentas

Serviços da AWS

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- O Docker Compose é uma ferramenta para definir e executar aplicativos com vários contêineres.
- LocalStackié um emulador de serviços em nuvem executado em um único contêiner. Ao usar LocalStack, você pode executar cargas de trabalho em sua máquina local que usam Serviços da AWS, sem se conectar ao Nuvem AWS.
- O Terraform é uma ferramenta de IaC HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.
- O Terraform Tests ajuda você a validar as atualizações de configuração do módulo Terraform por meio de testes que são análogos aos testes de integração ou de unidade.

Repositório de código

O código desse padrão está disponível na AWS infraestrutura de GitHub teste usando LocalStack o repositório Terraform Tests.

Práticas recomendadas

- Essa solução testa a AWS infraestrutura especificada nos arquivos de configuração do Terraform e não implanta esses recursos no Nuvem AWS. Se você quiser implantar os recursos, siga o princípio do privilégio mínimo (documentação do IAM) e configure adequadamente o back-end do Terraform (documentação do Terraform).
- Ao fazer a integração LocalStack em um pipeline de CI/CD, recomendamos que você não execute o contêiner LocalStack Docker no modo de privilégio. Para obter mais informações, consulte Privilégio de tempo de execução e recursos do Linux (documentação do Docker) e Segurança para executores autogerenciados (documentação). GitLab

Épicos

Implante a solução

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Em um shell bash, insira o comando a seguir. Isso clona a AWS infraestrutura de teste usando LocalStack o repositório Terraform Tests de: GitHub `git clone https://github.com/aws-samples/localstack-terraform-test.git`	DevOps engenheiro

Execute o LocalStack contêiner.	1. Digite o comando a seguir para navegar até o repositório clonado:
	`cd localstack-terraform-test`
	2. Digite o comando a seguir para iniciar o contêiner LocalStack Docker no modo desanexado:
	`docker-compose up -d`
	3. Espere até que o contêiner LocalStack Docker esteja operacional.
		DevOps engenheiro

Inicializar o Terraform.	Digite o seguinte comando para inicializar o Terraform:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`terraform init`	

Execute testes do Terraform.	1. Digite o seguinte comando para executar os testes do Terraform:
	`terraform test`
	2. Verifique se todos os testes foram concluídos com êxito. A saída deve ser semelhante ao seguinte:
	`Success! 3 passed, 0 failed.`
		DevOps engenheiro

Limpar recursos.	Digite o seguinte comando para destruir o LocalStack contêiner: `docker-compose down`	DevOps engenheiro

Solução de problemas

Problema	Solução
`Error: reading DynamoDB Table Item (Files|README.md): empty` resultado ao executar o `terraform test` comando.	1. Insira o `terraform test` comando novamente. 2. Se isso não resolver o erro, edite o arquivo main.tf para aumentar o tempo limite de espera para um valor maior que 15 segundos: `resource "time_sleep" "wait" {`

Problema	Solução

	`create_duration = "15s"`
	`triggers = {`
	`s3_object = local.key_json`
	`}`
	`}`

Recursos relacionados

- Introdução ao Terraform: orientação AWS CDK e orientação para AWS CloudFormation especialistas (orientação AWS prescritiva)
- Melhores práticas para usar o Terraform AWS Provider (orientação AWS prescritiva)
- CI/CD do Terraform e testes AWS com o novo Terraform Test Framework (postagem no blog)AWS
- Acelerando a entrega de software usando o LocalStack Cloud Emulator de AWS Marketplace (AWS postagem no blog)

Mais informações

Integração com GitHub ações

Você pode integrar LocalStack e testar o Terraform em um pipeline de CI/CD usando o Actions. GitHub Para obter mais informações, consulte a documentação de GitHub ações. Veja a seguir um exemplo de arquivo de configuração de GitHub ações:

```
name: LocalStack Terraform Test

on:
  push:
    branches:
      - '**'

  workflow_dispatch: {}

jobs:
  localstack-terraform-test:
    runs-on: ubuntu-latest

    steps:
```

```
    - uses: actions/checkout@v4

    - name: Build and Start LocalStack Container
      run: |
        docker compose up -d

    - name: Setup Terraform
      uses: hashicorp/setup-terraform@v3
      with:
        terraform_version: latest

    - name: Run Terraform Init and Validation
      run: |
        terraform init
        terraform validate
        terraform fmt --recursive --check
        terraform plan
        terraform show

    - name: Run Terraform Test
      run: |
        terraform test

    - name: Stop and Delete LocalStack Container
      if: always()
      run: docker compose down
```

Atualize os clusters do SAP Pacemaker de para ENSA1 ENSA2

Criado por Gergely Cserdi (AWS) e Balazs Sandor Skublics (AWS)

Resumo

Esse padrão explica as etapas e as considerações para atualizar um cluster SAP Pacemaker baseado no Standalone Enqueue Server () para. ENSA1 ENSA2 As informações desse padrão se aplicam aos sistemas operacionais SUSE Linux Enterprise Server (SLES) e Red Hat Enterprise Linux (RHEL).

Os clusters Pacemaker no SAP NetWeaver 7.52 ou S/4HANA 1709 e versões anteriores são executados em uma ENSA1 arquitetura e são configurados especificamente para o. ENSA1 Se você executa suas cargas de trabalho do SAP na Amazon Web Services (AWS) e está interessado em migrar para lá ENSA2, talvez descubra que a documentação do SAP, SUSE e RHEL não fornece informações abrangentes. Esse padrão descreve as etapas técnicas necessárias para reconfigurar os parâmetros do SAP e os clusters do Pacemaker para fazer o upgrade de para. ENSA1 ENSA2 Ele fornece exemplos de sistemas SUSE, mas o conceito é o mesmo para clusters RHEL.

Notas: ENSA1 e ENSA2 são conceitos que dizem respeito somente aos aplicativos SAP, portanto, as informações nesse padrão não se aplicam ao SAP HANA ou a outros tipos de clusters.

Tecnicamente, ENSA2 pode ser usado com ou sem o Enqueue Replicator 2. No entanto, a alta disponibilidade (HA) e a automação de failover (por meio de uma solução de cluster) exigem o Enqueue Replicator 2. Esse padrão usa o termo ENSA2 clusters para se referir a clusters com Standalone Enqueue Server 2 e Enqueue Replicator 2.

Pré-requisitos e limitações

Pré-requisitos

- Um cluster funcional ENSA1 que usa Pacemaker e Corosync no SLES ou no RHEL.
- Pelo menos duas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em que as instâncias (ABAP) do SAP Central Services (ASCS/SCS) e do Enqueue Replication Server (ERS) estão em execução.
- Conhecimento de gerenciamento de aplicativos e clusters SAP.
- Acesso ao ambiente Linux como usuário raiz.

Limitações

- ENSA1clusters baseados oferecem suporte somente a uma arquitetura de dois nós.
- ENSA2clusters baseados não podem ser implantados em NetWeaver versões do SAP anteriores à 7.52.
- EC2 instâncias em clusters devem estar em diferentes zonas de disponibilidade da AWS.

Versões do produto

- SAP NetWeaver versão 7.52 ou posterior
- A partir do S/4HANA 2020, somente clusters são suportados ENSA2
- Kernel 7.53 ou posterior, que suporta o Enqueue ENSA2 Replicator 2
- SLES para aplicativos SAP versão 12 ou superior
- RHEL para SAP com alta disponibilidade (HA) versão 7.9 ou superior

Arquitetura

Pilha de tecnologia de origem

- SAP NetWeaver 7.52 com SAP Kernel 7.53 ou posterior
- Sistema operacional SLES ou RHEL

Pilha de tecnologias de destino

- SAP NetWeaver 7.52 com SAP Kernel 7.53 ou posterior, incluindo S/4HANA 2020 com plataforma ABAP
- Sistema operacional SLES ou RHEL

Arquitetura de destino

O diagrama a seguir mostra uma configuração de HA das instâncias ASCS/SCS e ERS com base em um cluster. ENSA2

Comparação de ENSA2 clusters ENSA1 e clusters

A SAP foi apresentada ENSA2 como sucessora da. ENSA1 Um cluster ENSA1 baseado oferece suporte a uma arquitetura de dois nós em que a ASCS/SCS instance fails over to ERS when an error occurs. This limitation stems from how the ASCS/SCS instance regains the lock table information from the shared memory of the ERS node after failover. ENSA2-based clusters with Enqueue Replicator 2 eliminate this limitation, because the ASCS/SCS instance can collect the lock information from the ERS instance over the network. ENSA2-based clusters can have more than two nodes, because the ASCS/SCS instance is no longer required to fail over to the ERS node. (However, in a two-node ENSA2 cluster environment, the ASCS/SCS instância ainda fará o failover para o nó ERS porque não há outros nós no cluster para os quais realizar o failover.) ENSA2 é suportado a partir do SAP Kernel 7.50 com algumas limitações. Para a configuração de HA compatível com o Enqueue Replicator 2, o requisito mínimo é NetWeaver 7,52 (consulte a nota 2630416 do SAP OSS). O S/4HANA 1809 vem com a ENSA2 arquitetura recomendada por padrão, enquanto o S/4HANA oferece suporte somente a partir da versão 2020. ENSA2

Automação e escala

O cluster HA na arquitetura de destino faz com que o ASCS faça o failover para outros nós automaticamente.

Cenários para migrar para clusters ENSA2 baseados

Há dois cenários principais para fazer o upgrade para clusters ENSA2 baseados:

- Cenário 1: Você opta por fazer o upgrade para o SAP ou a conversão S/4HANA ENSA2 sem acompanhamento, supondo que sua versão do SAP e a versão do Kernel sejam compatíveis. ENSA2
- Cenário 2: Você passa para ENSA2 como parte de uma atualização ou conversão (por exemplo, para S/4HANA 1809 ou posterior) usando SUM.

A seção Épicos aborda as etapas desses dois cenários. O primeiro cenário exige que você configure manualmente os parâmetros relacionados ao SAP antes de alterar a configuração do cluster para ENSA2. No segundo cenário, os binários e os parâmetros relacionados ao SAP são implantados pelo SUM, e sua única tarefa restante é atualizar a configuração do cluster para HA. Ainda recomendamos que você valide os parâmetros do SAP depois de usar o SUM. Na maioria dos casos, a conversão S/4HANA é o principal motivo para uma atualização do cluster.

Ferramentas

- Para gerenciadores de pacotes do sistema operacional, recomendamos as ferramentas Zypper (para SLES) ou YUM (para RHEL).
- Para gerenciamento de clusters, recomendamos os shells crm (para SLES) ou pcs (para RHEL).
- Ferramentas de gerenciamento de instâncias SAP, como SAPControl.
- (Opcional) Ferramenta SUM para atualização de conversão S/4HANA.

Práticas recomendadas

- Para obter as melhores práticas de uso de workloads SAP na AWS, consulte o SAP Lens para o AWS Well-Architected Framework.
- Considere o número de nós de cluster (pares ou ímpares) em sua arquitetura de ENSA2 vários nós.
- Configure o ENSA2 cluster para o SLES 15 em alinhamento com o padrão de certificação SAP S/4-HA-CLU 1.0.
- Sempre salve ou faça backup do estado atual do cluster e do aplicativo antes de fazer o upgrade para o. ENSA2

Épicos

Configure os parâmetros do SAP manualmente para ENSA2 (somente cenário 1)

Tarefa	Descrição	Habilidades necessárias
Configure os parâmetros no perfil padrão.	Se você quiser fazer o upgrade para ENSA2 enquanto permanece na mesma versão do SAP ou se a versão de destino for padronizada ENSA1, defina os parâmetros no perfil padrão (arquivo DEFAULT.PFL) com os seguintes valores. `enq/enable=TRUE`	SAP

Tarefa	Descrição	Habilidades necessárias

	`enq/serverhost=sapas csvirt`
	`enq/serverinst=10`
	`(instance number of ASCS/SCS instance)`
	`enque/process_loc ation=REMOTESA`
	`enq/replicatorhost=sa persvirt`
	`enq/replicatorinst=11`
	`(instance number of ERS instance)`
	
	onde `sapascsvirt` é o nome do host virtual das instâncias do ASCS e `sapersvirt` é o nome do host virtual das instâncias do ERS. Você pode alterá-los para se adequar ao seu ambiente de destino.
	
	Note
	Para usar essa opção de upgrade, sua versão SAP e a versão do Kernel devem suportar o Enqueue ENSA2 Replicator 2.	

Tarefa	Descrição	Habilidades necessárias
Configure o perfil de instância ASCS/SCS.	Se você quiser fazer o upgrade para a ENSA2 mesma versão do SAP ou se a versão de destino for padronizada ENSA1, defina os seguintes parâmetros no perfil da instância ASCS/SCS. A seção do perfil em que ENSA1 está definido se parece com a seguinte. `#----------------- ----------------- ----------------- --------- Start SAP enqueue server #------------------ ----------------- ----------------- ------- _EN = en.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_04 = local rm - f $(_EN) Execute_05 = local ln - s -f $(DIR_EXECUTABLE)/ enserver$(FT_EXE) $(_EN) Start_Program_01 = local $(_EN) pf=$(_PF)` Para reconfigurar esta seção para ENSA2:	SAP

Tarefa	Descrição	Habilidades necessárias
	1. Altere o prefixo do programa `_EN` para `_ENQ` com base nas informaçõ es mais recentes da SAP (OSS Note 2501860; requer uma conta de usuário do SAP ONE Support Launchpad). 2. Altere o binário do servidor em fila de `enserver` para `enq_server` . 3. Defina o novo parâmetro `enq/server/replica tion/enable` para `TRUE`. 4. Verifique se está em `Autostart = 0`. Essa sessão do perfil ficaria com algo semelhante ao seguinte após suas alteraçõe s. `#----------` `----------` `----------` `---------` `Start SAP enqueue server` `#----------` `----------` `----------` `-------` `_ENQ = enq.sap$( SAPSYSTEMNAME)$(IN STANCE_NAME)`	

Tarefa	Descrição	Habilidades necessárias

	`Execute_04 = local rm -f $(_ENQ)`
	`Execute_05 = local ln -s -f $(DIR_EXECUTABLE)/enq_server$(FT_EXE) $(_ENQ)`
	`Start_Program_01 = local $(_ENQ) pf=$(_PF)`
	`...`
	`enq/server/replication/enable = TRUE`
	`Autostart = 0`
	
	Important
	_ENQnão deve ter a opção de reinicialização ativada. Se `RestartProgram_01` estiver definido para _ENQ, altere-o para `StartProgram_01` . Isso impede que o SAP reinicie o serviço ou interfira nos recursos gerenciados pelo cluster.	

Tarefa	Descrição	Habilidades necessárias
Configure o perfil ERS.	Se você quiser fazer o upgrade para ENSA2 a mesma versão do SAP ou se a versão de destino for padronizada ENSA1, defina os seguintes parâmetros no perfil da instância ERS. Encontre a seção em que o replicador de enqueue está definido. Ele será similar ao seguinte. `#------------------ ------------------ ------------------- Start enqueue replicati on server #------------------- ------------------ ------------------ _ER = er.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_03 = local rm - f $(_ER) Execute_04 = local ln - s -f $(DIR_EXECUTABLE)/ enrepserver$(FT_EXE) $(_ER) Start_Program_00 = local $(_ER) pf=$(_PF) NR=$(SCSID)` Para reconfigurar esta seção para o Enqueue Replicator 2:	SAP

Tarefa	Descrição	Habilidades necessárias

	1. Altere o prefixo `_ER` do programa para `_ENQR` com base nas notas mais recentes da SAP (OSS Note 2501860; requer uma conta de usuário do SAP ONE Support Launchpad).
	2. Altere o binário do replicador de enqueue para `enq_replicator` em vez de `enrepserver`.
	3. Verifique se está em `Autostart = 0`.
	
	Essa sessão do perfil deve parecer com algo semelhante ao seguinte após as alterações.
	
	`#----------`
	`----------`
	`----------`
	`Start enqueue replicati`
	`on server`
	`#----------`
	`----------`
	`----------`
	`_ENQR = enqr.sap$`
	`(SAPSYSTEMNAME)$(I`
	`NSTANCE_NAME)`
	`Execute_01 = local rm -`
	`f $(_ENQR)`
	`Execute_02 = local ln -`
	`s -f $(DIR_EXECUTABLE)/`
	`enq_replicator$(FT`
	`_EXE) $(_ENQR)`	

Tarefa	Descrição	Habilidades necessárias
	`Start_Program_00 = local $(_ENQR) pf= $(_PF) NR=$(SCSID) … Autostart = 0`	
	Important `_ENQR`não deve ter a opção de reinicialização ativada. Se `RestartProgram_01` estiver definido para `_ENQR`, altere-o para `StartProgram_01`. Isso impede que o SAP reinicie o serviço ou interfira nos serviços gerenciados por cluster.	

Tarefa	Descrição	Habilidades necessárias

Reinicie o SAP Start Services.	Depois de alterar os perfis descritos anteriormente neste épico, reinicie o SAP Start Services para ASCS/SCS e ERS.
	
	`sapcontrol -nr 10 -function RestartService SCT`
	
	`sapcontrol -nr 11 -function RestartService SCT`
	
	onde `SCT` se refere à ID do sistema SAP e supondo que 10 e 11 sejam os números de instância das instâncias ASCS/SCS e ERS, respectivamente.
		SAP

Reconfigure o cluster para ENSA2 (necessário para ambos os cenários)

Tarefa	Descrição	Habilidades necessárias
Verifique os números de versão nos agentes de recursos do SAP.	Quando você usa o SUM para atualizar o SAP para o S/4HANA 1809 ou superior, o SUM manipula as alterações de parâmetros nos perfis do SAP. Somente o cluster requer ajuste manual. No entanto, recomendamos que você verifique as configurações dos parâmetros antes de	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	fazer qualquer alteração no cluster. **Note** Os exemplos desse épico pressupõem que você esteja usando o sistema operacional SUSE. Se você estiver usando o RHEL, precisará usar ferramentas como o YUM e o shell pcs em vez do Zypper e do crm. Verifique os dois nós na arquitetura para confirmar se o pacote `resource-agents` corresponde à versão mínima recomendada pela SAP. Para SLES, consulte SAP OSS Note 2641019. Para RHEL, consulte SAP OSS Note 2641322. (O SAP Notes exige uma conta de usuário do SAP ONE Support Launchpad.) `sapers:sctadm 23> zypper search -s -i resource-agents Loading repository data...`	

Tarefa	Descrição	Habilidades necessárias
	`Reading installed packages... S | Name | Type | Version | Arch | Repository --+------------ ----+---------+--- ------------------ ---------------+-- ------+---------- ------------------ i | resource-agents | package | 4.8.0+git30.d0077df0-150300.8.28.1 | x86_64 | SLE-Product-HA15-SP3-Updates` Atualize a versão `resource-agents` , se necessário.	
Faça backup da configuração do cluster.	Faça backup da configuração do cluster do CRM da seguinte maneira. `crm configure show > /tmp/cluster_config_backup.txt`	Administrador de sistemas AWS
Definir o modo de manutenção.	Defina o cluster para o modo de manutenção. `crm configure property maintenance-mode="true"`	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

Verifique a configuração do cluster.	Verifique a configuração atual do cluster.
	`crm configure show`
	Aqui está um trecho da saída completa:
	`node 1: sapascs`
	`node 2: sapers`
	`...`
	`primitive rsc_sap_S`
	`CT_ASCS10 SAPInstance`
	`\`
	`operations $id=rsc_s`
	`ap_SCT_ASCS10-oper`
	`ations \`
	`op monitor interval=120`
	`timeout=60 on-fail=r`
	`estart \`
	`params InstanceN`
	`ame=SCT_ASCS10_sap`
	`ascsvirt START_PRO`
	`FILE="/sapmnt/SCT/`
	`profile/SCT_ASCS10`
	`_sapascsvirt" \`
	`AUTOMATIC_RECOVER=`
	`false \`
	`meta resource-stickines`
	`s=5000 failure-t`
	`imeout=60 migration-`
	`threshold=1 priority=`
	`10`
	`primitive rsc_sap_S`
	`CT_ERS11 SAPInstance \`
	`operations $id=rsc_s`
	`ap_SCT_ERS11-opera`
	`tions \`
	`op monitor interval=120`
	`timeout=60 on-fail=r`
	`estart \`
		Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>params InstanceN
	ame=SCT_ERS11_sape
	rsvirt START_PRO
	FILE="/sapmnt/SCT/
	profile/SCT_ERS11_
	sapersvirt" \
	   AUTOMATIC_RECOVER=
	false IS_ERS=true \
	meta priority=1000
	...
	colocation col_sap_S
	CT_no_both -5000:
	 grp_SCT_ERS11
	 grp_SCT_ASCS10
	location loc_sap_S
	CT_failover_to_ers
	 rsc_sap_SCT_ASCS10 \
	rule 2000: runs_ers_SCT
	 eq 1
	order ord_sap_S
	CT_first_start_asc
	s Optional: rsc_sap_S
	CT_ASCS10:start
	 rsc_sap_SCT_ERS11:
	stop symmetrical=false
	...</pre>
	onde `sapascsvirt` refere-se ao nome do host virtual para as instâncias ASCS, `sapersvirt` refere-se ao nome do host virtual para as instâncias ERS e SCT refere-se à ID do sistema SAP.	

Tarefa	Descrição	Habilidades necessárias
Remova a restrição de colocalização de failover.	No exemplo anterior, a restrição de localização `loc_sap_SCT_failover_to_ers` especifica que o ENSA1 recurso do ASCS deve sempre seguir a instância ERS após o failover. Com ENSA2, o ASCS deve ser capaz de realizar o failover livremente em qualquer nó participante, para que você possa remover essa restrição. `crm configure delete loc_sap_SCT_failover_to_ers`	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
Ajuste as primitivas.	Você também precisará fazer pequenas alterações nas SAPInstance primitivas ASCS e ERS. Aqui está um exemplo de uma SAPInstance primitiva ASCS configurada para. ENSA1 `primitive rsc_sap_S CT_ASCS10 SAPInstance \ operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=5000 failure-t imeout=60 migration- threshold=1 priority= 10`  Para fazer o upgrade para ENSA2, altere essa configura ção para a seguinte.  `primitive rsc_sap_S CT_ASCS10 SAPInstance \`	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=3000 Este é um exemplo de uma SAPInstance primitiva ERS configurada para ENSA1. primitive rsc_sap_S CT_ERS11 SAPInstance \ operations $id=rsc_s ap_SCT_ERS11-opera tions \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true \ meta priority=1000	

Tarefa	Descrição	Habilidades necessárias

	Para fazer o upgrade para ENSA2, altere essa configuração para a seguinte.
	
	`primitive rsc_sap_SCT_ERS11 SAPInstance \ operations $id=rsc_sap_SCT_ERS11-operations \ op monitor interval=120 timeout=60 on-fail=restart \ params InstanceName=SCT_ERS11_sapersvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ERS11_sapersvirt" \ AUTOMATIC_RECOVER=false IS_ERS=true`
	
	Você pode alterar as primitivas de várias maneiras. Por exemplo, você pode revisá-las em um editor como o vi, conforme exemplo a seguir.
	
	`crm configure edit rsc_sap_SCT_ERS11`	

Tarefa	Descrição	Habilidades necessárias
Desativar o modo de manutenção.	Desative o modo de manutenção no cluster. `crm configure property maintenance-mode="false"` Quando o cluster está fora do modo de manutenção, ele tenta colocar as instâncias ASCS e ERS on-line com as novas ENSA2 configurações.	Administrador de sistemas AWS

(Opcional) Adicionar nós do cluster

Tarefa	Descrição	Habilidades necessárias
Examine as melhores práticas.	Antes de adicionar mais nós, certifique-se de entender as práticas recomendadas, como usar um número par ou ímpar de nós.	Administrador de sistemas AWS
Adicionar nós.	Adicionar mais nós envolve uma série de tarefas, como atualizar o sistema operacional, instalar pacotes de software que correspondam aos nós existentes e disponibilizar montagens. Você pode usar a opção Preparar host adicional no SAP Software Provisioning Manager (SWPM) para criar uma linha de base específic	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	a do SAP do host. Para obter mais informações, consulte os guias do SAP listados na próxima sessão.	

Recursos relacionados

Referências SAP e SUSE

Para acessar o SAP Notes, você deve ter uma conta de usuário do SAP ONE Support Launchpad. Para obter mais informações, consulte o site do suporte do SAP.

- SAP Note 2501860 – Documentação do SAP NetWeaver Application Server para ABAP 7.52
- SAP Note 2641019 – Instalação ENSA2 e atualização de ENSA1 para ENSA2 no ambiente SUSE HA
- SAP Note 2641322 – Instalação ENSA2 e atualização de ENSA1 para ENSA2 ao usar as soluções Red Hat HA para SAP
- Nota SAP 2711036 – Uso do Standalone Enqueue Server 2 em um ambiente HA
- Standalone Enqueue Server 2 (documentação do SAP)
- SAP S/4 HANA – Cluster de alta disponibilidade do Enqueue Replication 2 - Guia de configuração (documentação da SUSE)

Referências da AWS

- SAP HANA na AWS: guia de configuração de alta disponibilidade para SLES e RHEL
- SAP Lens - AWS Well-Architected Framework

Use zonas de disponibilidade consistentes VPCs em diferentes contas da AWS

Criado por Adam Spicer (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), uma zona de disponibilidade tem um nome que pode variar entre suas contas da AWS e uma ID de zona de disponibilidade (AZ ID) que identifica sua localização. Se você usa CloudFormation a AWS para criar nuvens privadas virtuais (VPCs), você deve especificar o nome ou ID da zona de disponibilidade ao criar as sub-redes. Se você criar VPCs em várias contas, o nome da zona de disponibilidade será aleatório, o que significa que as sub-redes usam zonas de disponibilidade diferentes em cada conta.

Para usar a mesma zona de disponibilidade em todas as suas contas, você deve mapear o nome da zona de disponibilidade em cada conta para a mesma ID AZ. Por exemplo, o diagrama a seguir mostra que o ID AZ `use1-az6` é nomeado `us-east-1a` na conta A da AWS e `us-east-1c` na conta Z da AWS.

Esse padrão ajuda a garantir a consistência zonal fornecendo uma solução escalável e multicontas para usar as mesmas zonas de disponibilidade em suas sub-redes. A consistência zonal garante que seu tráfego de rede entre contas evite caminhos de rede entre zonas de disponibilidade, o que ajuda a reduzir os custos de transferência de dados e a diminuir a latência de rede entre suas cargas de trabalho.

Esse padrão é uma abordagem alternativa para a CloudFormation AvailabilityZoneId propriedade da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Pelo menos duas contas ativas da AWS na mesma região da AWS.
- Avalie quantas zonas de disponibilidade são necessárias para atender aos seus requisitos de VPC na região.
- Identifique e registre a ID AZ para cada zona de disponibilidade que você precisa suportar. Para obter mais informações sobre isso, consulte Zona de disponibilidade IDs para seus recursos da AWS na documentação do AWS Resource Access Manager.

- Uma lista ordenada e separada por vírgulas do seu AZ. IDs Por exemplo, a primeira zona de disponibilidade em sua lista é mapeada como `az1`, a segunda zona de disponibilidade é mapeada como `az2`, e essa estrutura de mapeamento continua até que sua lista separada por vírgulas esteja totalmente mapeada. Não há um número máximo de AZ IDs que possa ser mapeado.
- O `az-mapping.yaml` arquivo do repositório de mapeamento da Zona de Disponibilidade de GitHub Várias Contas, copiado para sua máquina local

Arquitetura

O diagrama a seguir mostra a arquitetura que é implantada em uma conta e que cria valores do AWS Systems Manager Parameter Store. Esses valores do Parameter Store são consumidos quando você cria uma VPC na conta.

O diagrama mostra o seguinte fluxo de trabalho:

1. A solução desse padrão é implantada em todas as contas que exigem consistência zonal para uma VPC.
2. A solução cria valores de armazenamento de parâmetros para cada ID de AZ e armazena o novo nome da zona de disponibilidade.
3. O CloudFormation modelo da AWS usa o nome da zona de disponibilidade armazenado em cada valor do Parameter Store e isso garante a consistência zonal.

O diagrama a seguir mostra o fluxo de trabalho para criar uma VPC com a solução desse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. Envie um modelo para criar uma VPC para a AWS. CloudFormation
2. A AWS CloudFormation resolve os valores do Parameter Store para cada zona de disponibilidade e retorna o nome da zona de disponibilidade para cada ID de AZ.
3. Uma VPC é criada com a AZ correta IDs necessária para a consistência zonal.

Depois de implantar a solução desse padrão, você poderá criar sub-redes que façam referência aos valores do Parameter Store. Se você usa a AWS CloudFormation, pode referenciar os valores

dos parâmetros de mapeamento da zona de disponibilidade a partir do seguinte código de amostra formatado em YAML:

```
Resources:
    PrivateSubnet1AZ1:
        Type: AWS::EC2::Subnet
        Properties:
            VpcId: !Ref VPC
            CidrBlock: !Ref PrivateSubnetAZ1CIDR
            AvailabilityZone:
                !Join
                    - ''
                    - - '{{resolve:ssm:/az-mapping/az1:1}}'
```

Esse código de exemplo está contido no `vpc-example.yaml` arquivo do repositório de mapeamento da Zona de Disponibilidade de GitHub Várias Contas. Ele mostra como criar uma VPC e sub-redes que se alinham aos valores do Parameter Store para obter consistência zonal.

Pilha de tecnologia

- AWS CloudFormation
- AWS Lambda
- AWS Systems Manager Parameter Store

Automação e escala

Você pode implantar esse padrão em todas as suas contas da AWS usando a AWS CloudFormation StackSets ou a solução Customizations for AWS Control Tower. Para obter mais informações, consulte Como trabalhar com a AWS CloudFormation StackSets na documentação do AWS Cloudformation e Personalizações para o AWS Control Tower na Biblioteca de Soluções da AWS.

Depois de implantar o CloudFormation modelo da AWS, você pode atualizá-lo para usar os valores do Parameter Store e implantá-los VPCs em pipelines ou de acordo com seus requisitos.

Ferramentas

Serviços da AWS

- CloudFormationA AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um

modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em várias contas e regiões da AWS.

- O AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- O AWS Systems Manager Parameter Store é um recurso do AWS Systems Manager. Oferece armazenamento hierárquico seguro para gerenciamento de dados de configuração e gerenciamento de segredos.

Código

O código desse padrão é fornecido no repositório de mapeamento da Zona de Disponibilidade de GitHub Várias Contas.

Épicos

Implante o arquivo az-mapping.yaml

Tarefa	Descrição	Habilidades necessárias
Determine as zonas de disponibilidade necessárias para a região.	1. Determine a AZ IDs que deve ser usada de forma consistente em sua região. 2. Registre essas AZ IDs em uma lista separada por vírgulas e na ordem em que você deseja que sejam aplicadas. Por exemplo, a primeira zona de disponibilidade em sua lista é mapeada como `az1` e a segunda é mapeada como `az2`. Não há um	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	número máximo de AZ IDs que possa ser mapeado.	
Implante o arquivo az-mapping.yaml	Use o `az-mapping.yaml` arquivo para criar uma CloudFormation pilha da AWS em todas as contas da AWS necessárias. No parâmetro `AZIds`, use a lista separada por vírgulas que você criou anteriormente. Recomendamos que você use a AWS CloudFormation StackSets ou a solução Customizations for AWS Control Tower.	Arquiteto de nuvem

Implemente o VPCs em suas contas

Tarefa	Descrição	Habilidades necessárias
Personalize os CloudFormation modelos da AWS.	Ao criar as sub-redes usando a AWS CloudFormation, personalize os modelos para usar os valores do Parameter Store que você criou anteriormente. Para ver um modelo de amostra, consulte o `vpc-example.yaml` arquivo no repositório de mapeamento da Zona de Disponibilidade de GitHub Várias Contas.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Implante VPCs o.	Implante os CloudFormation modelos personalizados da AWS em suas contas. Cada VPC na região, então, tem consistência zonal nas zonas de disponibilidade usadas para as sub-redes	Arquiteto de nuvem

Recursos relacionados

- Zona de disponibilidade IDs para seus recursos da AWS (documentação do AWS Resource Access Manager)
- AWS::EC2::Subnet(CloudFormation Documentação da AWS)

Use o usuário IDs nas políticas do IAM para controle de acesso e automação

Criado por Srinivas Ananda Babu (AWS) e Ram Kandaswamy (AWS)

Resumo

Esse padrão explica as possíveis armadilhas do uso de políticas baseadas em nome de usuário no AWS Identity and Access Management (IAM), os benefícios de usar o usuário IDs e como integrar essa abordagem à automação. AWS CloudFormation

No Nuvem AWS, o serviço IAM ajuda você a gerenciar as identidades dos usuários e o controle de acesso com precisão. No entanto, confiar nos nomes de usuário na criação de políticas do IAM pode levar a riscos de segurança imprevistos e problemas de controle de acesso. Por exemplo, considere este cenário: um novo funcionário, John Doe, se junta à sua equipe e você cria uma conta de usuário do IAM com o nome de usuário`j.doe`, que concede permissões por meio de políticas do IAM que fazem referência a nomes de usuário. Quando John sai da empresa, a conta é excluída. O problema começa quando uma nova funcionária, Jane Doe, se junta à sua equipe e o `j.doe` nome de usuário é recriado. As políticas existentes agora concedem a Jane Doe as mesmas permissões de John Doe. Isso cria um potencial pesadelo de segurança e conformidade.

A atualização manual de cada política para refletir os novos detalhes do usuário é um processo demorado e propenso a erros, especialmente à medida que sua organização cresce. A solução é usar um ID de usuário exclusivo e imutável. Ao criar uma conta de usuário do IAM, AWS atribui ao usuário do IAM um ID de usuário exclusivo (ou ID principal). Você pode usar esses usuários IDs em suas políticas do IAM para garantir um controle de acesso consistente e confiável que não seja afetado pelas alterações ou reutilização do nome de usuário.

Por exemplo, uma política do IAM que usa um ID de usuário pode ter a seguinte aparência:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::example-bucket",
            "Principal": { "AWS": "arn:aws:iam::123456789012:user/abcdef01234567890" }
        }
      ]
```

```
}
```

Os benefícios de usar o usuário IDs nas políticas do IAM incluem:

- Exclusividade. IDs Os usuários são únicos em todos Contas da AWS, portanto, fornecem uma aplicação de permissão correta e consistente.
- Imutabilidade. O usuário IDs não pode ser alterado, então eles fornecem um identificador estável para referenciar usuários nas políticas.
- Auditoria e conformidade. Serviços da AWS geralmente incluem o usuário IDs em registros e trilhas de auditoria, o que facilita o rastreamento de ações até usuários específicos.
- Automação e integração. O uso de scripts IDs de AWS APIs entrada SDKs de usuário ou de automação garante que os processos permaneçam inalterados pelas alterações do nome de usuário.
- Preparado para o futuro. Usar o usuário IDs nas políticas desde o início pode evitar possíveis problemas de controle de acesso ou extensas atualizações de políticas.

Automação

Quando você usa ferramentas de infraestrutura como código (IaC) AWS CloudFormation, como as armadilhas das políticas de IAM baseadas em nome de usuário, ainda podem causar problemas. O recurso de usuário do IAM retorna o nome de usuário quando você chama a função `Ref` intrínseca. À medida que a infraestrutura da sua organização evolui, o ciclo de criação e exclusão de recursos, incluindo contas de usuário do IAM, pode levar a problemas de controle de acesso não intencionais se você reutilizar nomes de usuário.

Para resolver esse problema, recomendamos que você incorpore o usuário IDs em seus CloudFormation modelos. No entanto, obter um usuário IDs para essa finalidade pode ser um desafio. É aqui que os recursos personalizados podem ser úteis. Você pode usar recursos CloudFormation personalizados para ampliar a funcionalidade do serviço por meio da integração com AWS APIs ou de serviços externos. Ao criar um recurso personalizado que busca o ID do usuário de um determinado usuário do IAM, você pode disponibilizar o ID do usuário nos seus CloudFormation modelos. Essa abordagem simplifica o processo de referenciar o usuário IDs e garante que seus fluxos de trabalho de automação permaneçam robustos e preparados para o futuro.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Uma função do IAM para um administrador de nuvem executar o AWS CloudFormation modelo

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Arquitetura de destino

O diagrama a seguir mostra como AWS CloudFormation usa um recurso personalizado apoiado por AWS Lambda para recuperar o ID de usuário do IAM.

Automação e escala

Você pode usar o CloudFormation modelo várias vezes para contas diferentes Regiões da AWS . Você precisa executá-lo apenas uma vez em cada região ou conta.

Ferramentas

Serviços da AWS

- IAM — AWS Identity and Access Management (IAM) é um serviço web que ajuda você a controlar com segurança o acesso aos AWS recursos. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.
- AWS CloudFormation— AWS CloudFormation ajuda você a modelar e configurar seus AWS recursos para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando nos aplicativos que são executados AWS. Você cria um modelo que descreve os AWS recursos que você deseja e CloudFormation se encarrega de provisionar e configurar esses recursos para você.
- AWS Lambda— AWS Lambda é um serviço de computação que oferece suporte à execução de código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.

Práticas recomendadas

Se você está começando do zero ou planejando uma implantação nova, é altamente recomendável que você use AWS IAM Identity Centerpara gerenciamento centralizado de usuários. O IAM Identity Center se integra aos seus provedores de identidade existentes (como Active Directory ou Okta) para federar identidades de usuários AWS, o que elimina a necessidade de criar e gerenciar usuários do IAM diretamente. Essa abordagem não apenas garante um controle de acesso consistente, mas também simplifica o gerenciamento do ciclo de vida do usuário e ajuda a aprimorar a segurança e a conformidade em todo o seu ambiente. AWS

Épicos

Valide as permissões

Tarefa	Descrição	Habilidades necessárias
Valide sua função Conta da AWS e do IAM.	Confirme se você tem uma função do IAM com permissões para implantar CloudFormation modelos no seu Conta da AWS. Se você planeja usar o AWS CLI em vez do CloudFormation console para implantar o modelo na última etapa desse procedimento, você também deve configurar credenciais temporárias para executar AWS CLI comandos. Para obter instruções, consulte a documentação do IAM.	Arquiteto de nuvem

Crie um CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Crie um CloudFormation modelo.	1. Crie um CloudFormation modelo seguindo as instruções na CloudFormation documentação. Você pode usar o formato JSON ou YAML. Esse padrão pressupõe que você esteja usando o formato YAML. 2. Salve o modelo com o nome `get_unique_user_id.yaml` .	AWS DevOps, arquiteto de nuvem

Adicione um parâmetro de entrada para o nome de usuário.	Adicione o código a seguir à `Parameters` seção do CloudFormation modelo:
	`Parameters:`
	`  NewIamUserName:`
	`  Type: String`
	`  Description: Unique username for the new IAM user`
	Esse parâmetro solicita ao usuário o nome de usuário.
		AWS DevOps, arquiteto de nuvem

Adicione um recurso personalizado para criar um usuário do IAM.	Adicione o código a seguir à `Resources` seção do CloudFormation modelo:
	`Resources:`
	`  rNewIamUser:`
	`  Type: 'AWS::IAM::User'`
	`  Properties:`
		AWS DevOps, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`UserName: !Ref NewIamUserName` Esse código adiciona um CloudFormation recurso que cria um usuário do IAM com o nome fornecido pelo `NewIamUserName` parâmetro.	

Tarefa	Descrição	Habilidades necessárias
Adicione uma função de execução para a função Lambda.	Nesta etapa, você cria uma função do IAM que concede uma permissão de AWS Lambda função para obter o IAM`UserId`. Especifique as seguintes permissões mínimas necessárias para a execução do Lambda: • `logs:CreateLogStream` • `logs:PutLogEvents` • `CreateLogGroup` • `iam:GetUser` • `AssumeRole` para `lambda.amazonaws.com` Para obter instruções sobre como criar uma função de execução, consulte a documentação do Lambda. Você referenciará essa função na próxima etapa, ao criar a função Lambda.	Administrador da AWS, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

Adicione uma função Lambda para obter o IAM exclusivo. `UserId`	Nesta etapa, você define uma função Lambda com um tempo de execução do Python para obter o IAM exclusivo . `UserId` Para fazer isso, adicione o código a seguir à `Resources` seção do CloudFormation modelo. `<<ROLENAME>>` Substitua pelo nome da função de execução que você criou na última etapa.
	
	`GetUserLambdaFunction:`
	`Type: 'AWS::Lambda::Function'`
	`Properties:`
	`Handler: index.handler`
	`Role: <<ROLENAME>>`
	`Timeout: 30`
	`Runtime: python3.11`
	`Code:`
	`ZipFile: |`
	`import cfnresponse, boto3`
	`def handler(event, context):`
	`try:`
	`print(event)`
	`user = boto3.client('iam').get_user(UserName=event['ResourceP`
		AWS DevOps, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	roperties'][NewIa mUserName'])['User'] cfnrespon se.send(event, context, cfnrespon se.SUCCESS, {'NewIamU serId': user['Use rId'], 'NewIamUs erPath': user['Pat h'], 'NewIamUserArn': user['Arn']}) except Exception as e: cfnrespon se.send(event, context, cfnrespon se.FAILED, {'NewIamU ser': str(e)})	
Adicione um recurso personalizado.	Adicione o código a seguir à `Resources` seção do CloudFormation modelo: `rCustomGetUniqueUserId: Type: 'Custom::rCustomGetUniqueUserIdWithLambda' Properties: ServiceToken: !GetAtt GetUserLambdaFunction.Arn NewIamUserName: !Ref NewIamUserName` Esse recurso personalizado chama a função Lambda para obter o IAM. `UserID`	AWS DevOps, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

Defina as CloudFormation saídas.	Adicione o código a seguir à `Outputs` seção do CloudFormation modelo:
	`Outputs:`
	`  NewIamUserId:`
	`  Value: !GetAtt rCustomGetUniqueUserId.NewIamUserId`
	Isso exibe o IAM `UserID` para o novo usuário do IAM.
		AWS DevOps, arquiteto de nuvem

Salve o modelo.	Salve suas alterações no CloudFormation modelo.	AWS DevOps, arquiteto de nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	Para implantar o `get_unique_user_id.yaml` modelo usando o CloudFormation console, siga as instruções na CloudFormation documentação. Como alternativa, você pode executar o seguinte AWS CLI comando para implantar o modelo: `aws cloudformation create-stack \`	AWS DevOps, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

	`--stack-name DemoNewUser \`
	`--template-body file://get_unique_user_id.yaml \`
	`--parameters ParameterKey=NewIamUserName,ParameterValue=demouser \`
	`--capabilities CAPABILITY_NAMED_IAM`	

Recursos relacionados

- Crie uma pilha a partir do CloudFormation console (CloudFormation documentação)
- Recursos personalizados apoiados pelo Lambda (documentação) CloudFormation
- Identificadores exclusivos (documentação do IAM)
- Use credenciais temporárias com AWS recursos (documentação do IAM)

Valide o código do Account Factory for Terraform (AFT) localmente

Criado por Alexandru Pop (AWS) e Michal Gorniak (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão mostra como testar localmente o código do HashiCorp Terraform gerenciado pelo AWS Control Tower Account Factory for Terraform (AFT). O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem. O AFT configura um pipeline do Terraform que ajuda você a provisionar e personalizar várias entradas Contas da AWS . AWS Control Tower

Durante o desenvolvimento do código, pode ser útil testar sua infraestrutura como código (IaC) do Terraform localmente, fora do pipeline do AFT. Este padrão mostra como fazer o seguinte:

- Recupere uma cópia local do código do Terraform que está armazenado nos AWS CodeCommit repositórios da sua conta de gerenciamento do AFT.
- Simular o pipeline AFT localmente usando o código recuperado.

Esse procedimento também pode ser usado para executar comandos do Terraform que não fazem parte do pipeline AFT normal. Por exemplo, você pode usar esse método para executar comandos como `terraform validate`, `terraform plan`, `terraform destroy` e `terraform import`.

Pré-requisitos e limitações

Pré-requisitos

- Um ambiente ativo AWS de várias contas que usa AWS Control Tower
- Um ambiente AFT totalmente implantado
- AWS Command Line Interface (AWS CLI), instalado e configurado
- AWS CLI auxiliar de credencial para AWS CodeCommit, instalado e configurado
- Python 3.x
- Git, instalado e configurado em sua máquina local
- `git-remote-commit`utilitário, instalado e configurado

- Terraform, instalado e configurado (a versão local do pacote Terraform deve corresponder à versão usada na implantação do AFT)

Limitações

- Esse padrão não abrange as etapas de implantação necessárias para AWS Control Tower o AFT ou qualquer módulo específico do Terraform.
- A saída gerada localmente durante esse procedimento não é salva nos logs de runtime do pipeline AFT.

Arquitetura

Pilha de tecnologias de destino

- Infraestrutura AFT implantada em uma AWS Control Tower implantação
- Terraform
- Git
- AWS CLI versão 2

Automação e escala

Esse padrão mostra como invocar localmente o código do Terraform para personalizações de contas globais AFT em um único AFT gerenciado. Conta da AWS Depois que seu código do Terraform for validado, você poderá aplicá-lo às contas restantes em seu ambiente de várias contas. Para obter mais informações, consulte Reinvocar personalizações na documentação. AWS Control Tower

Você também pode usar um processo semelhante para executar personalizações de contas do AFT em um terminal local. Para invocar localmente o código do Terraform a partir das personalizações da conta AFT, clone o aft-account-customizationsrepositório em vez do repositório na sua conta de gerenciamento do aft-global-account-customizationsAFT. CodeCommit

Ferramentas

Serviços da AWS

- AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas.

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.

Outros serviços

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.
- O Git é um sistema de controle de versão distribuído e de código aberto.

Código

Veja a seguir um exemplo de script bash que pode ser usado para executar localmente o código do Terraform gerenciado pelo AFT. Para usar o script, siga as instruções na seção Épicos desse padrão.

```
#! /bin/bash
# Version: 1.1 2022-06-24 Unsetting AWS_PROFILE since, when set, it interferes with
 script operation
#          1.0 2022-02-02 Initial Version
#
# Purpose: For use with AFT: This script runs the local copy of TF code as if it were
 running within AFT pipeline.
#        * Facilitates testing of what the AFT pipline will do
#           * Provides the ability to run terraform with custom arguments (like 'plan'
 or 'move') which are currently not supported within the pipeline.
#
# © 2021 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.
# This AWS Content is provided subject to the terms of the AWS Customer Agreement
# available at http://aws.amazon.com/agreement or other written agreement between
# Customer and either Amazon Web Services, Inc. or Amazon Web Services EMEA SARL or
 both.
#
# Note: Arguments to this script are passed directly to 'terraform' without parsing nor
 validation by this script.
#
# Prerequisites:
#    1. local copy of ct GIT repositories
#    2. local backend.tf and aft-providers.tf filled with data for the target account
 on which terraform is to be run
#       Hint: The contents of above files can be obtain from the logs of a previous
 execution of the AFT pipeline for the target account.
```

```
#    3. 'terraform' binary is available in local PATH
#    4. Recommended: .gitignore file containing 'backend.tf', 'aft_providers.tf' so the
 local copy of these files are not pushed back to git

readonly credentials=$(aws sts assume-role \
    --role-arn arn:aws:iam::$(aws sts get-caller-identity --query "Account" --output
 text ):role/AWSAFTAdmin \
    --role-session-name AWSAFT-Session \
    --query Credentials )

unset AWS_PROFILE
export AWS_ACCESS_KEY_ID=$(echo $credentials | jq -r '.AccessKeyId')
export AWS_SECRET_ACCESS_KEY=$(echo $credentials | jq -r '.SecretAccessKey')
export AWS_SESSION_TOKEN=$(echo $credentials | jq -r '.SessionToken')
terraform "$@"
```

Épicos

Salve o código de exemplo como um arquivo local

Tarefa	Descrição	Habilidades necessárias
Salve o código de exemplo como um arquivo local.	1. Copie o exemplo de script bash que está na seção Código desse padrão e cole-o em um editor de código. 2. Dê um nome ao arquivo `ct_terraform.sh` e salve-o localmente dentro de uma pasta dedicada, como `~/scripts` ou `~/bin`.	Administrador da AWS
Torne o código de exemplo executável.	Abra uma janela de terminal e autentique-se em sua conta de gerenciamento do AWS AFT fazendo o seguinte:	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	• Use um AWS CLI perfil existente configurado com as permissões necessárias para acessar a conta de gerenciamento do AFT. Para usar o perfil, você pode executar o comando a seguir: `export AWS_PROFILE=<aft account profile name>` • Se sua organização usa o SSO para acessar AWS, insira as credenciais da sua conta de gerenciamento do AFT na página de SSO da sua organização. **Note** Sua organização também pode ter uma ferramenta personalizada para fornecer credenciais de autenticação ao seu AWS ambiente.	

Tarefa	Descrição	Habilidades necessárias

Verifique se o acesso à conta de gerenciamento do AFT está correto Região da AWS.	**⚠ Important**
	Certifique-se de usar a mesma sessão de terminal com a qual você se autentico u em sua conta de gerenciamento do AFT.
	
	1. Navegue até sua implantaç ão do AFT Região da AWS executando o seguinte comando:
	`export AWS_REGIO N=<aft_region>`
	2. Verifique se você está na conta correta.
	a. Execute o seguinte comando:
	`aws code-commit list-repositories`
	b. Verifique se os repositór ios listados na saída correspondem aos nomes dos repositórios que estão na sua conta de gerenciamento do AFT.
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Crie um novo diretório local para armazenar o código do repositório do AFT.	Na mesma sessão de terminal, execute os comandos a seguir:
	`mkdir my_aft`
	`cd my_aft`
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Clone o código do repositório do AFT remoto.	1. Em seu terminal local, execute o seguinte comando: `git clone codecommit::$AWS_REGION://aft-global-customizations` **Note** Para simplificar, esse procedimento e o AFT usam somente uma ramificação de código principal. Para usar a ramificação de código, você também pode inserir comandos de ramificação de código aqui. No entanto, todas as alterações aplicadas da ramificação não principal serão revertidas quando a automação do AFT aplicar o código da ramificação principal.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	2. Navegue até o diretório clonado: `cd aft-global-customizations/terraform`	

Crie os arquivos de configuração do Terraform necessários para que o pipeline do AFT seja executado localmente

Tarefa	Descrição	Habilidades necessárias
Abra um pipeline do AFT executado anteriormente e copie os arquivos de configuração do Terraform em uma pasta local.	**Note** Os arquivos `backend.tf` e de `aft-providers.tf` configuração criados neste épico são necessários para que o pipeline do AFT seja executado localmente. Esses arquivos são criados automaticamente no pipeline do AFT baseado em nuvem, mas devem ser criados manualmente para que o pipeline seja executado localmente. Executar o pipeline AFT localmente requer um conjunto de arquivos que	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	representam a execução do pipeline em um único Conta da AWS. 1. Usando as credenciais da sua conta de AWS Control Tower gerenciamento, entre no e abra o AWS CodePipeline console. AWS Management Console Verifique se você está no mesmo Região da AWS local em que implantou o AFT. 2. No painel de navegação à esquerda, selecione Pipelines. 3. Escolha ############-customizations-pipeline. (O ############ é o Conta da AWS ID que você está usando para executar o código do Terraform localmente.) 4. Certifique-se de que a opção Execução mais recente marcada mostre um valor Bem-sucedido. Se o valor for diferente, você deverá invocar novamente suas personalizações no pipeline do AFT. Para obter	

Tarefa	Descrição	Habilidades necessárias
	mais informações, consulte Reinvocar personalizações na documentação. AWS Control Tower 5. Escolha o runtime mais recente para exibir seus detalhes. 6. Na seção Apply-AFT-Global-Customizations, encontre o estágio Apply-Terraform. 7. Selecione a seção Detalhes do estágio Apply-Terraform. 8. Encontre o log de runtime para o estágio Apply-Ter raform. 9. No registro de tempo de execução, procure a seção que começa e termina com as seguintes linhas: `"\n\n aft-provi ders.tf ... "\n \n backend.tf"` 10. Copie a saída entre esses dois rótulos e salve-os como um arquivo local nomeado `aft-provi ders.tf` na pasta local do Terraform (o diretório de trabalho atual da sua sessão de terminal).	

Tarefa	Descrição	Habilidades necessárias

	Exemplo de declaração providers.tf gerada automaticamente
	
	``
	## Autogenerated providers.tf ##
	## Updated on: 2022-05-31 16:27:45 ##
	provider "aws" {
	  region = "us-east-2"
	  assume_role {
	    role_arn = "arn:aws:iam::########:role/AWSAFTExecution"
	  }
	  default_tags {
	    tags = {
	      managed_by = "AFT"
	    }
	  }
	}
	``
	
	11. No registro de tempo de execução, procure a seção que começa e termina com as seguintes linhas:
	
	``
	"\n\n tf
	...
	"\n \n backend.tf"
	``
	
	12. Copie a saída entre esses dois rótulos e salve-os como um arquivo local nomeado `tf` na pasta local	

Tarefa	Descrição	Habilidades necessárias
	do Terraform (o diretório de trabalho atual da sua sessão de terminal). Exemplo de declaração backend.tf gerada automaticamente `## Autogenerated backend.tf ## ## Updated on: 2022-05-31 16:27:45 ## terraform { required_version = ">= 0.15.0" backend "s3" { region = "us-east-2" bucket = "aft-backend-###########-primary-region" key = "############-aft-global-customizations/terraform.tfstate" dynamodb_table = "aft-backend-#######" encrypt = "true" kms_key_id = "########-####-####-####-############" role_arn = "arn:aws:iam::#########:role/AWSAFTExecution" }`	

Tarefa	Descrição	Habilidades necessárias
	`}` **Note** Os `aft-providers.tf` arquivos `backend.tf` e estão vinculados a uma implantação e pasta específicas Conta da AWS do AFT. Esses arquivos também são diferentes, dependendo se estão no aft-account-customizationsrepositório aft-global-customizationse dentro da mesma implantação do AFT. Certifique-se de gerar os dois arquivos a partir da mesma listagem de runtime.	

Execute o pipeline do AFT localmente usando o script bash de exemplo

Tarefa	Descrição	Habilidades necessárias
Implemente as alterações de configuração do Terraform que você deseja validar.	1. Navegue até o aft-global-customizationsrepositório clonado executando o seguinte comando:	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`cd aft-global-customizations/terraform` **Note** Os arquivos `backend.tf` e `aft-providers.tf` estão nesse diretório. O diretório também contém arquivos Terraform do aft-global-customizations repositório. 2. Incorpore as alterações de código do Terraform que você deseja testar localmente nos arquivos de configuração.	

Tarefa	Descrição	Habilidades necessárias

Execute o `ct_terraform.sh` script e revise a saída.	1. Navegue até a pasta local que contém o script sh.
	2. Para validar seu código modificado do Terraform, execute o script `ct_terraform.sh` executando o seguinte comando:
	`~/scripts/ct_terraform.sh apply`
	`terraform --help`
	Note
	Você pode executar qualquer comando do Terraform durante essa etapa. Para ver uma lista completa dos comandos do Terraform, execute o seguinte comando:
	3. Revise a saída do comando e, em seguida, depure as alterações no código localmente antes de confirmar e enviar as alterações de volta para o repositório AFT.
		Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Important • Todas as alterações feitas localmente e não enviadas de volta ao repositório remoto são temporárias e podem ser desfeitas a qualquer momento por uma automação de pipeline do AFT em execução. • A automação do AFT pode ser executada a qualquer momento, pois pode ser invocada por outros usuários e acionadores de automação do AFT. • O AFT sempre aplicará o código da ramificação principal do repositório, desfazendo quaisquer alterações não confirmadas.	

Envie suas alterações de código local de volta para o repositório AFT

Tarefa	Descrição	Habilidades necessárias
Adicione referências aos `aft-providers.tf` arquivos `backend.tf` e a um `.gitignore` arquivo.	Adicione os arquivos `backend.tf` e `aft-providers.tf` que você criou a um arquivo `.gitignor`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	e executando os seguintes comandos:
	
	`echo backend.tf >> .gitignore`
	`echo aft-providers.tf >>.gitignore`
	
	Note
	Mover os arquivos para o `.gitignor` e arquivo garante que eles não sejam confirmados e enviados de volta para o repositório AFT remoto.	

Tarefa	Descrição	Habilidades necessárias

Confirme e envie suas alterações de código para o repositório do AFT remoto.	1. Para adicionar novos arquivos de configuração do Terraform ao repositór io, execute o seguinte comando:
	`git add <filename>`
	2. Para confirmar suas alterações e enviá-las para o repositório AFT remoto CodeCommitt, execute os seguintes comandos:
	`git commit -a`
	`git push`
	Important
	As alterações de código que você introduz seguindo esse procedimento até esse ponto são aplicadas Conta da AWS somente a uma.
		Administrador da AWS

Implemente as alterações em várias contas

Tarefa	Descrição	Habilidades necessárias
Implemente as alterações em todas as suas contas gerenciadas pela AFT.	Para implementar as alterações em várias Contas da AWS que são gerenciadas pelo AFT, siga as instruções em Reinvocar personalizações na documentação. AWS Control Tower	Administrador da AWS

Mais padrões

- Adicione HA ao Oracle PeopleSoft no Amazon RDS Custom usando uma réplica de leitura
- Audite automaticamente grupos AWS de segurança que permitem acesso a partir de endereços IP públicos
- Automatize a criação de contas usando o Landing Zone Accelerator em AWS
- Automatizar a adição ou atualização de entradas de registro do Windows usando o AWS Systems Manager
- Automatize a avaliação de recursos da AWS
- Automatize o portfólio e a implantação de produtos do AWS Service Catalog usando o AWS CDK
- Automatize o failover e o failback entre regiões usando o DR Orchestrator Framework
- Automatize a exclusão de AWS CloudFormation pilhas e recursos associados
- Automatize a ingestão e a visualização de métricas personalizadas do Amazon MWAA no Amazon Managed Grafana usando o Terraform
- Automatize a configuração RabbitMQ no Amazon MQ
- Automatize a replicação de instâncias do Amazon RDS em Contas da AWS
- Anexe automaticamente uma política gerenciada da AWS para Systems Manager aos perfis de EC2 instância usando o Cloud Custodian e o AWS CDK
- Compile automaticamente pipelines de CI/CD e clusters do Amazon ECS para microsserviços usando o AWS CDK
- Detecte alterações automaticamente e inicie diferentes CodePipeline pipelines para um monorepo em CodeCommit
- Reative automaticamente a AWS CloudTrail usando uma regra de remediação personalizada no AWS Config
- Crie um pipeline de dados para ingerir, transformar e analisar dados do Google Analytics usando o AWS DataOps Development Kit
- Crie um PAC de servidor corporativo da Micro Focus com o Amazon EC2 Auto Scaling e o Systems Manager
- Crie e envie imagens do Docker para o Amazon ECR usando GitHub Actions e Terraform
- Centralize o gerenciamento de chaves de acesso do IAM no AWS Organizations usando o Terraform
- Centralize a distribuição de pacotes de software no AWS Organizations usando o Terraform

- Reúna os serviços da AWS usando uma abordagem de tecnologia sem servidor
- Configure uma extensão de datacenter para a VMware nuvem na AWS usando o modo vinculado híbrido
- Configure o registro de invocação de modelo no Amazon Bedrock usando AWS CloudFormation
- Configurar o roteamento somente leitura em um grupo de disponibilidade Always On (Sempre ativo) no SQL Server na AWS
- Configurar o VMware vRealize Automation para provisionar VMs na VMware nuvem na AWS
- Crie um portal para microfrontends usando Angular e AWS Amplify Module Federation
- Crie uma EventBridge conexão entre contas da Amazon em uma organização
- Criar pipelines dinâmicos de CI para projetos Java e Python automaticamente
- Implante uma API do Amazon API Gateway em um site interno usando endpoints privados e um Application Load Balancer
- Implantar e depure clusters do Amazon EKS
- Implemente e gerencie AWS Control Tower controles usando AWS CDK e CloudFormation
- Implemente e gerencie AWS Control Tower controles usando o Terraform
- Implante canários CloudWatch Synthetics usando o Terraform
- Implemente um sistema de arquivos Lustre para processamento de dados de alto desempenho usando o Terraform e o DRA
- Implemente um caso de uso do RAG AWS usando o Terraform e o Amazon Bedrock
- Implante recursos em uma AWS Wavelength zona usando o Terraform
- Implante instâncias de cluster de failover do SQL Server na Amazon EC2 e na Amazon FSx usando o Terraform
- Implemente as automações de segurança para a AWS WAF solução usando o Terraform
- Detecte instâncias de banco de dados Amazon RDS e Aurora que têm certificados CA expirados
- Documente seu projeto de landing zone na AWS
- Certifique-se de que um perfil do IAM esteja associado a uma EC2 instância
- Exporte relatórios do AWS Backup de toda a organização no AWS Organizations como um arquivo CSV
- Gere recomendações personalizadas e reclassificadas usando o Amazon Personalize
- Identifique e alerte quando os recursos do Amazon Data Firehose não estiverem criptografados com uma chave AWS KMS

- Implemente o Account Factory for Terraform (AFT) usando um pipeline de bootstrap
- Implemente o controle de versão de API baseado em caminhos usando domínios personalizados no Amazon API Gateway
- Instale o agente SSM nos nós de trabalho do Amazon EKS usando o Kubernetes DaemonSet
- Instale o agente SSM e o CloudWatch agente nos nós de trabalho do Amazon EKS usando preBootstrapCommands
- Integre o VMware vRealize Network Insight com a VMware nuvem na AWS
- Gerencie conjuntos de AWS IAM Identity Center permissões como código usando AWS CodePipeline
- Gerencie produtos do AWS Service Catalog em várias contas e regiões da AWS
- Gerencie aplicativos de contêineres on-premises configurando o Amazon ECS Anywhere com o AWS CDK
- Gerencie AWS Organizations políticas como código usando o AWS CodePipeline Amazon Bedrock
- Migre registros de DNS em massa para uma zona hospedada privada do Amazon Route 53
- Migre o Oracle E-Business Suite para o Amazon RDS Custom
- Migre o Oracle PeopleSoft para o Amazon RDS Custom
- Migre sistemas RHEL BYOL para instâncias com licença incluída da AWS usando o AWS MGN
- Migre o VMware SDDC para a VMware nuvem na AWS usando o HCX VMware
- Configure um espaço de dados mínimo viável para compartilhar dados entre organizações
- Monitore ElastiCache clusters da Amazon para criptografia em repouso
- Monitore a atividade do aplicativo usando o CloudWatch Logs Insights
- Monitore ElastiCache clusters para grupos de segurança
- Monitore clusters do SAP RHEL Pacemaker usando os serviços da AWS
- Otimize implantações sem servidor de várias contas usando os fluxos de trabalho e Actions AWS CDK GitHub
- Acesse de forma privada um endpoint central de serviços da AWS a partir de vários VPCs
- Provisione AWS Service Catalog produtos com base em AWS CloudFormation modelos usando GitHub Ações
- Provisione funções do IAM com privilégios mínimos implantando uma solução de máquina de venda automática de funções
- Remova EC2 as entradas Contas da AWS da Amazon em frente AWS Managed Microsoft AD usando a AWS Lambda automação

- Remova EC2 as entradas da Amazon na mesma forma Conta da AWSAWS Managed Microsoft AD usando a AWS Lambda automação
- Alternar as credenciais do banco de dados sem reiniciar os contêineres
- Enviar uma notificação quando um usuário do IAM for criado
- Envie registros do VMware Cloud on AWS para o Splunk usando o VMware Aria Operations for Logs
- Configure um roteador celular sem servidor para uma arquitetura baseada em células
- Configure um pipeline de CI/CD para cargas de trabalho híbridas no Amazon ECS Anywhere usando o AWS CDK e GitLab
- Configure uma infraestrutura de desktop virtual com escalabilidade automática usando o NICE EnginFrame e o NICE DCV Session Manager
- Configure uma arquitetura de HA/DR para o Oracle E-Business Suite no Amazon RDS Custom com um banco de dados ativo em espera
- Configure a resolução de DNS para redes híbridas em um ambiente com várias contas AWS
- Configure a infraestrutura Multi-AZ para um SQL Server Always On FCI usando a Amazon FSx
- Configure a funcionalidade Oracle UTL_FILE no Aurora compatível com PostgreSQL
- Simplifique a autenticação de aplicativos com TLS mútuo no Amazon ECS usando o Application Load Balancer
- Simplificar o gerenciamento de certificados privados usando a CA privada da AWS e o AWS RAM
- Simplifique os fluxos de trabalho de aprendizado de máquina, do desenvolvimento local aos experimentos escaláveis, usando SageMaker IA e Hydra
- Marque anexo do gateway de trânsito automaticamente usando o AWS Organizations
- Funções de transição para um PeopleSoft aplicativo Oracle no Amazon RDS Custom for Oracle
- Use o Amazon Q Developer como assistente de codificação para aumentar sua produtividade

Aplicativos para web e dispositivos móveis

Tópicos

- Autentique os usuários existentes do aplicativo React usando o Amazon Cognito e a interface do usuário do AWS Amplify
- Implemente continuamente um aplicativo web moderno do AWS Amplify a partir de um repositório da AWS CodeCommit
- Crie um aplicativo React usando o AWS Amplify e adicione autenticação com o Amazon Cognito
- Crie um portal para microfrontends usando Angular e AWS Amplify Module Federation
- Implante um aplicativo de página única baseado em React no Amazon S3 e CloudFront
- Implante uma API do Amazon API Gateway em um site interno usando endpoints privados e um Application Load Balancer
- Incorpore um QuickSight painel da Amazon em um aplicativo Angular local
- Explore o desenvolvimento completo de aplicativos web nativos de nuvem com o Green Boost
- Execute testes unitários para um aplicativo Node.js GitHub usando a AWS CodeBuild
- Estruture um projeto Python em arquitetura hexagonal usando o AWS Lambda
- Mais padrões

Autentique os usuários existentes do aplicativo React usando o Amazon Cognito e a interface do usuário do AWS Amplify

Criado por Daniel Kozhemyako (AWS)

Resumo

Esse padrão mostra como adicionar recursos de autenticação a um aplicativo React de front-end existente usando uma biblioteca de AWS Amplify interface de usuário e um grupo de usuários do Amazon Cognito.

O padrão usa o Amazon Cognito para fornecer autenticação, autorização e gerenciamento de usuários para o aplicativo. Ele também usa um componente do Amplify UI, uma biblioteca de código aberto que estende os recursos do desenvolvimento da interface do AWS Amplify usuário (UI). O componente Authenticator UI gerencia as sessões de login e executa o fluxo de trabalho conectado à nuvem que autentica os usuários por meio do Amazon Cognito.

Depois de implementar esse padrão, os usuários podem entrar usando qualquer uma das seguintes credenciais:

- Nome de usuário e senha
- Provedores de identidades sociais, como o Apple, Facebook, o Google e o Amazon
- Provedores de identidade corporativa compatíveis com SAML 2.0 ou OpenID Connect (OIDC)

> **Note**
>
> Para criar um componente de UI de autenticação personalizado, você pode executar o componente Authenticator UI no modo headless.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um aplicativo web React 18.2.0 ou posterior
- Node.js e npm 6.14.4 ou posterior, instalados

Limitações

- Esse padrão se aplica somente aos aplicativos web React.
- Esse padrão usa um componente Amplify UI pré-construído. A solução não abrange as etapas necessárias para implementar um componente de UI personalizado.

Versões do produto

- Amplify UI 6.1.3 ou posterior (Gen 1)
- Amplify 6.0.16 ou posterior (Gen 1)

Arquitetura

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura que usa o Amazon Cognito para autenticar usuários para um aplicativo web React.

Ferramentas

Serviços da AWS

- O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para suas aplicações Web e móveis.

Outras ferramentas

- O Amplify UI é uma biblioteca de interface de usuário de código aberto que fornece componentes personalizáveis que você pode conectar à nuvem.
- O Node.js é um ambiente de tempo de JavaScript execução orientado a eventos projetado para criar aplicativos de rede escaláveis.
- O npm é um registro de software executado em um ambiente Node.js e usado para compartilhar ou emprestar pacotes e gerenciar a implantação de pacotes privados.

Práticas recomendadas

Se você estiver criando um novo aplicativo, recomendamos que você use o Amplify Gen 2.

Épicos

Criar um grupo de usuários do Amazon Cognito

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de usuários.	Criar um grupo de usuários do Amazon Cognito. Configure as opções de login e os requisitos de segurança do grupo de usuários de acordo com seu caso de uso.	Desenvolvedor de aplicativos
Adicionar um cliente de aplicativo.	Configure um cliente do aplicativo do grupo de usuários. Esse cliente é necessário para que seu aplicativo interaja com o grupo de usuários do Amazon Cognito.	Desenvolvedor de aplicativos

Integre seu grupo de usuários do Amazon Cognito com o componente Authenticator UI

Tarefa	Descrição	Habilidades necessárias
Instale as dependências.	Para instalar os pacotes `aws-amplify` e `@aws-amplify/ui-react`, execute o seguinte comando no diretório raiz do seu aplicativo: `npm i @aws-amplify/ui-react aws-amplify`	Desenvolvedor de aplicativos
Configure o grupo de usuários.	Com base no exemplo a seguir, crie um `aws-exports.js` arquivo e salve na	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	`src` pasta. O arquivo deve incluir as seguintes informaçõ es:
	• Região da AWS em que seu grupo de usuários do Amazon Cognito está
	• ID do grupo de usuários do Amazon Cognito
	• ID do cliente do aplicativo
	`// replace the user pool region, id, and app client id details`
	`const awsmobile = { "aws_project_region": "put_your_region_here", "aws_cognito_region": "put_your_region_here", "aws_user_pools_id": "put_your_user_pool_id_here", "aws_user_pools_web_client_id": "put_your_user_pool_app_id_here" }`
	`export default awsmobile;`	

Tarefa	Descrição	Habilidades necessárias

Importe e configure o serviço Amplify.	1. No arquivo de ponto de entrada do aplicativo (por exemplo,`App.js`), importe e carregue o `aws-exports.js` arquivo inserindo as seguintes linhas de código:
	`import { Amplify } from 'aws-amplify';`
	`import awsExports from './aws-exports';`
	2. Com base no exemplo a seguir, configure o cliente Amplify usando o `aws-exports.js` arquivo:
	`// Configure Amplify in index file or root file`
	`Amplify.configure({ ...awsExports });`
	Para obter mais informações, consulte Configurar categorias do Amplify na documentação do Amplify.
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Adicione o componente Authenticator UI.	Para exibir o componente `Authenticator UI`, adicione as seguintes linhas de código ao arquivo do ponto de entrada do aplicativo (`App.js`):
	`import { Authenticator } from '@aws-amplify/ui-react';`
	`import '@aws-amplify/ui-react/styles.css';`
	Note
	O trecho de código de exemplo importa o componente `Authenticator UI` e o arquivo styles.css do Amplify UI, que é necessário ao usar os temas pré-criados do componente.
	O componente de `Authenticator` interface do usuário fornece dois valores de retorno:
	• Detalhes do usuário
	• Uma função que pode ser invocada para desconectar o usuário
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Veja o componente do exemplo a seguir: `function App() { return ( <Authenticator> {({ signOut, user }) => ( <div> <p>Welcome {user.username}</p> <button onClick={signOut}>Sign out</button> </div> )} </Authenticator> ); }` **Note** Para obter um exemplo de `App.js` arquivo, consulte a seção Informações adicionais desse padrão.	

Tarefa	Descrição	Habilidades necessárias

(Opcional) Recupere as informações da sessão.	Depois que um usuário é autenticado, você pode recuperar dados do cliente Amplify sobre sua sessão. Por exemplo, você pode recuperar o token web JSON (JWT) da sessão de um usuário para autenticar as solicitações da sessão em uma API de backend.
	
	Veja o exemplo a seguir de um cabeçalho de solicitação que inclui um JWT:
	
	`import { fetchAuthSession } from 'aws-amplify/auth';`
	`(await fetchAuthSession()).tokens?.idToken?.toString();`
		Desenvolvedor de aplicativos

Solução de problemas

Problema	Solução
Novos usuários não podem se cadastrar no aplicativo.	Da seguinte forma, certifique-se de que seu grupo de usuários do Amazon Cognito esteja configurado para permitir que os usuários se inscrevam para fazer parte do grupo de usuários: • Faça login no e AWS Management Console, em seguida, abra o console do Amazon Cognito.

Problema	Solução
	• No painel de navegação à esquerda, escolha grupo de usuários. • Escolha seu grupo de usuários na lista. • Em General Settings (Configurações gerais), escolha Políticas. • Escolha Permitir que os próprios usuários se cadastrem.
O componente Auth parou de funcionar após a atualização da v5 para a v6.	A `Auth` categoria mudou para uma abordagem funcional e nomeou parâmetros no Amplify v6. Agora você deve importar o funcional APIs diretamente do `aws-amplify/auth` caminho. Para obter mais informações, consulte Migrar da v5 para a v6 na documenta ção do Amplify.

Recursos relacionados

- Introdução ao Amazon Cognito (site)AWS
- Crie um novo aplicativo React (documentação do React)
- O que é o Amazon Cognito? (Documentação do Amazon Cognito)
- Biblioteca do Amplify UI (documentação do Amplify)

Mais informações

O `App.js` arquivo deve conter o seguinte código:

```
import './App.css';
import { Amplify } from 'aws-amplify';
import awsExports from './aws-exports';
import { fetchAuthSession } from 'aws-amplify/auth';
import { Authenticator } from '@aws-amplify/ui-react';
import '@aws-amplify/ui-react/styles.css';
Amplify.configure({ ...awsExports });
let token = (await fetchAuthSession()).tokens?.idToken?.toString();
```

```
function App() {
  return (
      <Authenticator>
        {({ signOut, user }) => (
            <div>
              <p>Welcome {user.username}</p>
                <p>Your token is: {token}</p>
              <button onClick={signOut}>Sign out</button>
            </div>
        )}
      </Authenticator>
  );
}

export default App;
```

Implemente continuamente um aplicativo web moderno do AWS Amplify a partir de um repositório da AWS CodeCommit

Criado por Deekshitulu Pentakota (AWS) e Sai Katakam (AWS)

Resumo

Aviso: CodeCommit A AWS não está mais disponível para novos clientes. Os clientes atuais da AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais.

Os aplicativos web modernos são construídos como aplicativos de página única (SPAs) que empacotam todos os componentes do aplicativo em arquivos estáticos. Ao usar o AWS Amplify Hosting, você pode criar um pipeline de integração contínua e implantação contínua (CI/CD) que cria, implanta e hospeda um aplicativo web moderno que é gerenciado em um repositório baseado em Git. Quando você conecta o Amplify Hosting ao repositório de código, cada confirmação inicia um único fluxo de trabalho para implantar o frontend e o backend do aplicativo. O benefício dessa abordagem é que o aplicativo web é atualizado somente depois que a implantação tenha sido concluída com êxito, o que evita inconsistências entre o frontend e o backend.

Nesse padrão, você usa um CodeCommit repositório da AWS para gerenciar seu aplicativo web moderno. O exemplo de aplicativo web nessas instruções usa a estrutura React SPA. No entanto, o Amplify Hosting oferece suporte a muitas outras estruturas de SPA, como Angular, Vue, Next.js, e também oferece suporte a geradores de site único, como Gatsby, Hugo e Jekyll.

Esse padrão é destinado aos builders AWS que têm experiência com os seguintes serviços e conceitos:

- AWS CodeCommit
- AWS Amplify Hosting
- React
- JavaScript
- Node.js
- npm
- Git

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões para criar recursos no Amplify e. CodeCommit Para obter mais informações, consulte Identity and Access Management for Amplify e Identity and Access Management for AWS. CodeCommit
- AWS Command Line Interface (AWS CLI), instalada e configurada.
- Um Editor de texto ou Editor de código.
- CodeCommit, configurado para usuários HTTPS usando credenciais do Git.
- Um perfil de serviço do IAM para o Amplify.
- npm e Node.js, instalados (documentação do npm).

Limitações

- Esse padrão não discute o desenvolvimento e a integração de um backend para o aplicativo Amplify, como uma API, autenticação ou banco de dados. Para obter mais informações sobre backends, consulte Criar um backend na documentação do Amplify.

Versões do produto

- AWS CLI versão 2.0
- Node.js versão 16.x ou superior

Arquitetura

Pilha de tecnologias de destino

- CodeCommitRepositório AWS contendo um React SPA
- AWS Amplify Hosting

Arquitetura de destino

Ferramentas

Serviços da AWS

- O AWS Amplify Hosting fornece um fluxo de trabalho baseado em git para hospedar aplicativos web de pilha completa com tecnologia sem servidor com implantação contínua.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

Outras ferramentas

- O Node.js é um ambiente de tempo de JavaScript execução orientado a eventos projetado para criar aplicativos de rede escaláveis.
- O npm é um registro de software executado em um ambiente Node.js e usado para compartilhar ou emprestar pacotes e gerenciar a implantação de pacotes privados.

Épicos

Crie um CodeCommit repositório

Tarefa	Descrição	Habilidades necessárias
Criar um repositório.	Para obter instruções, consulte Criar um CodeCommit repositório da AWS na CodeCommit documentação.	AWS DevOps
Clonar o repositório.	Para obter instruções, consulte Conectar-se ao CodeCommit repositório clonando o repositório na documentação. CodeCommit Caso seja solicitado, forneça suas credenciais do Git.	Desenvolvedor de aplicativos

Criar um aplicativo React

Tarefa	Descrição	Habilidades necessárias

Criar um novo aplicativo React.	1. Insira comando a seguir para navegar para o repositório clonado. `<repo name>`Substitua pelo nome do seu CodeCommit repositório.
	`$ cd <repo name>`
	2. Insira comando a seguir para criar um novo aplicativo React no repositório clonado.
	`$ npx create-react-app .`
	3. Codifique o aplicativo e insira o comando a seguir para iniciá-lo.
	`$ npm start`
	Para obter mais informações sobre a criação de um aplicativo React personalizado, consulte as instruções Criar um aplicativo React na documentação Criar aplicativo React. Você também pode implantar um aplicativo React de amostra em sua conta do Amplify seguindo as instruçõe
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	s em Implantar um frontend na documentação do Amplify.	

Criar uma ramificação e enviar o código.	1. Digite o comando a seguir para criar uma nova ramificação localmente, onde <branch> é o nome que você deseja atribuir à nova ramificação.
	`$ git checkout -b <branch>`
	2. Digite o comando a seguir para enviar a ramificação para o CodeCommit repositório, onde <branch> está o nome que você atribuiu na etapa anterior. Para obter mais informações, consulte Trabalhar com confirmações.
	`$ git push --set-upstream origin <branch>`
		Desenvolvedor de aplicativos

Implantar o aplicativo no AWS Amplify Hosting

Tarefa	Descrição	Habilidades necessárias
Conectar o Amplify ao repositório.	Para obter instruções, consulte Conectar um repositório na documentação do Amplify Hosting.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Selecione AWS CodeCommit e o repositório e a filial que você criou anteriormente.	

Definir as configurações de criação do frontend.	Para obter instruções, consulte Confirmar as configurações de criação para o frontend na documentação do Amplify Hosting. Aceite os padrões ou insira o seguinte.
	`Build settings:`
	`version: 0.1`
	`frontend:`
	`  phases:`
	`  preBuild:`
	`  commands:`
	`  - npm ci`
	`  build:`
	`  commands:`
	`  - npm run build`
	`  artifacts:`
	`  baseDirectory:`
	`build`
	`  files:`
	`  - '**/*'`
	`  cache:`
	`  paths:`
	`  - node_modules/`
	`**/*`
		Desenvolvedor de aplicativos

Analisar e implantar.	Para obter instruções, consulte Salvar e implantar na documentação do Amplify Hosting. Espere até que o processo de implantação seja concluído.	Desenvolvedor de aplicativos

Validar a implantação contínua

Tarefa	Descrição	Habilidades necessárias
Verificar a implantação inicial.	Quando o processo de implantação estiver concluído , em Domínio, escolha o link. Verifique se o aplicativ o está operando conforme o esperado.	Desenvolvedor de aplicativos
Enviar as alterações para o repositório de código.	Edite o código na sua estação de trabalho local e envie as alterações para o CodeCommi t repositório. O Amplify Hosting detecta a alteração no repositório e inicia automatic amente o processo de criação e implantação. Confirmar se as atualizações do aplicativo estão visíveis no domínio.	Desenvolvedor de aplicativos

Recursos relacionados

CodeCommit Documentação da AWS

- Configuração para a AWS CodeCommit
  - Configuração para usuários de HTTPS usando credenciais do Git
  - Etapas de configuração para conexões HTTPS com CodeCommit repositórios da AWS em Linux, macOS ou Unix com o auxiliar de credenciais da AWS CLI
- Comece a usar a AWS CodeCommit

Documentação do AWS Amplify Hosting

- Conceitos básicos do código existente
- Configurar domínios personalizados

Atributos do React

- Criar um site do aplicativo React
- Criar a documentação do aplicativo React
- Criar repositório do React App () GitHub

Crie um aplicativo React usando o AWS Amplify e adicione autenticação com o Amazon Cognito

Criado por Rishi Singla (AWS)

Resumo

Esse padrão demonstra como usar o AWS Amplify para criar um aplicativo baseado em React e como adicionar autenticação ao frontend usando o Amazon Cognito. AWS Amplify consiste em um conjunto de ferramentas (estrutura de código aberto, ambiente de desenvolvimento visual, console) e serviços (aplicação Web e hospedagem de site estático) para acelerar o desenvolvimento de aplicativos móveis e web na AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Node.js e npm instalados em sua máquina

Versões do produto

- Node.js versão 10.x ou superior (para verificar sua versão, execute `node -v` em uma janela de terminal)
- npm versão 6.x ou superior (para verificar sua versão, execute `npm -v` em uma janela de terminal)

Arquitetura

Pilha de tecnologias de destino

- AWS Amplify
- Amazon Cognito

Ferramentas

- Command Line Interface (CLI) do Amplify
- Amplify Libraries (bibliotecas cliente de código aberto)

- Amplify Studio (interface visual)

Épicos

Instale a CLI do AWS Amplify

Tarefa	Descrição	Habilidades necessárias

Instale a CLI do Amplify.	A CLI do Amplify é uma cadeia de ferramentas unificada para criar serviços de nuvem AWS para seu aplicativo React. Para instalar a CLI do Amplify, execute:
	`npm install -g @aws-amplify/cli`
	O npm notificará você se uma nova versão principal estiver disponível. Se sim, use o comando a seguir para atualizar sua versão do npm:
	`npm install -g npm@9.8.0`
	onde 9.8.0 se refere à versão que você deseja instalar.
		Desenvolvedor de aplicativos

Crie um aplicativo React

Tarefa	Descrição	Habilidades necessárias
Crie um aplicativo React.	Para criar um novo aplicativo React, use o comando:	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	`npx create-react-app amplify-react-application`
	
	onde `ampify-react-application` é o nome do aplicativo.
	
	Quando o aplicativo for criado com êxito, você verá a mensagem:
	
	`Success! Created amplify-react-application`
	
	Um diretório com várias subpastas será criado para o aplicativo React.	

Inicie o aplicativo na sua máquina local.	Vá para o diretório `amplify-react-application` que foi criado na etapa anterior e execute o comando: `amplify-react-application% npm start` Isso inicia o aplicativo React na sua máquina local.	Desenvolvedor de aplicativos

Configurar a CLI do Amplify

Tarefa	Descrição	Habilidades necessárias
Configure o Amplify para se conectar à sua conta da AWS.	Configure o Amplify executando o comando: `amplify-react-application % amplify configure` A CLI do Amplify solicita que você siga estas etapas para configurar o acesso à sua conta da AWS: 1. Faça login em sua conta de administrador da AWS. 2. Especifique a região da AWS que deseja usar. 3. Crie um usuário do AWS Identity and Access Management (IAM) com acesso programático e anexe a política de permissões `AdministratorAccess-Amplify` ao usuário. 4. Crie e copie o ID de chave de acesso e a chave de acesso secreta. 5. Insira esses detalhes no terminal. 6. Crie um nome de perfil ou use o perfil padrão.	AWS geral, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Warning Esse cenário exige que os usuários do IAM tenham acesso programát ico e credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissõe s necessárias para realizar a tarefa e que você os remova quando não forem mais necessários. As chaves de acesso podem ser atualizad as, se necessári o. Para obter mais informações, consulte Atualização de chaves de acesso no Guia de usuário do IAM. Essas etapas aparecem no terminal da seguinte forma.	

Tarefa	Descrição	Habilidades necessárias
	Follow these steps to set up access to your AWS account: Sign in to your AWS administrator account: https://console.aws.amazon.com/ Press Enter to continue Specify the AWS Region ? region: us-east-1 Follow the instructions at https://docs.amplify.aws/cli/start/install/#configure-the-amplify-cli to complete the user creation in the AWS console https://console.aws.amazon.com/iamv2/home#/users/create Press Enter to continue Enter the access key of the newly created user: ? accessKeyId: ******************** ? secretAccessKey: ********** This would update/create the AWS Profile in your local machine ? Profile Name: new Successfully set up the new user. Para obter mais informações sobre essas etapas, consulte	

Tarefa	Descrição	Habilidades necessárias
	a documentação no Amplify Dev Center.	

Inicialize o Amplify

Tarefa	Descrição	Habilidades necessárias

Inicialize o Amplify.	1. Para inicializar o Amplify no novo diretório, execute:
	`amplify init`
	O Amplify solicita o nome do projeto e os parâmetros de configuração
	2. Especifique todos os parâmetros e pressione Y para inicializar o projeto com a configuração especificada.
	`Project information`
	`| Name: amplifyre`
	`actproject`
	`| Environment: dev`
	`| Default editor:`
	`Visual Studio Code`
	`| App type: javascrip`
	`t`
	`| Javascript`
	`framework: react`
		Desenvolvedor de aplicativos, AWS geral

Tarefa	Descrição	Habilidades necessárias

	<pre>| Source Directory
	Path: src
	
	| Distribution
	Directory Path: build
	
	| Build Command: npm
	run-script build
	
	| Start Command: npm
	run-script start</pre>
	3. Selecione o perfil que você criou na etapa anterior. Os recursos serão implantados no `dev` ambiente do projeto Amplify que você criou.
	4. Para confirmar que os recursos foram criados, você pode abrir o console do AWS Amplify e visualizar o CloudFormation modelo da AWS que foi usado para criar os recursos e os detalhes.
	<pre>Deploying root stack
	amplifyreactproject
	[==========
	==========
	----] 2/4
	amplify-amplif
	yreactproject-d…
	AWS::CloudFormatio
	n::Stack
	CREATE_IN_PROGRESS</pre>	

Tarefa	Descrição	Habilidades necessárias

	`UnauthRole AWS::IAM::Role CREATE_COMPLETE`
	
	`DeploymentBucket AWS::S3::Bucket CREATE_IN_PROGRESS`
	
	`AuthRole AWS::IAM::Role CREATE_COMPLETE`	

Adicione autenticação ao frontend

Tarefa	Descrição	Habilidades necessárias
Adição de autenticação.	Você pode usar o comando `amplify add <category>` para adicionar atributos como um login de usuário ou uma API de backend. Nesta etapa, você usará o comando para adicionar autenticação. O Amplify fornece um serviço de autenticação de backend com o Amazon Cognito, bibliotecas de frontend e um componente de interface de usuário do Autenticador drop-in. Os atributos incluem inscrição do usuário, login do	Desenvolvedor de aplicativos, AWS geral

Tarefa	Descrição	Habilidades necessárias

	usuário, autenticação multifator, saída do usuário e login sem senha. Você também pode autenticar usuários por meio da integração com provedores de identidade federados, como Amazon, Google e Facebook. A categoria de autenticação do Amplify se integra perfeitamente a outras categorias do Amplify, como API, análise e armazenamento, para que você possa definir regras de autorização para usuários autenticados e não autenticados.
	
	1. Para configurar a autenticação para seu aplicativo React, execute o comando:
	
	`amplify-react-application1 % amplify add auth`
	
	Isso exibe as informações e os prompts a seguir. Você pode escolher a configuração apropriada de acordo com seus requisitos comerciais e de segurança.
	
	`Using service: Cognito, provided by: awscloudformation`	

Tarefa	Descrição	Habilidades necessárias
	``` The current configured provider is Amazon Cognito. Do you want to use the default authentication and security configuration? (Use arrow keys) # Default configuration Default configuration with Social Provider (Federation) Manual configuration I want to learn more. ```	
	2. Para um exemplo simples, escolha a configuração padrão e, em seguida, selecione o mecanismo de login para usuários (nesse caso, e-mail): ``` How do you want users to be able to sign in? Username # Email Phone Number Email or Phone Number ```	

Tarefa	Descrição	Habilidades necessárias

	<pre> I want to learn more.</pre> 3. Ignore as configurações avançadas para concluir a adição de recursos de autenticação: <pre>Do you want to configure advanced settings? (Use arrow keys)
	# No, I am done.
	
	  Yes, I want to make some additional changes.</pre> 4. Compile seus recursos de backend locais e provision e-os na nuvem: <pre>amplify-react-application1 % amplify push</pre> Esse comando faz as alterações apropriadas nos grupos de usuários do Congito em sua conta. 5. Pressione Y para configurar o `auth` recurso usando CloudFormation. Isso configura os seguintes recursos:	

Tarefa	Descrição	Habilidades necessárias

	`UserPool AWS::Cognito::UserPool CREATE_COMPLETE`
	`UserPoolClientWeb AWS::Cognito::UserPoolClient CREATE_COMPLETE`
	
	`UserPoolClientWeb AWS::Cognito::UserPoolClient CREATE_COMPLETE`
	
	`UserPoolClientRole AWS::IAM::Role CREATE_COMPLETE`
	
	`UserPoolClientLambda AWS::Lambda::Function CREATE_COMPLETE`
	`UserPoolClientLambdaPolicy AWS::IAM::Policy CREATE_COMPLETE`
	
	`UserPoolClientLogPolicy AWS::IAM::Policy CREATE_IN_PROGRESS`
	
	Você também pode usar o console do AWS Cognito para visualizar esses	

Tarefa	Descrição	Habilidades necessárias
	recursos (procure grupos de usuários e banco de identidades do Cognito). Esta etapa atualiza o arquivo `aws-exports.js` na pasta `src` do seu aplicativo React com as configurações do grupo de usuários e do banco de identidades do Cognito.	

Alterar o arquivo App.js

Tarefa	Descrição	Habilidades necessárias
Alterar o arquivo App.js.	Na pasta `src`, abra e revise o arquivo `App.js`. O arquivo modificado deve ficar assim: `{  App.Js File after modifications: import React from 'react'; import logo from './logo.svg'; import './App.css'; import { Amplify } from 'aws-amplify'; import { withAuthenticator, Button, Heading } from '@aws-amplify/ui-react'; import awsconfig from './aws-exports'; Amplify.configure(awsconfig);`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`function App({ signOut }) { return ( <div> <h1>Thankyou for doing verification</h1> <h2>My Content</h2> <button onClick={signOut}>Sign out</button> </div> ); } export default withAuthenticator(App);`	
Importe pacotes React.	O arquivo `App.js` importa dois pacotes React. Instale esses pacotes usando o seguinte comando: `amplify-react-application1 % npm install --save aws-amplify @aws-amplify/ui-react`	Desenvolvedor de aplicativos

Inicie o aplicativo React e verifique a autenticação

Tarefa	Descrição	Habilidades necessárias
Inicie o aplicativo.	Inicie o aplicativo na sua máquina local:	Desenvolvedor de aplicativos, AWS geral

Tarefa	Descrição	Habilidades necessárias
	`amplify-react-appl ication1 % npm start`	
Verifique a autenticação.	Verifique se o aplicativ o solicita parâmetros de autenticação. (Em nosso exemplo, configuramos o e-mail como método de login.) A interface de usuário do frontend deve solicitar suas credenciais de login e fornecer a opção de criar uma conta. Você também pode configura r o processo de criação do Amplify para adicionar o backend como parte de um fluxo de trabalho de implantaç ão contínua. No entanto, esse padrão não cobre essa opção.	Desenvolvedor de aplicativos, AWS geral

Recursos relacionados

- Conceitos básicos (documentação do npm)
- Crie uma conta autônoma da AWS (documentação do AWS Account Management)
- Documentação do AWS Amplify
- Documentação do Amazon Cognito

Crie um portal para microfrontends usando Angular e AWS Amplify Module Federation

Criado por Milena Godau (AWS) e Pedro Garcia (AWS)

Resumo

Uma arquitetura de microfront-end permite que várias equipes trabalhem em diferentes partes de um aplicativo de front-end de forma independente. Cada equipe pode desenvolver, criar e implantar um fragmento do front-end sem interferir em outras partes do aplicativo. Do ponto de vista do usuário final, parece ser um aplicativo único e coeso. No entanto, eles estão interagindo com vários aplicativos independentes publicados por equipes diferentes.

Este documento descreve como criar uma arquitetura de micro-frontend usando AWS Amplifya estrutura de front-end Angular e a Federação de Módulos. Nesse padrão, os microfrontends são combinados no lado do cliente por um aplicativo shell (ou pai). O aplicativo shell atua como um contêiner que recupera, exibe e integra os microfront-ends. O aplicativo shell manipula o roteamento global, que carrega diferentes microfront-ends. O plug-in @angular -architects/module-federation integra a Federação de Módulos com o Angular. Você implanta o aplicativo shell e os microfrontends usando o. AWS Amplify Os usuários finais acessam o aplicativo por meio de um portal baseado na web.

O portal está dividido verticalmente. Isso significa que os microfront-ends são visualizações inteiras ou grupos de visualizações, em vez de partes da mesma visualização. Portanto, o aplicativo shell carrega apenas um micro-frontend por vez.

Os microfront-ends são implementados como módulos remotos. O aplicativo shell carrega lentamente esses módulos remotos, o que adia a inicialização do microfrontend até que seja necessária. Essa abordagem otimiza o desempenho do aplicativo carregando somente os módulos necessários. Isso reduz o tempo de carregamento inicial e melhora a experiência geral do usuário. Além disso, você compartilha dependências comuns entre os módulos por meio do arquivo de configuração do webpack (webpack.config.js). Essa prática promove a reutilização de código, reduz a duplicação e simplifica o processo de agrupamento.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS

- Node.js e npm, instalados
- Amplify CLI, instalado
- CLI angular, instalada
- Permissões de uso AWS Amplify
- Familiaridade com o Angular

Versões do produto

- Angular CLI versão 13.1.2 ou posterior
- @angular -architects/module-federation versão 14.0.1 ou posterior
- webpack versão 5.4.0 ou posterior
- AWS Amplify Geração 1

Limitações

Uma arquitetura de microfrontend é uma abordagem poderosa para criar aplicativos web escaláveis e resilientes. No entanto, é fundamental entender os seguintes desafios em potencial antes de adotar essa abordagem:

- Integração — Um dos principais desafios é o aumento potencial da complexidade em comparação com front-ends monolíticos. Orquestrar vários microfront-ends, lidar com a comunicação entre eles e gerenciar dependências compartilhadas pode ser mais complexo. Além disso, pode haver uma sobrecarga de desempenho associada à comunicação entre os microfront-ends. Essa comunicação pode aumentar a latência e reduzir o desempenho. Isso precisa ser resolvido por meio de mecanismos eficientes de mensagens e estratégias de compartilhamento de dados.
- Duplicação de código — Como cada microfrontend é desenvolvido de forma independente, existe o risco de duplicar o código para funcionalidades comuns ou bibliotecas compartilhadas. Isso pode aumentar o tamanho geral do aplicativo e introduzir desafios de manutenção.
- Coordenação e gerenciamento — Coordenar os processos de desenvolvimento e implantação em vários microfront-ends pode ser um desafio. Garantir o controle de versão consistente, o gerenciamento de dependências e a manutenção da compatibilidade entre os componentes se torna mais importante em uma arquitetura distribuída. Estabelecer uma governança clara, diretrizes e pipelines automatizados de teste e implantação é essencial para uma colaboração e entrega perfeitas.

- Teste — Testar arquiteturas de microfront-end pode ser mais complexo do que testar front-ends monolíticos. Isso requer esforço adicional e estratégias de teste especializadas para realizar testes e end-to-end testes de integração entre componentes e validar experiências de usuário consistentes em vários microfront-ends.

Antes de se comprometer com a abordagem de microfrontend, recomendamos que você analise Entendendo e implementando microfrontends em. AWS

Arquitetura

Em uma arquitetura de microfrontend, cada equipe desenvolve e implanta recursos de forma independente. A imagem a seguir mostra como várias DevOps equipes trabalham juntas. A equipe do portal desenvolve o aplicativo shell. O aplicativo shell atua como um contêiner. Ele recupera, exibe e integra os aplicativos de microfront-end publicados por outras equipes. DevOps Você usa AWS Amplify para publicar o aplicativo shell e os aplicativos de microfrontend.

O diagrama da arquitetura mostra o seguinte fluxo de trabalho:

1. A equipe do portal desenvolve e mantém o aplicativo shell. O aplicativo shell orquestra a integração e a renderização dos microfront-ends para compor o portal geral.
2. As equipes A e B desenvolvem e mantêm um ou mais microfront-ends ou recursos integrados ao portal. Cada equipe pode trabalhar de forma independente em seus respectivos microfront-ends.
3. O usuário final se autentica usando o Amazon Cognito.
4. O usuário final acessa o portal e o aplicativo shell é carregado. Conforme o usuário navega, o aplicativo shell lida com o roteamento e recupera o micro-frontend solicitado, carregando seu pacote.

Ferramentas

Serviços da AWS

- AWS Amplifyé um conjunto de ferramentas e recursos específicos que ajudam desenvolvedores front-end da Web e de dispositivos móveis a criar rapidamente aplicativos completos em. AWS Nesse padrão, você usa a CLI do Amplify para implantar os aplicativos de microfront-end do Amplify.

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.

Outras ferramentas

- @angular -architects/module-federation é um plugin que integra o Angular com o Module Federation.
- O Angular é uma estrutura de aplicativos web de código aberto para criar aplicativos de página única modernos, escaláveis e testáveis. Ele segue uma arquitetura modular e baseada em componentes que promove a reutilização e a manutenção do código.
- O Node.js é um ambiente de JavaScript tempo de execução orientado a eventos projetado para criar aplicativos de rede escaláveis.
- O npm é um registro de software executado em um ambiente Node.js e usado para compartilhar ou emprestar pacotes e gerenciar a implantação de pacotes privados.
- O Webpack Module Federation ajuda você a carregar código compilado e implantado de forma independente, como microfront-ends ou plug-ins, em um aplicativo.

Repositório de código

O código desse padrão está disponível no portal Micro-frontend usando o repositório Angular e Module Federation GitHub . Esse repositório contém as duas pastas a seguir:

- `shell-app`contém o código para o aplicativo shell.
- `feature1-app`contém uma amostra de micro-frontend. O aplicativo shell busca esse micro-frontend e o exibe como uma página dentro do aplicativo do portal.

Práticas recomendadas

As arquiteturas de microfront-end oferecem inúmeras vantagens, mas também introduzem complexidade. A seguir estão algumas das melhores práticas para um desenvolvimento tranquilo, código de alta qualidade e uma ótima experiência do usuário:

- Planejamento e comunicação — Para agilizar a colaboração, invista em planejamento antecipado, design e canais de comunicação claros.

- Consistência do design — aplique um estilo visual consistente em microfront-ends usando sistemas de design, guias de estilo e bibliotecas de componentes. Isso proporciona uma experiência de usuário coesa e acelera o desenvolvimento.
- Gerenciamento de dependências — Como os microfrontends evoluem de forma independente, adote contratos padronizados e estratégias de controle de versão para gerenciar dependências de forma eficaz e evitar problemas de compatibilidade.
- Arquitetura de microfrontend — Para permitir o desenvolvimento e a implantação independentes, cada microfrontend deve ter uma responsabilidade clara e bem definida por uma funcionalidade encapsulada.
- Integração e comunicação — Para facilitar a integração e minimizar conflitos, defina contratos e protocolos de comunicação claros entre microfront-ends APIs, incluindo eventos e modelos de dados compartilhados.
- Teste e garantia de qualidade — Implemente pipelines de automação de testes e integração contínua para microfront-ends. Isso melhora a qualidade geral, reduz o esforço de teste manual e valida a funcionalidade entre as interações de microfront-end.
- Otimização de desempenho — monitore continuamente as métricas de desempenho e acompanhe as dependências entre microfront-ends. Isso ajuda você a identificar gargalos e manter o desempenho ideal do aplicativo. Use ferramentas de monitoramento de desempenho e análise de dependências para essa finalidade.
- Experiência do desenvolvedor — Concentre-se na experiência do desenvolvedor fornecendo documentação, ferramentas e exemplos claros. Isso ajuda você a otimizar o desenvolvimento e integrar novos membros da equipe.

Épicos

Crie o aplicativo shell

Tarefa	Descrição	Habilidades necessárias
Crie o aplicativo shell.	1. Na CLI Angular, digite o seguinte comando: `ng new shell --routing`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	2. Digite o comando a seguir para navegar até a pasta do projeto: `cd shell` **Note** A estrutura de pastas e projetos para os aplicativos de shell e micro-frontend pode ser totalmente independente. Eles podem ser tratados como aplicativos angulares independentes.	
Instale o plug-in .	Na CLI Angular, digite o seguinte comando para instalar o plug-in @angular - architects/module-federation: `ng add @angular-architects/module-federation --project shell --port 4200`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Adicione o URL do microfrontend como uma variável de ambiente.	1. Abra o arquivo environment.ts. 2. Adicione `mfe1URL: 'http://localhost:5000'` ao `environment` objeto: `export const environment = { production: false, mfe1URL: 'http://localhost:5000', };` 3. Salve e feche o arquivo environment.ts.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Defina o roteamento.	1. Abra o arquivo app-routing.module.ts.
	2. Na CLI Angular, insira o seguinte comando para importar o `loadRemoteModule` módulo do plug-in @angular -architects/module-federation:
	`import { loadRemoteModule } from '@angular-architects/module-federation';`
	3. Defina a rota padrão da seguinte forma:
	`{ path: '', pathMatch: 'full', redirectTo: 'mfe1' },`
	4. Defina a rota para o micro-frontend:
	`{ path: 'mfe1', loadChildren: () => loadRemoteModule({ type: 'module', remoteEntry: `${environment.mfe`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	1URL}/remoteEntry. js`, exposedMo dule: './Module' }) .then(m => m.Mfe1Module) }, 5. Salve e feche o arquivo app-routing.module.ts.	
Declare o `mfe1` módulo.	1. Na `src` pasta, crie um novo arquivo chamado decl.d.ts. 2. Abra o arquivo decl.d.ts. 3. Adicione o seguinte ao arquivo: `declare module 'mfe1/Module';` 4. Salve e feche o arquivo decl.d.ts.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Prepare o pré-carregamento para o micro-frontend.	O pré-carregamento do micro-frontend ajuda o webpack a negociar adequadamente as bibliotecas e pacotes compartilhados.
	1. Abra o arquivo main.ts.
	2. Substitua o conteúdo pelo seguinte:
	`import { loadRemoteEntry } from '@angular-architects/module-federation';`
	`Promise.all([ loadRemoteEntry(`${environment.mfe1URL}/remoteEntry.js`, 'mfe1'), ]) .catch(err => console.error('Error loading remote entries', err)) .then(() => import('./bootstrap')) .catch(err => console.error(err) );`
	3. Salve e feche o arquivo main.ts.
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Ajuste o conteúdo HTML.	1. Abra o arquivo app.component.html. 2. Substitua o conteúdo pelo seguinte: `<h1>Shell application is running!</h1> <router-outlet></router-outlet>` 3. Salve e feche o arquivo app.component.html.	Desenvolvedor de aplicativos

Crie o aplicativo de microfrontend

Tarefa	Descrição	Habilidades necessárias

Crie o microfrontend.	1. Na CLI Angular, digite o seguinte comando:
	`ng new mfe1 --routing`
	2. Digite o comando a seguir para navegar até a pasta do projeto:
	`cd mfe1`
		Desenvolvedor de aplicativos

Instale o plug-in .	Digite o comando a seguir para instalar o plug-in @angular -architects/module-federation: `ng add @angular-architects/module-`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`federation --project mfe1 --port 5000`	

Crie um módulo e um componente.	Insira os seguintes comandos para criar um módulo e um componente e exportá-los como módulo de entrada remota:
	`ng g module mfe1 --routing`
	`ng g c mfe1`
		Desenvolvedor de aplicativos

Defina o caminho de roteamento padrão.	1. Abra o arquivo mfe-routing.module.ts. 2. Defina a rota padrão da seguinte forma: `{ path: '', component: Mfe1Component },` 3. Salve e feche o arquivo mfe-routing.module.ts.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Adicione a `mfe1` rota.	1. Abra o arquivo app-routing.module.ts.
	2. Defina a rota padrão da seguinte forma:
	`{ path: '', pathMatch: 'full', redirectTo: 'mfe1' },`
	3. Adicione a seguinte `mfe1` rota:
	`{ path: 'mfe1', loadChildren: () => import('./mfe1/mfe1.module').then((m) => m.Mfe1Module), },`
	4. Salve e feche o arquivo app-routing.module.ts.
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Edite o arquivo webpack.config.js.	1. Abra o arquivo webpack.config.js.
	2. Edite a `For remotes` seção para que corresponda ao seguinte:
	`// For remotes (please adjust)`
	`name: "mfe1",`
	`filename: "remoteEntry.js",`
	`exposes: {`
	`'./Module': './src/app/mfe1/mfe1.module.ts',`
	`},`
	3. Na `shared` seção, adicione todas as dependências que o `mfe1` aplicativo compartilha com o aplicativo shell:
	`shared: share({`
	`"@angular/core": { singleton: true, strictVersion: true, requiredVersion: 'auto' },`
	`"@angular/common": { singleton: true, strictVersion: true, requiredVersion: 'auto' },`
	`"@angular/common/http": { singleton: true, strictVersion: true, requiredVersion: 'auto' },`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	"@angular/router": { singleton: true, strictVersion: true, requiredVersion: 'auto' }, ...sharedMappings.getDescriptors() })	
	4. Salve e feche o arquivo webpack.config.js.	
Ajuste o conteúdo HTML.	1. Abra o arquivo app.component.html. 2. Substitua o conteúdo pelo seguinte: <router-outlet></router-outlet> 3. Salve e feche o arquivo app.component.html.	Desenvolvedor de aplicativos

Execute os aplicativos localmente

Tarefa	Descrição	Habilidades necessárias
Execute o `mfe1` aplicativo.	1. Digite o seguinte comando para iniciar o `mfe1` aplicativo: `npm start`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	2. Em um navegador da web, acesse `http://localhost:5000` . 3. Verifique se o micro-frontend pode ser executado de forma independente. O `mfe1` aplicativo deve ser renderizado corretamente sem erros.	
Execute o aplicativo shell.	1. Digite o comando a seguir para iniciar o aplicativo shell: `npm start` 2. Em um navegador da web, acesse `http://localhost:4200/mfe1` . 3. Verifique se o `mfe1` microfrontend está incorporado no aplicativo shell. O aplicativo do portal deve ser renderizado adequadamente, sem erros, e o `mfe1` aplicativo deve ser incorporado a ele.	Desenvolvedor de aplicativos

Refatore o aplicativo shell para lidar com um erro de carregamento do microfrontend

Tarefa	Descrição	Habilidades necessárias
Crie um módulo e um componente.	Na pasta raiz do aplicativo shell, insira os seguintes comandos para criar um	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	módulo e um componente para uma página de erro:
	`ng g module error-page --routing`
	`ng g c error-page`	

Ajuste o conteúdo HTML.	1. Abra o arquivo error-page.component.html. 2. Substitua o conteúdo pelo seguinte: `<p>Sorry, this page is not available.</p>` 3. Salve e feche o arquivo error-page.component.html.	Desenvolvedor de aplicativos
Defina o caminho de roteamento padrão.	1. Abra o arquivo error-page-routing.module.ts. 2. Defina a rota padrão da seguinte forma: `{ path: '', component: ErrorPageComponent },` 3. Salve e feche o error-page-routingarquivo .module.ts.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Crie uma função para carregar microfrontends.	1. Abra o arquivo app-routing.module.ts.
	2. Crie a seguinte função:
	`function loadMFE(url: string) { return loadRemoteModule({ type: 'module', remoteEntry: `${url}/remoteEntry.js`, exposedModule: './Module' }) .then(m => m.Mfe1Module) .catch( () => import('./error-page/error-page.module').then(m => m.ErrorPageModule) ); }`
	3. Modifique a `mfe1` rota para ser a seguinte:
	`{ path: 'mfe1', loadChildren: () => loadMFE(environment.mfe1URL) },`
	4. Salve e feche o arquivo app-routing.module.ts.
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Teste o tratamento de erros.	1. Se ainda não estiver em execução, digite o seguinte comando para iniciar o aplicativo shell:
	`npm start`
	2. Em um navegador da web, acesse `http://localhost:4200/mfe1` .
	3. Verifique se a página de erro foi renderizada. Você deve ver o seguinte texto:
	`Sorry, this page is not available.`
		Desenvolvedor de aplicativos

Implante os aplicativos usando AWS Amplify

Tarefa	Descrição	Habilidades necessárias
Implante o microfrontend.	1. Na CLI do Amplify, navegue até a pasta raiz do aplicativo de microfront-end. 2. Digite o seguinte comando para inicializar o Amplify: `amplify init` 3. Quando você for solicitado a inserir um nome para seu projeto do Amplify, pressione Enter. Isso	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	reutiliza o nome do arquivo package.json. 4. Quando você for solicitado a inicializar o projeto com a configuração acima, insira. `Yes` 5. Quando você for solicitado a selecionar um método de autenticação, escolha`AWS Profile`. 6. Selecione o perfil que você deseja usar. 7. Aguarde até que o Amplify inicialize o projeto. Quando esse processo for concluído , você receberá uma mensagem de confirmação no terminal. 8. Insira o comando a seguir para adicionar uma categoria de hospedage m do Amplify ao micro-fro ntend: `amplify add hosting` 9. Quando você for solicitad o a selecionar o módulo do plug-in, escolha`Hosting with Amplify Console`. 10. Quando você for solicitado a escolher um tipo, escolha`Manual deployment` .	

Tarefa	Descrição	Habilidades necessárias

	11. Instale as dependências do npm do projeto digitando o seguinte comando:
	`npm install`
	12. Publique o aplicativo no console do Amplify digitando o seguinte comando:
	`amplify publish -y`
	Quando a publicação estiver concluída, o Amplify retornará a URL do microfrontend.
	13. Copie o URL. Você precisa desse valor para atualizar o aplicativo shell.	

Tarefa	Descrição	Habilidades necessárias

Implante o aplicativo shell.	1. Na src/app/environmentspasta, abra o arquivo environments.prod.ts.
	2. Substitua o `mfe1URL` valor pelo URL do microfrontend implantado:
	`export const environment = { production: true, mfe1URL: 'https://<env>.<Amplify-app-ID>.amplifyapp.com' };`
	3. Salve e feche o arquivo environments.prod.ts.
	4. Na CLI do Amplify, navegue até a pasta raiz do aplicativo shell.
	5. Digite o seguinte comando para inicializar o Amplify:
	`amplify init`
	6. Quando você for solicitado a inserir um nome para seu projeto do Amplify, pressione Enter. Isso reutiliza o nome do arquivo package.json.
	7. Quando você for solicitado a inicializar o projeto com a configuração acima, insira. `Yes`
		Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias

	8. Quando você for solicitado a selecionar um método de autenticação, escolha`AWS Profile`.
	9. Selecione o perfil que você deseja usar.
	10. Aguarde até que o Amplify inicialize o projeto. Quando esse processo for concluído, você receberá uma mensagem de confirmação no terminal.
	11. Adicione uma categoria de hospedagem Amplify ao aplicativo shell:
	`amplify add hosting`
	12. Quando você for solicitado a selecionar o módulo do plug-in, escolha`Hosting with Amplify Console`.
	13. Quando você for solicitado a escolher um tipo, escolha`Manual deployment` .
	14. Instale as dependências do npm do projeto digitando o seguinte comando:
	`npm install`
	15. Publique o aplicativo shell no console do Amplify	

Tarefa	Descrição	Habilidades necessárias
	digitando o seguinte comando: `amplify publish -y` Quando a publicação estiver concluída, o Amplify retornará a URL do aplicativo shell implantado. 16 Anote o URL do aplicativo shell.	

Tarefa	Descrição	Habilidades necessárias
Ativar CORS.	Como os aplicativos shell e de microfrontend são hospedados de forma independente em domínios diferentes, você deve habilitar o compartilhamento de recursos de origem cruzada (CORS) no microfrontend. Isso permite que o aplicativo shell carregue o conteúdo de uma origem diferente. Para habilitar o CORS, você adiciona cabeçalhos personalizados. 1. Na CLI do Amplify, navegue até a pasta raiz do microfrontend. 2. Digite o comando: `amplify configure hosting` 3. Quando você for solicitado a definir configurações personalizadas, digiteY. 4. Faça login no e AWS Management Console, em seguida, abra o console do Amplify. 5. Escolha o micro-frontend. 6. No painel de navegação, escolha Hospedagem e, em seguida, escolha Cabeçalhos personalizados.	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	7. Escolha Editar.
	8. Na janela Editar cabeçalhos personalizados, digite o seguinte:
	
	`customHeaders:`
	`  - pattern: '*.js'`
	`    headers:`
	`      - key: Access-Control-Allow-Origin`
	`        value: '*'`
	`      - key: Access-Control-Allow-Methods`
	`        value: 'GET, OPTIONS'`
	`      - key: Access-Control-Allow-Headers`
	`        value: '*'`
	
	9. Escolha Salvar.
	10. Reimplante o microfrontend para aplicar os novos cabeçalhos personalizados.	

Tarefa	Descrição	Habilidades necessárias
Crie uma regra de reescrita no aplicativo shell.	O aplicativo Angular shell está configurado para usar HTML5 roteamento. Se o usuário fizer uma atualização definitiva, o Amplify tentará carregar uma página do URL atual. Isso gera um erro 403. Para evitar isso, você adiciona uma regra de reescrita no console do Amplify. Para criar a regra de regravação, siga estas etapas: 1. Na CLI do Amplify, navegue até a pasta raiz do aplicativo shell. 2. Digite o comando: `amplify configure hosting` 3. Quando você for solicitado a definir configurações personalizadas, digiteY. 4. Abra o console do Amplify. 5. Escolha o aplicativo shell. 6. No painel de navegação, escolha Hospedagem e, em seguida, escolha Regravações e redirecionamentos. 7. Na página Regravações e redirecionamentos,	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	escolha Gerenciar redirecionamentos. 8. Escolha Abrir editor de texto. 9. No editor JSON, insira o seguinte redirecionamento: `[ { "source": "/<*>", "target": "/index.html", "status": "404-200", "condition": null } ]` 10. Escolha Salvar.	
Teste o portal da web.	1. Em um navegador da Web, insira a URL do aplicativo shell implantado. 2. Verifique se o aplicativo shell e o microfrontend estão carregados corretamente.	Desenvolvedor de aplicativos

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Exclua os aplicativos.	Se você não precisar mais do shell e dos aplicativos de	AWS geral

Tarefa	Descrição	Habilidades necessárias
	microfrontend, exclua-os. Isso ajuda a evitar cobranças por recursos que você não está usando. 1. Faça login no e AWS Management Console, em seguida, abra o console do Amplify. 2. Escolha o micro-frontend. 3. No painel de navegação, escolha Configurações do aplicativo e, em seguida, escolha Configurações gerais. 4. Escolha Excluir aplicativo. 5. Na janela de confirmaç ão`delete`, insira e escolha Excluir aplicativo. 6. Repita essas etapas para excluir o aplicativo shell.	

Solução de problemas

Problema	Solução
Nenhum AWS perfil disponível ao executar o `amplify init` comando	Se você não tiver um AWS perfil configurado, ainda poderá continuar com o `amplify init` comando. No entanto, você precisa seleciona r a `AWS access keys` opção quando for solicitado o método de autenticação. Tenha sua chave de AWS acesso e chave secreta disponíveis.

Problema	Solução
	Como alternativa, você pode configurar um perfil nomeado para AWS CLI o. Para obter instruções, consulte Configurações e configurações do arquivo de credenciais na AWS CLI documentação.
Erro ao carregar entradas remotas	Se você encontrar um erro ao carregar as entradas remotas no arquivo main.ts do aplicativo shell, verifique se a `environment.mfe1URL` variável está definida corretamente. O valor dessa variável deve ser a URL do microfrontend.
Erro 404 ao acessar o micro-frontend	Se você receber um erro 404 ao tentar acessar o micro-frontend local, como em`http://localhost:4200/mfe1` , verifique o seguinte: • Para o aplicativo shell, verifique se a configuração de roteamento no arquivo app-routing.module.ts está configurada corretamente e se a função está chamando corretamente o microfrontend. `loadRemoteModule` • Para o micro-frontend, verifique se o arquivo webpack.config.js tem a **`exposes`** configuração correta e se o arquivo remoteEntry.js está sendo gerado corretamente.

Mais informações

AWS documentação

- Compreendendo e implementando microfront-ends em AWS(orientaçãoAWS prescritiva)
- Amplify CLI (documentação do Amplify)
- Amplify Hosting (documentação do Amplify)

Outras referências

- Federação de módulos
- Node.js
- Angular
- @angular -architects/module-federation

Implante um aplicativo de página única baseado em React no Amazon S3 e CloudFront

Criado por Jean-Baptiste Guillois (AWS)

Resumo

Um aplicativo de página única (SPA) é um site ou aplicativo da web que atualiza dinamicamente o conteúdo de uma página da Web exibida usando. JavaScript APIs Essa abordagem aprimora a experiência do usuário e o desempenho de um site porque atualiza apenas novos dados em vez de recarregar a página inteira do servidor.

Esse padrão fornece uma step-by-step abordagem para codificar e hospedar um SPA escrito em React no Amazon Simple Storage Service (Amazon S3) e na Amazon. CloudFront O SPA nesse padrão usa uma API REST que é configurada no Amazon API Gateway e exposta por meio de uma CloudFront distribuição da Amazon para simplificar o gerenciamento do compartilhamento de recursos de origem cruzada (CORS).

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Node.js e `npm`, instalado e configurado. Para obter mais informações, consulte a seção Fazer download da documentação de Node.js.
- Yarn, instalado e configurado. Para obter mais informações, consulte a documentação do Yarn.
- Git, instalado e configurado. Para obter mais informações, consulte a documentação do Git.

Arquitetura

Essa arquitetura é implantada automaticamente usando AWS CloudFormation (infraestrutura como código). Ele usa serviços regionais, como o Amazon S3 para armazenar os ativos estáticos e o Amazon CloudFront com o Amazon API Gateway para expor os endpoints da API regional (REST). Os registros do aplicativo são coletados usando a Amazon CloudWatch. Todas as chamadas de AWS API são auditadas em AWS CloudTrail. Todas as configurações de segurança (por exemplo, identidades e permissões) são gerenciadas no AWS Identity and Access Management (IAM). O

conteúdo estático é entregue pela rede de distribuição de CloudFront conteúdo (CDN) da Amazon, e as consultas de DNS são tratadas pelo Amazon Route 53.

Ferramentas

Serviços da AWS

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- A Amazon CloudFront acelera a distribuição do seu conteúdo da web entregando-o por meio de uma rede mundial de data centers, o que reduz a latência e melhora o desempenho.
- AWS CloudTrailajuda você a auditar a governança, a conformidade e o risco operacional do seu Conta da AWS.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Código

O código de aplicativo de amostra desse padrão está disponível no repositório de aplicativos de página única GitHub CORS baseado em React.

Práticas recomendadas

Ao usar o armazenamento de objetos do Amazon S3, você pode armazenar os ativos estáticos do seu aplicativo de forma segura, altamente resiliente, eficiente e econômica. Não há necessidade de usar um contêiner dedicado ou uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para essa tarefa.

Ao usar a rede de distribuição de CloudFront conteúdo da Amazon, você pode reduzir a latência que seus usuários podem experimentar ao acessar seu aplicativo. Você também pode conectar um firewall de aplicativo da web (AWS WAF) para proteger seus ativos contra ataques maliciosos.

Épicos

Criar e implantar localmente o código do aplicativo

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Execute o comando a seguir para clonar o repositório do aplicativo de amostra: `git clone https://github.com/aws-samples/react-cors-spa react-cors-spa && cd react-cors-spa`	Desenvolvedor de aplicativos, AWS DevOps
Implante o aplicativo localmente.	1. No diretório do projeto, execute o comando `npm install` para iniciar as dependências do aplicativo. 2. Execute o comando `yarn dev` para iniciar o aplicativo localmente.	Desenvolvedor de aplicativos, AWS DevOps
Acesse o aplicativo localmente.	Abra uma janela do navegador e insira o URL `http://localhost:3000` para acessar o aplicativo.	Desenvolvedor de aplicativos, AWS DevOps

Implantar a aplicação

Tarefa	Descrição	Habilidades necessárias
Implante o AWS CloudFormation modelo.	1. Faça login no e AWS Management Console, em seguida, abra o AWS CloudFormation console. 2. Selecione Criar pilha e Com novos recursos (padrão). 3. Selecione Carregar um arquivo de modelo. 4. Escolha Escolher arquivo, escolha o arquivo `react-cors-spa-stack.yaml` do repositório clonado e escolha Avançar. 5. Insira um nome para a pilha e escolha Avançar. 6. Mantenha as opções padrão, escolha Avançar. 7. Verifique as configurações finais da pilha e, em seguida, selecione Criar pilha.	Desenvolvedor de aplicativos, AWS DevOps
Personalize os arquivos de origem do seu aplicativo.	1. Depois que sua pilha for implantada, abra a guia Saída e identifique o `Bucket` nome e `APIDomain` o valor. 2. Copie o domínio CloudFront de distribuição para a API REST.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	3. Navegue até e<project_root>/src/pages/index.tsx , em seguida, insira ou cole esse domínio no valor da APIEndPoint variável na linha 13 do index.tsx arquivo.	
Crie o pacote do aplicativo.	No diretório do projeto, execute o comando yarn build para criar o pacote do aplicativo.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Implemente o pacote do aplicativo.	1. Abra o console Amazon S3. 2. Identifique e escolha o bucket S3 que foi criado anteriormente pela CloudFormation pilha. 3. Selecione Fazer upload e clique em Adicionar arquivo. 4. Escolha o conteúdo da sua `out` pasta. 5. Escolha Adicionar pasta e, em seguida, escolha o `_next` diretório. **Important** Escolha o `_next` diretório, não o conteúdo. 6. Escolha Fazer o upload para carregar os arquivos e o diretório em seu bucket do S3.	Desenvolvedor de aplicativos, AWS DevOps

Teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Acessar e testar o aplicativo.	Abra uma janela do navegador e cole o domínio de CloudFront distribuição (a `SPADomain` saída da CloudFormation pilha que você implantou anteriorm	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	ente) para acessar o aplicativo.	

Limpe os recursos

Tarefa	Descrição	Habilidades necessárias
Exclua os conteúdos do bucket do S3.	1. Abra o console do Amazon S3 e escolha o bucket que foi criado anteriormente pela pilha (o primeiro bucket cujo nome começa com). `react-cors-spa-` 2. Escolha Esvaziar para excluir o conteúdo do bucket. 3. Escolha o segundo bucket que foi criado anteriormente pela pilha (o segundo bucket cujo nome começa com `react-cors-spa-` e termina com `-logs`). 4. Escolha Esvaziar para excluir o conteúdo do bucket.	AWS DevOps, desenvolvedor de aplicativos
Exclua a AWS CloudFormation pilha.	1. Abra o AWS CloudFormation console e escolha a pilha que você criou anteriormente.	AWS DevOps, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	2. Escolha Excluir para excluir a pilha e todos os recursos relacionados.	

Recursos relacionados

Para implantar e hospedar seu aplicativo web, você também pode usar o AWS Amplify Hosting, que fornece um fluxo de trabalho baseado em Git para hospedar aplicativos web completos e sem servidor com implantação contínua. O Amplify Hosting faz parte do AWS Amplify, que fornece um conjunto de ferramentas e recursos específicos que permitem que desenvolvedores front-end web e móveis criem aplicativos completos de forma rápida e fácil. AWS

Mais informações

Para lidar com URLs solicitações inválidas pelo usuário que podem gerar erros 403, uma página de erro personalizada configurada na CloudFront distribuição captura erros 403 e os redireciona para o ponto de entrada do aplicativo (). `index.html`

Para simplificar o gerenciamento do CORS, a API REST é exposta por meio de uma CloudFront distribuição.

Implante uma API do Amazon API Gateway em um site interno usando endpoints privados e um Application Load Balancer

Criado por Saurabh Kothari (AWS)

Resumo

Esse padrão mostra como implantar uma API do Amazon API Gateway em um site interno que pode ser acessado a partir de uma rede on-premises.. Você aprende a criar um nome de domínio personalizado para uma API privada usando uma arquitetura projetada com endpoints privados, um Application Load Balancer, PrivateLink AWS e Amazon Route 53. Essa arquitetura evita as consequências não intencionais do uso de um nome de domínio personalizado e um servidor proxy para ajudar no roteamento baseado em domínio em uma API. Por exemplo, se você implantar um endpoint de nuvem privada virtual (VPC) em uma sub-rede não roteável, sua rede não conseguirá acessar o API Gateway. Uma solução comum é usar um nome de domínio personalizado e depois implantar a API em uma sub-rede roteável, mas isso pode interromper outros sites internos quando a configuração do proxy passar o tráfego (`execute-api.{region}.vpce.amazonaws.com`) para o AWS Direct Connect. Por fim, esse padrão pode ajudar você a atender aos requisitos organizacionais de uso de uma API privada que não pode ser acessada pela Internet e de um nome de domínio personalizado.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um certificado de Indicação do nome do servidor (SNI, Server Name Indication) para o site e a API
- Uma conexão de um ambiente local com uma conta da AWS que é configurada usando o AWS Direct Connect ou o AWS VPN Site-to-Site
- Uma zona hospedada privada com um domínio correspondente (por exemplo, domain.com) que é resolvida a partir de uma rede on-premises e encaminha consultas ao DNS para o Route 53
- Uma sub-rede privada roteável que pode ser acessada a partir de uma rede on-premises

Limitações

Para obter mais informações sobre cotas (anteriormente chamadas de limites) para balanceadores de carga, regras e outros recursos, consulte Cotas para seus Application Load Balancers na documentação do Elastic Load Balancing.

Arquitetura

Pilha de tecnologia

- Amazon API Gateway
- Amazon Route 53
- Application Load Balancer
- AWS Certificate Manager
- AWS PrivateLink

Arquitetura de destino

O diagrama a seguir mostra como um Application Load Balancer é implantado em uma VPC que direciona o tráfego da web para um grupo de destino do site ou do API Gateway com base nas regras de receptor do Application Load Balancer. O grupo de destino do API Gateway é uma lista de endereços IP do endpoint da VPC no API Gateway. O API Gateway está configurado para tornar a API privada com sua política de recursos. A política nega todas as chamadas que não sejam de um endpoint da VPC específico. Os nomes de domínio personalizados no gateway da API são atualizados para usar api.domain.com para a API e seu estágio. As regras do Application Load Balancer são adicionadas para rotear o tráfego com base no nome do host.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário de uma rede on-premises tenta acessar um site interno. A solicitação é enviada para ui.domain.com e api.domain.com. Em seguida, a solicitação é resolvida para o Application Load Balancer interno da sub-rede privada roteável. O SSL é encerrado no Application Load Balancer para ui.domain.com e api.domain.com.
2. As regras de receptor, configuradas no Application Load Balancer, verificam o cabeçalho do host.

   a. Se o cabeçalho do host para api.domain.com, a solicitação será encaminhada para o grupo de destino do API Gateway. O Application Load Balancer inicia uma nova conexão com o API Gateway pela porta 443.

b. Se o cabeçalho do host for ui.domain.com, a solicitação será encaminhada para o grupo de destino do site.

3. Quando a solicitação chega ao API Gateway, o mapeamento de domínio personalizado configurado no API Gateway determina o nome do host e qual API executar.

Automação e escala

As etapas desse padrão podem ser automatizadas usando a AWS CloudFormation ou o AWS Cloud Development Kit (AWS CDK). Para configurar o grupo de destino das chamadas do API Gateway, você precisa usar um recurso personalizado para recuperar o endereço IP do endpoint da VPC. A API chama describe-vpc-endpointse describe-network-interfacesretorna os endereços IP e o grupo de segurança, que podem ser usados para criar o grupo-alvo de endereços IP da API.

Ferramentas

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável.
- O AWS Certificate Manager (ACM) lida com a complexidade de criar, armazenar e renovar chaves e certificados SSL/TLS X.509 públicos e privados que protegem seus sites e aplicativos.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- PrivateLinkA AWS ajuda você a criar conexões unidirecionais e privadas de seus serviços VPCs para fora da VPC.

Épicos

Como criar um certificado de SNI

Tarefa	Descrição	Habilidades necessárias
Crie um certificado de SNI e importe-o para o ACM.	1. Crie um certificado de SNI para ui.domain.com e api.domain.com. Para obter mais informações,	Administrador de rede

Tarefa	Descrição	Habilidades necessárias
	consulte Escolhendo como CloudFront atende às solicitações HTTPS na CloudFront documentação da Amazon. 2. Importe certificados de SNI para o AWS Certificate Manager (ACM). Para obter mais informações, consulte Importar certificados para o AWS Certificate Manager na documentação do ACM.	

Implante um endpoint da VPC em uma sub-rede privada não roteável

Tarefa	Descrição	Habilidades necessárias
Criar um endpoint da VPC de interface do API Gateway	Para criar um endpoint da VPC de interface, siga as instruções em Acessar serviço da AWS usando um endpoint da VPC de interface na documentação da Amazon Virtual Private Cloud (Amazon VPC).	Administrador de nuvem

Configure o Application Load Balancer.

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de destino para seu aplicativo.	Crie um grupo de destino para os recursos de interface do usuário do seu aplicativo.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um grupo de destino para o endpoint do API Gateway.	1. Crie um grupo de destino com um tipo de endereço IP e, em seguida, adicione o endereço IP do endpoint da VPC para o endpoint do API Gateway ao grupo de destino. 2. Configure verificações de saúde para seus grupos-alvo com o código de sucesso 403. 403 é necessário porque o VPC endpoint para o API Gateway retorna um código 403 quando é invocado sem nenhum cabeçalho pela verificação de integrida de do grupo-alvo.	Administrador de nuvem
Criar um Application Load Balancer.	1. Crie um Application Load Balancer (interno) em uma sub-rede privada roteável. 2. Adicione o receptor 443 ao Application Load Balancer e escolha o certificado do ACM.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Cria regras de receptor.	Crie regras de receptor para fazer o seguinte: 1. Encaminhe o host api.domain.com para o grupo de destino do API Gateway 2. Encaminhe o host ui.domain.com para o grupo de destino dos recursos de interface do usuário	Administrador de nuvem

Configure o Route 53

Tarefa	Descrição	Habilidades necessárias
Criar uma zona hospedada privada	Crie uma zona hospedada privada para domain.com.	Administrador de nuvem
Crie registros de domínio.	Crie registros CNAME para o seguinte: • Uma API com o valor definido como o nome DNS do Application Load Balancer • Uma IU com o valor definido como o nome DNS do Application Load Balancer	Administrador de nuvem

Criar um endpoint de API privado no API Gateway

Tarefa	Descrição	Habilidades necessárias
Crie e configure um endpoint de API privada.	1. Para criar um endpoint de API privado, siga as instruções em Como criar uma API privada no Amazon API Gateway na documentação do API Gateway. 2. Configure a política de recursos para permitir chamadas somente para a API a partir do endpoint da VPC. Para obter mais informações, consulte Como controlar o acesso a uma API com as políticas de recursos na documentação do API Gateway.	Desenvolvedor de aplicativos, administrador de nuvem
Criar um nome de domínio personalizado	1. Crie um nome de domínio personalizado para api.domain.com. Para obter mais informações, consulte Configuração de nomes de domínio personalizados para REST APIs na documentação do API Gateway. 2. Selecione a API e o estágio criados. Para obter mais informações, consulte Como trabalhar com mapeamentos de API para	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	REST APIs na documentação do API Gateway.	

Recursos relacionados

- Amazon API Gateway
- Amazon Route 53
- Application Load Balancer
- AWS PrivateLink
- AWS Certificate Manager

Incorpore um QuickSight painel da Amazon em um aplicativo Angular local

Criado por Sean Griffin (AWS) e Milena Godau (AWS)

Resumo

Esse padrão fornece orientação para incorporar um QuickSight painel da Amazon em um aplicativo Angular hospedado localmente para desenvolvimento ou teste. O recurso de análise incorporada QuickSight não oferece suporte nativo a essa funcionalidade. Isso requer uma QuickSight conta com um painel existente e conhecimento do Angular.

Quando você trabalha com QuickSight painéis incorporados, normalmente precisa hospedar seu aplicativo em um servidor web para visualizar o painel. Isso dificulta o desenvolvimento, porque você precisa enviar continuamente suas alterações para o servidor da Web para garantir que tudo esteja se comportando corretamente. Esse padrão mostra como executar um servidor hospedado localmente e usar análises QuickSight incorporadas para tornar o processo de desenvolvimento mais fácil e simplificado.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS)
- Uma QuickSight conta ativa com preços de capacidade de sessão
- QuickSight SDK de incorporação instalado
- CLI do Angular instalada
- Familiaridade com o Angular
- mkcert instalado

Limitações

- Esse padrão fornece orientação sobre como incorporar um QuickSight painel usando o tipo de autenticação `ANONYMOUS` (acessível ao público). Se você estiver usando o AWS Identity and Access Management (IAM) ou a QuickSight autenticação com seus painéis incorporados, o código fornecido não se aplicará. No entanto, as etapas para hospedar o aplicativo Angular na seção Epics (Épicos) ainda são válidas.
- Usar a GetDashboardEmbedUrlAPI com o tipo de `ANONYMOUS` identidade exige um plano QuickSight de preços de capacidade.

Versões

- CLI do Angular versão 13.3.4
- QuickSight SDK de incorporação versão 2.3.1

Arquitetura

Pilha de tecnologia

- Frontend do Angular
- Backend do AWS Lambda e do Amazon API Gateway

Arquitetura

Nessa arquitetura, o HTTP APIs no API Gateway permite que o aplicativo Angular local chame a função Lambda. A função Lambda retorna a URL para incorporar o painel. QuickSight

Automação e escala

Você pode automatizar a implantação de back-end usando a AWS ou o CloudFormation AWS Serverless Application Model (AWS SAM).

Ferramentas

Ferramentas

- A CLI do Angular é uma ferramenta de interface de linha de comando usada para inicializar, desenvolver, estruturar e manter aplicativos do Angular diretamente de um shell de comando.
- QuickSight O SDK de incorporação é usado para incorporar QuickSight painéis em seu HTML.
- mkcert é uma ferramenta simples para criar certificados de desenvolvimento confiáveis localmente. Não requer configuração. O mkcert é necessário porque QuickSight permite somente solicitações HTTPS para a incorporação de painéis.

Serviços da AWS

- O Amazon API Gateway é um serviço da AWS para criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.

- O AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- QuickSightA Amazon é um serviço de análise de negócios para criar visualizações, realizar análises ad hoc e obter insights de negócios a partir de seus dados.

Épicos

Gerar EmbedURL

Tarefa	Descrição	Habilidades necessárias
Crie uma EmbedUrl política.	Crie uma política do IAM chamada QuicksightGetDashboardEmbedUrlque tenha as propriedades a seguir. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "quicksight:GetDashboardEmbedUrl", "quickSight:GetAnonymousUserEmbedUrl" ], "Resource": "*" } ]`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	} ```	

Tarefa	Descrição	Habilidades necessárias

Criar a função do Lambda.	1. No console do Lambda, abra a página Funções.
	
	2. Escolha Criar função.
	
	3. Escolha Criar do zero.
	
	4. Em Function name (Nome da função), insira `get-qs-embed-url` .
	
	5. Em Runtime, escolha Python 3.9.
	
	6. Escolha Criar função.
	
	7. Na guia Código, copie o código a seguir na função do Lambda.
	
	`import json`
	`import boto3`
	`from botocore.exceptions import ClientError`
	`import time`
	`from os import environ`
	
	`qs = boto3.client('quicksight',region_name='us-east-1')`
	`sts = boto3.client('sts')`
	
	`ACCOUNT_ID = boto3.client('sts').get_caller_identity().get('Account')`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	DASHBOARD_ID =
	 environ['DASHBOARD
	_ID']
	
	def getDashboardURL(ac
	countId, dashboardId,
	 quicksightNamespac
	e, resetDisabled,
	 undoRedoDisabled):
	  try:
	  response = qs.get_da
	shboard_embed_url(
	  AwsAccountId =
	 accountId,
	  DashboardId =
	 dashboardId,
	  Namespace =
	 quicksightNamespace,
	  IdentityType =
	 'ANONYMOUS',
	  SessionLi
	fetimeInMinutes = 600,
	  UndoRedoDisabled
	 = undoRedoDisabled,
	  ResetDisabled =
	 resetDisabled
	  )
	  return response
	
	  except ClientError as
	 e:
	  print(e)
	  return "Error
	 generating embeddedU
	RL: " + str(e)
	
	def lambda_handler(eve
	nt, context):
	  url = getDashbo
	ardURL(ACCOUNT_ID,
	 DASHBOARD_ID,	

Tarefa	Descrição	Habilidades necessárias

	"default", True, True)
	['EmbedUrl']
	return {
	'statusCode':
	200,
	'url': url
	}
	
	8. Escolha Implantar.	

Tarefa	Descrição	Habilidades necessárias
Adicione o ID do painel como uma variável de ambiente.	Adicione a variável de ambiente `DASHBOARD_ID` à função do Lambda: 1. Na guia Configuração, selecione Variáveis de ambiente, Editar, Adicionar variável de ambiente. 2. Adicione uma variável de ambiente com a chave `DASHBOARD_ID` . 3. Para obter o valor de`DASHBOARD_ID` , navegue até seu painel QuickSight e copie o UUID no final da URL em seu navegador. Por exemplo, se o URL for `https://us-east-1.quicksight.aws.amazon.com/sn/dashboards/<dashboard-id>` , especifique a parte `<dashboard-id>` do URL como o valor da chave. 4. Escolha Salvar.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Adicione permissões para a função do Lambda.	Modifique a função de execução da função Lambda e adicione a Quicksigh tGetDashboardEmbed Urlpolítica a ela. 1. Na guia Configuração, selecione Permissões e, em seguida, selecione o nome do perfil. 2. Selecione Anexar políticas), pesquise por `Quicksigh tGetDashboardEmbed Url` , marque a caixa de seleção correspondente e selecione Anexar política.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Testar a função do Lambda.	Crie e execute um evento para teste. Você pode usar o modelo “Hello World”, porque a função não usará nenhum dado no evento de teste. 1. Selecione a guia Testar. 2. Dê um nome ao seu evento de teste e selecione Salvar. 3. Para testar sua função do Lambda, escolha Testar. A resposta deve ser semelhante à seguinte. `{ "statusCode": 200, "url": "\"https://us-east-1.quicksight.aws.amazon.com/embed/f1acc0786687783b9a4543a05ba929b3a/dashboards/... }` Note Conforme mencionado na seção Pré-requisitos e limitações, sua QuickSight conta deve estar sob um plano de preços de capacidade e de sessão. Caso contrário, esta	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	etapa exibirá uma mensagem de erro.	

Tarefa	Descrição	Habilidades necessárias
Crie uma API no API Gateway.	1. No console do API Gateway, selecione Criar API e, em seguida, selecione API REST, Construir. • Para o nome da API, insira `qs-embed-api` . • Selecione Criar API. 2. Em Ações, escolha Criar método. • Selecione OBTER e confirme escolhendo a marca de seleção. • Escolha Função do Lambda como tipo de integração. • Em Função do Lambda, insira `get-qs-embed-url`. • Escolha Salvar. • Na caixa Adicionar permissão à função do Lambda, escolha OK. 3. Ativar CORS. • Em Ações, selecione Ativar CORS. • Para Access-Control-Allow-Origin, insira `'https://my-qs-app.net:4200'` . • Escolha Habilitar CORS e substituir cabeçalho	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	s CORS existentes e confirme. 4. Implantar a API. • Em Ações selecione Implantar API. • Em Estágio de implantação, escolha Novo estágio. • Em Stage name (Nome do estágio), insira `dev`. • Escolha Deploy (Implantar). • Copie o URL do Invoke. **Note** `my-qs-app.net` pode ser qualquer domínio. Se quiser usar um nome de domínio diferente, atualize as informações de Access-Control-Allow-Origin na etapa 3 e altere `my-qs-app.net` nas etapas subsequentes.	

Crie o aplicativo Angular

Tarefa	Descrição	Habilidades necessárias

Crie o aplicativo com a CLI do Angular.	1. Criar o aplicativo.
	`ng new quicksight-app --defaults`
	`cd quicksight-app/src/app`
	2. Crie o componente do painel.
	`ng g c dashboard`
	3. Navegue até seu arquivo `src/environments/environment.ts` e adicione `apiUrl: '<Invoke URL from previous steps>'` ao objeto do ambiente.
	`export const environment = { production: false, apiUrl: '<Invoke URL from previous steps>', };`
		Desenvolvedor de aplicativos

Adicione o SDK QuickSight de incorporação.	1. Instale o SDK QuickSight de incorporação executando o comando a seguir na pasta raiz do seu projeto.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	``` npm i amazon-qu icksight-embedding- sdk ``` 2. Crie um novo arquivo `decl.d.ts` na pasta `src` com o seguinte conteúdo. ``` declare module 'amazon-quicksight- embedding-sdk'; ```	

Tarefa	Descrição	Habilidades necessárias

Adicione código ao seu arquivo dashboard.component.ts.	`import { Component, OnInit } from '@angular/core';`
	`import { HttpClient } from '@angular/common/http';`
	`import * as QuicksightEmbedding from 'amazon-quicksight-embedding-sdk';`
	`import { environment } from "../../environments/environment";`
	`import { take } from 'rxjs';`
	`import { EmbeddingContext } from 'amazon-quicksight-embedding-sdk/dist/types';`
	`import { createEmbeddingContext } from 'amazon-quicksight-embedding-sdk';`
	
	`@Component({`
	`  selector: 'app-dashboard',`
	`  templateUrl: './dashboard.component.html',`
	`  styleUrls: ['./dashboard.component.scss']`
	`})`
	`export class DashboardComponent implements OnInit {`
	
	`  constructor(private http: HttpClient) { }`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	`  loadingError = false;`
	`  dashboard: any;`
	
	`  ngOnInit() {`
	`  this.GetDashboardU`
	`RL();`
	`  }`
	
	`  public GetDashbo`
	`ardURL() {`
	`  this.http.get(envi`
	`ronment.apiUrl)`
	`  .pipe(`
	`  take(1),`
	`  )`
	`  .subscribe((data:`
	` any) => this.Dash`
	`board(data.url));`
	`  }`
	
	`  public async Dashboard`
	`(embeddedURL: any) {`
	`  var containerDiv`
	` = document.getElemen`
	`tById("dashboardCo`
	`ntainer") || '';`
	`  const frameOptions`
	` = {`
	`  url: embeddedURL,`
	`  container:`
	` containerDiv,`
	`  height: "850px",`
	`  width: "100%",`
	`  resizeHei`
	`ghtOnSizeChangedEv`
	`ent: true,`
	`  }`
	`  const embedding`
	`Context: Embedding`
	`Context = await`
	` createEmbeddingCon`
	`text();`	

Tarefa	Descrição	Habilidades necessárias
	`this.dashboard = embeddingContext.embedDashboard(frameOptions); } }`	
Adicione código ao seu arquivo dashboard.component.html.	Adicione o seguinte código ao arquivo `src/app/dashboard/dashboard.component.html` . `<div id="dashboardContainer"></div>`	Desenvolvedor de aplicativos
Modifique seu arquivo app.component.html para carregar seu componente do painel.	1. Exclua o conteúdo do arquivo `src/app/app.component.html` . 2. Adicione o seguinte. `<app-dashboard></app-dashboard>`	Desenvolvedor de aplicativos
Importe HttpClientModule para seu arquivo app.module.ts.	1. No topo do arquivo `src/app/app.module.ts` , adicione o seguinte. `import { HttpClientModule } from '@angular/common/http';` 2. Adicione `HttpClientModule` à matriz `imports` do seu `AppModule` .	Desenvolvedor de aplicativos

Host o aplicativo Angular

Tarefa	Descrição	Habilidades necessárias

Configure o mkcert.	**Note**
	Os comandos a seguir são para máquinas Unix ou macOS. Se você estiver usando o Windows, consulte a seção Informações adicionais para o comando echo equivalente.
	
	1. Crie uma autoridade de certificação (CA) local em sua máquina.
	`mkcert -install`
	2. Configure `my-qs-app.net` para sempre redirecionar para seu PC local.
	`echo "127.0.0.1 my-qs-app.net" | sudo tee -a /private/etc/hosts`
	3. Certifique-se de que você esteja no diretório `src` do projeto do Angular.
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`mkcert my-qs-app.net 127.0.0.1`	
Configure QuickSight para permitir seu domínio.	1. Em QuickSight, escolha seu nome no canto superior direito e escolha Gerenciar Quicksight. 2. Navegue até Domínios e incorporação. 3. Adicione `https://my-qs-app.net:4200` como um domínio permitido.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Testar a solução.	Inicie um servidor de desenvolvimento local do Angular executando o seguinte comando. `ng serve --host my-qs-app.net --port 4200 --ssl --ssl-key "./src/my-qs-app.net-key.pem" --ssl-cert "./src/my-qs-app.net.pem" -o` Isso ativa o Secure Sockets Layer (SSL) com o certifica do personalizado criado anteriormente. Quando a compilação estiver concluída, ela abrirá uma janela do navegador e você poderá visualizar seu QuickSight painel incorpora do hospedado localmente no Angular.	Desenvolvedor de aplicativos

Recursos relacionados

- Site do Angular
- Incorporação de painéis de QuickSight dados para usuários anônimos (não registrados) (documentação) QuickSight
- QuickSight SDK de incorporação
- ferramenta do mkcert

Mais informações

Se você estiver usando o Windows, execute a janela do Prompt de Comando como administrador e configure `my-qs-app.net` para sempre redirecionar para o PC local usando o comando a seguir.

```
echo 127.0.0.1 my-qs-app.net >> %WINDIR%\System32\Drivers\Etc\Hosts
```

Explore o desenvolvimento completo de aplicativos web nativos de nuvem com o Green Boost

Criado por Ben Stickley (AWS) e Amiin Samatar (AWS)

Resumo

Em resposta às crescentes necessidades dos desenvolvedores, a Amazon Web Services (AWS) reconhece a demanda crítica por uma abordagem eficiente para o desenvolvimento de aplicativos web nativo de nuvem. O foco da AWS é ajudar você a superar obstáculos comuns associados à implantação de aplicativos web de nuvem AWS. Ao aproveitar os recursos de tecnologias modernas, como o TypeScript AWS Cloud Development Kit (AWS CDK), o React e o Node.js, esse padrão visa simplificar e agilizar o processo de desenvolvimento.

Apoiado pelo kit de ferramentas Green Boost (GB), o padrão oferece um guia prático para a estruturação de aplicativos web que usam os amplos recursos da AWS em sua totalidade. Ele atua como um roteiro abrangente, guiando você pelo processo de implantação de um aplicativo web CRUD (Criar, ler, atualizar, excluir) fundamental integrado à edição do Amazon Aurora compatível com PostgreSQL. Isso é feito usando a interface de linha de comando Green Boost (CLI do Green Boost) e estabelecendo um ambiente de desenvolvimento local.

Após a implantação bem-sucedida do aplicativo, o padrão investiga os principais componentes do aplicativo web, incluindo design de infraestrutura, desenvolvimento de backend e frontend e ferramentas essenciais, como cdk-dia, para visualização, facilitando o gerenciamento eficiente de projetos.

Pré-requisitos e limitações

Pré-requisitos

- Git instalado
- Visual Studio Code (VS Code) instalado
- AWS Command Line Interface (AWS CLI) instalado
- Kit de ferramentas AWS CDK instalado
- Node.js 18 instalado ou Node.js 18 com pnpm ativado
- pnpm instalado, se não fizer parte da instalação do Node.js
- Familiaridade básica com TypeScript AWS CDK, Node.js e React

- Uma conta AWS ativa
- Bootstrap de uma conta da AWS usando o AWS CDK em `us-east-1`. A região `us-east-1` da AWS é necessária para dar suporte às funções do Amazon CloudFront Lambda @Edge.
- Credenciais de segurança da AWS, inclusive `AWS_ACCESS_KEY_ID`, configuradas corretamente em seu ambiente de terminal
- Para usuários do Windows, um terminal no modo administrador (para acomodar a forma como o pnpm manipula os módulos de nós)

Versões do produto

- AWS SDK para a JavaScript versão 3
- AWS CDK versão 2
- AWS CLI versão 2.2
- Node.js versão 18
- React versão 18

Arquitetura

Pilha de tecnologias de destino

- Amazon Aurora Edição Compatível com PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch
- Nuvem de computação elástica da Amazon (Amazon EC2)
- AWS Lambda
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS WAF

Arquitetura de destino

O diagrama a seguir mostra que as solicitações dos usuários passam pela Amazon CloudFront, AWS WAF e AWS Lambda antes de interagir com um bucket do S3, um banco de dados Aurora, uma

instância e, finalmente EC2 , chegar aos desenvolvedores. Os administradores, por outro lado, usam o Amazon SNS e a CloudWatch Amazon para fins de notificações e monitoramento.

Para obter uma visão mais aprofundada do aplicativo após a implantação, você pode criar um diagrama usando cdk-dia, conforme mostrado no exemplo a seguir.

Esses diagramas mostram a arquitetura do aplicativo web a partir de dois ângulos distintos. O diagrama cdk-dia oferece uma visão técnica detalhada da infraestrutura de o AWS CDK, destacando serviços específicos da AWS, como o Amazon Aurora compatível com PostgreSQL e o AWS Lambda. Por outro lado, o outro diagrama tem uma perspectiva mais ampla, enfatizando o fluxo lógico de dados e as interações do usuário. A principal distinção está no nível de detalhe: o cdk-dia investiga as complexidades técnicas, enquanto o primeiro diagrama fornece uma visão mais centrada no usuário.

A criação do diagrama cdk-dia é abordada no épico Understand the app infrastructure by using AWS CDK (Entenda a infraestrutura do aplicativo usando o AWS CDK).

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- A Amazon CloudFront acelera a distribuição do seu conteúdo da web entregando-o por meio de uma rede mundial de data centers, o que reduz a latência e melhora o desempenho.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.

- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente.
- O AWS Systems Manager ajuda você a gerenciar seus aplicativos e infraestrutura em execução na nuvem AWS. Isso simplifica o gerenciamento de aplicações e recursos, diminui o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus recursos da AWS de modo seguro e em grande escala. Esse padrão usa o Session Manager do AWS Systems Manager.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado em nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados. O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O AWS WAF é um firewall para aplicativos web que ajuda você a monitorar solicitações HTTP e HTTPS que são encaminhadas aos recursos protegidos do seu aplicativo web

Outras ferramentas

- O Git é um sistema de controle de versão distribuído e de código aberto.
- O Green Boost é um kit de ferramentas para criar aplicativos web na AWS.
- O Next.js é uma estrutura do React para adicionar atributos e otimizações.
- O Node.js é um ambiente de tempo de JavaScript execução orientado a eventos projetado para criar aplicativos de rede escaláveis.
- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.
- O pnpm é um gerenciador de pacotes para dependências do projeto Node.js.

Práticas recomendadas

Consulte a seção Épicos para obter mais informações sobre as seguintes recomendações:

- Monitore a infraestrutura usando CloudWatch painéis e alarmes da Amazon.
- Aplique as práticas recomendadas da AWS usando cdk-nag para executar a análise estática de infraestrutura como código (IaC).
- Estabeleça o encaminhamento de portas de banco de dados por meio de tunelamento SSH (Secure Shell) com o Session Manager do Systems Manager, que é mais seguro do que ter um endereço IP exposto publicamente.
- Gerencie vulnerabilidades executando o `pnpm audit`.
- Aplique as melhores práticas usando ESLintpara realizar análises estáticas de TypeScript código e Prettier para padronizar a formatação de código.

Épicos

Implemente um aplicativo web CRUD com o Aurora compatível com PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Instale a CLI do Green Boost.	Para instalar o Green Boost CLI, execute o seguinte comando. `pnpm add -g gboost`	Desenvolvedor de aplicativos
Crie um aplicativo do GB.	1. Para criar um aplicativo usando o Green Boost, execute o comando `gboost create`. 2. Escolha o modelo `CRUD App with Aurora PostgreSQL` .	Desenvolvedor de aplicativos
Instale dependências e implante o aplicativo.	1. Navegue até o diretório de projeto do `cd <your directory>` . 2. Para instalar dependências, execute o comando `pnpm i`.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	3. Navegue até o diretório infra: `cd infra`. 4. Para implantar o aplicativo localmente, execute o comando `pnpm deploy:local` . Esse é um alias para um comando `cdk deploy ...` definido em `infra/package.json` . Aguarde a conclusão da implantação (aproximadamente 20 minutos). Enquanto você espera, monitore as CloudFormation pilhas da AWS no CloudFormation console. Observe como as estruturações definidas no código são mapeadas para o recurso implantado. Analise a visualização em árvore do CDK Construct no CloudFormation console.	

Tarefa	Descrição	Habilidades necessárias
Acesse o aplicativo.	Depois de implantar seu aplicativo GB localmente, você pode acessá-lo usando o CloudFront URL. O URL é impresso na saída do terminal, mas pode ser um pouco difícil encontrá-lo. Para encontrá-lo mais rapidamente, siga as seguintes etapas: 1. Abra o terminal em que você executou o comando `pnpm deploy:local` . 2. Procure uma seção na saída do terminal que se assemelhe ao texto a seguir. `myapp5stickbui9C39A55A.CloudFrontDomainName = d1q16n5pof924c.cloudfront.net` O URL será exclusivo para a implantação. Como alternativa, você pode encontrar a CloudFront URL acessando o CloudFront console da Amazon: 1. Faça login no AWS Management Console e	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	navegue até o CloudFront serviço. 2. Procure a distribuição mais recente implantada na lista. Copie o Nome de domínio associado à distribuição. Ele se parece com `your-unique-id.cloudfront.net` .	

Monitore usando a Amazon CloudWatch

Tarefa	Descrição	Habilidades necessárias
Veja o CloudWatch painel.	1. Abra o CloudWatch console e escolha Painéis. 2. Selecione o painel que tem o nome <appId>-<stageName>-dashboard. 3. Revise o painel. Quais recursos estão sendo monitorados? Quais métricas estão sendo registradas? Esse painel é possível graças à construção cdk-monitoring-constructsde código aberto.	Desenvolvedor de aplicativos
Habilitar alertas.	Um CloudWatch painel ajuda você a monitorar ativamente seu aplicativo web. Para monitorar passivamente seu	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	aplicativo da web, você pode ativar os alertas.
	
	1. Navegue até `/infra/src/app/stateless/monitor-stack.ts` , que define a pilha de monitores.
	2. Remova o comentário da linha a seguir e substitua `admin@example.com` pelo seu endereço de e-mail.
	
	`onAlarmTopic.addSubscription(new EmailSubscription("admin@example.com"));`
	
	3. Adicione as seguintes informações de importação ao início do arquivo.
	
	`import { EmailSubscription } from "aws-cdk-lib/aws-sns-subscriptions";`
	
	4. Dentro de `infra/`, execute o seguinte comando.
	
	`cdk deploy "*/monitor" --exclusively.`
	
	5. Para confirmar sua assinatura do tópico SNS que é iniciado quando um	

Tarefa	Descrição	Habilidades necessárias
	alarme de monitoramento é iniciado, escolha o link na mensagem de e-mail.	

Entenda a infraestrutura do aplicativo usando o AWS CDK

Tarefa	Descrição	Habilidades necessárias
Crie um diagrama de arquitetura.	Gere um diagrama de arquitetura do seu aplicativo web usando cdk-dia. A visualização da arquitetura ajuda a melhorar a compreensão e a comunicação entre os membros da equipe. Ele fornece uma visão geral clara dos componentes do sistema e seus relacionamentos. 1. Instale o Graphviz. 2. Dentro de `infra/`, execute o comando `pnpm cdk-dia`. 3. Exibir seu `infra/diagram.png` .	Desenvolvedor de aplicativos
Use o cdk-nag para aplicar as práticas recomendadas.	Use o cdk-nag para ajudar você a manter a infraestrutura segura e compatível, aplicando as práticas recomendadas, reduzindo o risco de vulnerabilidades de segurança e configurações incorretas.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	1. Explore a aplicação das práticas recomendadas da cdk-nag por meio de sua seção de regras, incluindo verificações do pacote de regras da Biblioteca de Soluções da AWS. 2. Para ver como o cdk-nag aplica as regras, faça uma alteração no código. Por exemplo, em `infra/src/app/stateful/data-stacks.ts` , altere `storageEncrypted: true` para `storageEncrypted: false` . 3. Dentro de `infra/`, execute o comando `cdk synth "*/data"`. Durante a síntese, você encontrará um erro de compilação que indica uma violação da regra. `AwsSolutions-RDS2: The RDS instance or Aurora DB cluster does not have storage encryption enabled.` Esse erro mostra como o cdk-nag é um mecanismo de segurança para aplicar as práticas recomendadas	

Tarefa	Descrição	Habilidades necessárias
	de infraestrutura e evitar configurações incorretas de segurança. 4. Se necessário, você também pode suprimir regras em escopos diferentes. Por exemplo, para suprimir AwsSolutions-RDS2, adicione o código a seguir abaixo da instanciação de. `DbIamCluster` `NagSuppressions.addResourceSuppressions( cluster.node.findChild("Resource"), [ { id: "AwsSolutions-RDS2", reason: "Customer requirement necessitates having unencrypted DB storage", }, ], );` 5. Após a supressão, execute `cdk synth "*/data"` novamente. Seu aplicativo AWS CDK agora deve ser sintetizado com sucesso. Você pode encontrar todas as regras suprimidas em `infra/cdk.out/asse`	

Tarefa	Descrição	Habilidades necessárias
	`mbly-<appId>-<stageName>/AwsSolutions-<appId>-<stageName>-${stackId}-NagReport.csv` .	

Avalie a configuração e o esquema do banco de dados

Tarefa	Descrição	Habilidades necessárias
Adquira variáveis de ambiente.	Para obter as variáveis de ambiente necessárias, use as seguintes etapas: 1. Para encontrar o`DB_BASTION_ID` , entre no console e navegue até o EC2 console. Escolha Instâncias (em execução) e encontre a linha que contém - ssm-db-bastion Nome<stageName>. O ID da instância começa com i-. 2. Para encontrar o `DB_ENDPOINT` , no console do Amazon Relational Database Service (Amazon RDS), selecione Instâncias do DB e selecione o cluster regional que tem um identificador de banco de dados começando com <appId>-<stageName>-	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	data. Localize o endpoint da instância do gravador, que termina com rds.amazonaws.com.	
Estabeleça o encaminhamento de portas.	Para estabelecer o encaminhamento de portas, siga as etapas a seguir: 1. Instale o plug-in do Session Manager do AWS Systems Manager. 2. Inicie o encaminhamento de portas executando `pnpm db:connect` dentro de `core/` para estabelecer uma conexão segura por meio de bastion host. 3. Depois de ver o texto `Waiting for connections...,` em seu terminal, um túnel SSH foi estabelecido com sucesso entre sua máquina local e o servidor Aurora por meio EC2 do host bastion.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Ajuste o tempo limite do Session Manager do Systems Manager.	(Opcional) Se o tempo limite padrão da sessão de 20 minutos for muito curto, você poderá aumentá-lo em até 60 minutos no console do Systems Manager selecionando Session Manager, Preferências, Editar, Tempo limite de sessão ociosa.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Visualize o banco de dados.	O pgAdmin é uma ferramenta de código aberto fácil de usar para gerenciar bancos de dados PostgreSQL. Ele simplifica as tarefas do banco de dados, permitindo que você crie, gerencie e otimize bancos de dados com eficiência. Esta seção orienta você na instalação do pgAdmin e no uso de seus atributos para o gerenciamento do banco de dados do PostgreSQL. 1. No Explorador de objetos, abra o menu de contexto (clique com o botão direito do mouse) para Servidores e selecione Registrar, Servidor. 2. Na guia Geral, insira <appId>-<stageName> no campo Nome. 3. Para buscar a senha do banco de dados, abra o console do AWS Secrets Manager, selecione o segredo que tem a descrição Gerado pelo CDK para a pilha: <appId>-<stageName>-data e escolha o cartão Valor de segredo. Selecione Recuperar valor de segredo	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	e copie o Valor de segredo com uma chave de senha. 4. Na guia Conexão, insira 0.0.0 no campo Nome/ endereço do host e insira <appId>_admin no campo Nome de usuário. No campo Senha, use o segredo que você buscou anteriormente. Escolha sim para o campo Salvar senha?. 5. Escolha Salvar. 6. Para visualizar as tabelas, navegue até <appId>-<stageName>, Bancos de dados, <appId>_db, Esquemas, <appId>, Tabelas. 7. Abra o menu de contexto (clique com o botão direito) da tabela de itens e selecione Exibir/Editar dados, Todas as linhas. 8. Explore a tabela.	

Depure com Node.js

Tarefa	Descrição	Habilidades necessárias
Depure o caso de uso do item criado.	Para depurar o caso de uso do item criado, siga estas etapas:	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	1. Abra o arquivo `core/src/modules/item/create-item.use-case.ts` e insira o seguinte código.
	
	`import { fileURLToPath } from "node:url";`
	
	`// existing create-item.use-case.ts code here`
	
	`if (process.argv[1] === fileURLToPath(import.meta.url)) {`
	`  createItemUseCase({`
	`  description: "Item 1's Description",`
	`  name: "Item 1",`
	`  });`
	`}`
	
	2. O código adicionado na etapa anterior garante que a função `createItemUseCase` seja chamada quando esse módulo for executado diretamente. Defina pontos de interrupção nas linhas desse bloco de código em que você deseja iniciar a depuração. line-by-line	

Tarefa	Descrição	Habilidades necessárias
	1. Abra o Terminal de JavaScript Depuração do VS Code e, em seguida, execute `pnpm tsx core/src/modules/item/create-item.use-case.ts` para executar o código com line-by-line depuração. Como alternativa, você pode usar `console.log` declarações, mas as declarações impressas podem ser inadequadas quando você está trabalhando com uma lógica comercial complexa. Line-by-linea depuração oferece mais contexto.	

Desenvolva o frontend

Tarefa	Descrição	Habilidades necessárias
Configure o servidor de desenvolvimento.	1. Navegue até `ui/` e execute `pnpm dev` para iniciar o servidor de desenvolvimento Next.js. 2. Acesse seu aplicativo web localmente em `http://localhost:3000`. O servidor de desenvolvimento do Next.js é configurado com feedback instantâneo do Fast	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Refresh sobre as edições feitas em seus component es do React. 3. Experimente personalizar a cor da barra de aplicativos. Abra o arquivo `ui/src/co mponents/theme/the me.tsx` e localize a seção que define o tema da barra de aplicativos. Na seção `colorSchemes.light .palette.primary` , atualize o valor principal de `colors.lagoon` para `colors.carrot` . Depois de fazer essa alteração, salve o arquivo e observe a atualização no seu navegador. 4. Experimente modificar texto, componentes e adicionar novas páginas.	

Ferramentas com Green Boost

Tarefa	Descrição	Habilidades necessárias
Configure o monorepo e o gerenciador de pacotes pnpm.	1. Revise `pnpm-work space.yaml` na raiz do seu repositório do GB e observe como os espaços de trabalho são definidos. Para obter mais informações sobre espaços	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	de trabalho, consulte a documentação do pnpm. 2. Analise `ui/package.json` e observe como ele faz referência ao espaço de trabalho `core/` com o nome do pacote `"<appId>/core": "workspace:^",` . 3. Observe como TypeScript a ESLint configuração é centralizada nos pacotes de utilitários definidos em `packages/` . Essa configuração é, então, usada por pacotes de aplicativos como `core/`, `infra/` e `ui/`. Isso é útil quando seu aplicativo é dimensionado e você define mais pacotes de aplicativos, que podem referenciar os pacotes de utilitários sem duplicar o código de configuração.	

Tarefa	Descrição	Habilidades necessárias
Execute scripts pnpm.	Execute os seguintes comandos na raiz do seu repositório: 1. Executar `pnpm lint`. Esse comando executa a análise estática de código com ESLint. 2. Executar `pnpm typecheck .` Esse comando executa o TypeScript compilador para verificar os tipos do seu código. 3. Executar `pnpm test`. Esse comando executa o Vitest para executar testes de unidade. Observe como esses comandos são executados em todos os espaços de trabalho. Os comandos são definidos no campo `package.json#scripts` de cada espaço de trabalho.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Use ESLint para análise de código estático.	Para testar a capacidade de análise de código estático do ESLint, faça o seguinte:
	
	1. Primeiro, certifique-se de que a ESLint extensão VS Code (ID:`dbaeumer.vscode-eslint`) esteja instalada. Recomendamos também instalar o VS Code Error Lens (ID: `usernamehw.errorlens`) para ver os erros em linha.
	2. Em seu código, inclua propositalmente uma linha de código que usa a função `eval()`, conforme mostrado no exemplo a seguir.
	
	``
	const userInput =
	"import("fs").then
	((fs) => console.l
	og(fs.readFileSync
	("/etc/passwd",
	{ encoding:
	"utf8" }))";
	eval(userInput);
	``
	
	Important
	Isso é apenas para fins de teste. O uso de `eval()` é considerado potencialmente
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	perigoso e deve ser evitado devido a riscos de segurança . 3. Depois de incluir a `eval()` linha, abra seu editor de código para confirmar se ESLint indicou o cheiro do código usando rabiscos vermelhos. 4. Revise ESLint os plug-ins e a configuração em `packages/eslint-config-{node,next}/.eslintrc.cjs` .	

Tarefa	Descrição	Habilidades necessárias
Gerencie dependências e vulnerabilidades.	1. Para identificar quaisquer vulnerabilidades e exposições comuns (CVEs), execute `pnpm audit` na raiz do seu repositório. Você deve ver Nenhuma vulnerabilidade conhecida encontrada. 2. Instale um pacote intencionalmente vulnerável em `core/` executando `pnpm add minimist@0.2.3` e, em seguida, `pnpm audit`. Observe a vulnerabilidade que está sendo relatada. 3. Desinstale o pacote vulnerável em `core/` executando `pnpm remove minimist`.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Pré-comprometa hooks com o Husky.	1. Faça algumas pequenas alterações nos TypeScript arquivos em todo o repositório. As mudanças podem ser tão simples quanto adicionar comentários. 2. Organize e confirme essas alterações usando `git add -A` e, depois, `git commit -m "test husky"`. O gatilho do hook de pré-confirmação do Husky, definido em `.husky/pre-commit` , executa o comando `pnpm lint-staged` . 3. Observe como o lint-staged executa comandos especificados em arquivos `*/.lintstagedrc.js` em todo o repositório em arquivos que foram preparados pelo Git. Essas ferramentas são mecanismos para ajudar a impedir que códigos incorretos entrem em seu aplicativo.	Desenvolvedor de aplicativos

Destrua a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Remova a implantação da sua conta.	1. Para destruir a infraestrutura que você provisionou no primeiro épico, execute `pnpm destroy:local` em `infra/`. 2. Aguarde 15 minutos após a conclusão de `pnpm destroy:local` e exclua a função do Lambda@Edge retida ao pesquisar o ID do seu aplicativo no console do Lambda. As funções do Lambda@Edge são replicadas, o que as torna difíceis de excluir. Para obter mais informações sobre como excluir funções do Lambda @Edge, consulte CloudFront a documentação.	Desenvolvedor de aplicativos

Solução de problemas

Problema	Solução
Não foi possível estabelecer o encaminhamento de porta	Certifique-se de que suas credenciais da AWS estejam configuradas adequadamente e tenham as permissões necessárias. Verifique novamente se as variáveis de ambiente bastion host ID (`DB_BASTION_ID`)

Problema	Solução
	e database endpoint (`DB_ENDPOINT `) estão definidas corretamente. Se você ainda encontrar problemas, consulte a documentação da AWS para a solução de problemas de conexões SSH e do Session Manager.
O site não está sendo carregado no `localhost:3000`	Confirme se a saída do terminal indica um encaminhamento de porta bem-sucedido, incluindo o endereço de encaminhamento. Certifique-se de que não haja processos conflitantes usando a porta 3000 em sua máquina local. Verifique se o aplicativo Green Boost está configurado e é executado corretamente na porta esperada (3000). Verifique se há extensões ou configurações de segurança em seu navegador que possam bloquear conexões locais.
Mensagens de erro durante a implantação local (`pnpm deploy:local `)	Analise cuidadosamente as mensagens de erro para identificar a causa do problema. Verifique se as variáveis de ambiente e os arquivos de configuração necessários estão definidos corretamente.

Recursos relacionados

- Documentação do AWS CDK
- Documentação do Green Boost
- Documentação do Next.js

- Documentação do Node.js
- Documentação do React
- TypeScript documentação

Execute testes unitários para um aplicativo Node.js GitHub usando a AWS CodeBuild

Criado por Thomas Scott (AWS) e Jean-Baptiste Guillois (AWS)

Resumo

Esse padrão fornece um exemplo de código-fonte e dos principais componentes de teste de unidade para uma API de jogo Node.js. Também inclui instruções para executar esses testes unitários a partir de um GitHub repositório usando a AWS CodeBuild, como parte de seu fluxo de trabalho de integração contínua e entrega contínua (CI/CD).

O teste de unidade é um processo de desenvolvimento de software no qual diferentes partes de um aplicativo, chamadas de unidades, são testadas de forma individual e independente para operação correta. Os testes validam a qualidade do código e confirmam que ele funciona conforme o esperado. Outros desenvolvedores também podem se familiarizar facilmente com sua base de código consultando os testes. Os testes de unidade reduzem o tempo futuro de refatoração, ajudam os engenheiros a se familiarizarem com sua base de código com mais rapidez e fornecem confiança no comportamento esperado.

O teste de unidade envolve testar funções individuais, incluindo funções do AWS Lambda. Para criar testes de unidade, você precisa de uma estrutura de testes e de uma forma de validar testes (asserções). Os exemplos de código nesse padrão usam a estrutura de teste Mocha e a biblioteca de asserções Chai.

Para obter mais informações sobre testes de unidade e exemplos de componentes de teste, consulte a seção Informações adicionais.

Pré-requisitos e limitações

- Uma conta ativa da AWS com CodeBuild as permissões corretas
- Uma GitHub conta (veja as instruções para se inscrever)
- Git (consulte as instruções de instalação)
- Um editor de código para fazer alterações e enviar seu código para GitHub

Arquitetura

Esse padrão implementa a arquitetura mostrada no diagrama a seguir.

Ferramentas

Ferramentas

- O Git é um sistema de controle de versão que você pode usar para desenvolvimento de código.
- CodeBuildA AWS é um serviço de integração contínua totalmente gerenciado que compila o código-fonte, executa testes e produz pacotes de software prontos para implantação. Com CodeBuild, você não precisa provisionar, gerenciar e escalar seus próprios servidores de compilação. CodeBuild escala continuamente e processa várias compilações simultaneamente, para que suas compilações não fiquem esperando em uma fila. Você pode começar a usar ambientes de compilação pré-empacotados rapidamente ou criar ambientes de compilação personalizados que usem suas próprias ferramentas de compilação. Com CodeBuild, você é cobrado por minuto pelos recursos computacionais que usa.

Código

O código-fonte desse padrão está disponível em GitHub, no repositório de aplicativos Sample Game Unit Test. Você pode criar seu próprio GitHub repositório a partir dessa amostra (opção 1) ou usar o repositório de amostra diretamente (opção 2) para esse padrão. Siga as instruções de cada opção na próxima seção. A opção que você seguirá dependerá do seu caso de uso.

Épicos

Opção 1 - Execute testes de unidade em seu GitHub repositório pessoal com CodeBuild

Tarefa	Descrição	Habilidades necessárias
Crie seu próprio GitHub repositório com base no projeto de amostra.	1. Faça login em GitHub. 2. Crie um novo repositór io. Para obter instruçõe s, consulte a GitHub documentação. 3. Clone e envie o repositór io de amostra para o novo repositório em sua conta.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Crie um novo CodeBuild projeto.	1. Faça login no AWS Management Console e abra o CodeBuild console em https://console.aws.amazon.com/codesuite/codebuild/home. 2. Selecione Create build project (Criar projeto de compilação). 3. Na seção Configuração do projeto, em Nome do projeto, digite aws-tests-sample-node-js. 4. Na seção Fonte, em Provedor de origem, escolha GitHub. 5. Em Repositório, escolha Repositório em minha GitHub conta e cole a URL no seu repositório recém-criado GitHub . 6. Na seção Primary source webhook events (Eventos de webhook de origem primária), selecione Rebuild every time a code change is pushed to this repository (Recompilar sempre que uma alteração de código é enviada a esse repositório). 7. Em Event type (Tipo de evento), selecione PUSH.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	8. Na seção Ambiente, escolha Imagem gerenciada, Amazon Linux e a imagem mais recente. 9. Deixe as configurações padrão para todas as outras opções e, em seguida, escolha Criar projeto de compilação.	
Inicie a compilação.	Na página Revisão, escolha Iniciar compilação para executar a compilação.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Opção 2 - Executar testes unitários em um repositório público com CodeBuild

Tarefa	Descrição	Habilidades necessárias
Crie um novo projeto de CodeBuild construção.	1. Faça login no AWS Management Console e abra o CodeBuild console em https://console.aws.amazon.com/codesuite/codebuild/home. 2. Selecione Create build project (Criar projeto de compilação). 3. Na seção Configuração do projeto, em Nome do projeto, digite aws-tests-sample-node-js. 4. Na seção Fonte, em Provedor de origem, escolha GitHub.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	5. Em Repositório, escolha Repositório público e cole a URL:. https://github.com/aws-samples/node-js-tests-sample 6. Na seção Ambiente, escolha Imagem gerenciada, Amazon Linux e a imagem mais recente. 7. Deixe as configurações padrão para todas as outras opções e, em seguida, escolha Criar projeto de compilação.	
Inicie a compilação.	Na página Revisão, escolha Iniciar compilação para executar a compilação.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Analise os testes de unidade

Tarefa	Descrição	Habilidades necessárias
Visualizar resultados do teste	No CodeBuild console, revise os resultados do teste de unidade do CodeBuild trabalho. Eles devem corresponder aos resultados mostrados na seção Informações adicionais. Esses resultados validam a integração do GitHub repositório com o. CodeBuild	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Aplique um webhook.	Agora você pode aplicar um webhook, para poder iniciar automaticamente uma compilação sempre que enviar alterações de código para a ramificação principal do seu repositório. Para obter instruções, consulte a CodeBuild documentação.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Recursos relacionados

- Exemplo de aplicativo de teste de unidade de jogo (GitHub repositório com código de amostra)
- CodeBuild Documentação da AWS
- GitHub eventos de webhook (CodeBuild documentação)
- Criando um novo repositório (GitHub documentação)

Mais informações

Resultados do teste de unidade

No CodeBuild console, você deve ver os seguintes resultados de teste após a criação bem-sucedida do projeto.

Exemplo de componentes de teste da unidade

Esta seção descreve os quatro tipos de componentes de teste usados em testes de unidade: asserções, espiões, stubs e simulações. Ela inclui uma breve explicação e um exemplo de código de cada componente.

Asserções

Uma asserção é usada para verificar um resultado esperado. Esse é um componente de teste importante porque valida a resposta esperada de uma determinada função. O exemplo de declaração a seguir valida que o ID retornado está entre 0 e 1000 ao inicializar um novo jogo.

```
const { expect }  = require('chai');
const { Game } = require('../src/index');

describe('Game Function Group', () => {
 it('Check that the Game ID is between 0 and 1000', function() {
      const game = new Game();
      expect(game.id).is.above(0).but.below(1000)
 });
});
```

Espiões

Um espião é usado para observar o que está acontecendo quando uma função está em execução. Por exemplo, convém validar se a função foi chamada corretamente. O exemplo a seguir mostra que os métodos iniciar e parar são chamados em um objeto da classe Jogo.

```
const { expect }  = require('chai');
const { spy } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () => {
   it('should verify that the correct function is called', () => {
      const spyStart = spy(Game.prototype, "start");
      const spyStop = spy(Game.prototype, "stop");

      const game = new Game();
      game.start();
      game.stop();

      expect(spyStart.called).to.be.true
      expect(spyStop.called).to.be.true
    });
});
```

Stub

Um stub é usado para substituir a resposta padrão de uma função. Isso é especialmente útil quando a função faz uma solicitação externa, porque você quer evitar fazer solicitações externas a partir de testes de unidade. (As solicitações externas são mais adequadas para testes de integração, que podem testar fisicamente as solicitações entre componentes diferentes.) No exemplo a seguir, um stub força um ID de retorno da função getId.

```
const { expect }  = require('chai');
const {.stub } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let generateIdStub = stub(Game.prototype, 'getId').returns(999999);

      const game = new Game();

      expect(game.getId).is.equal(999999);

      generateIdStub.restore();
    });
});
```

Simulações

Uma simulação é um método falso que tem um comportamento pré-programado para testar diferentes cenários. Uma simulação pode ser considerada uma forma estendida de um stub e pode realizar várias tarefas simultaneamente. No exemplo a seguir, uma simulação é usada para validar três cenários:

- Função é chamada
- Função é chamada com argumentos
- Função retorna o 9 inteiro

```
const { expect }  = require('chai');
const {.mock } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let mock = mock(Game.prototype).expects('getId').withArgs().returns(9);

      const game = new Game();
      const id = get.getId();
```

```
      mock.verify();
      expect(id).is.equal(9);
    });
});
```

Estruture um projeto Python em arquitetura hexagonal usando o AWS Lambda

Criado por Furkan Oruc (AWS), Dominik Goby (AWS), Darius Kunce (AWS) e Michal Ploski (AWS)

Resumo

Esse padrão mostra como estruturar um projeto Python em arquitetura hexagonal usando o AWS Lambda. O padrão usa o AWS Cloud Development Kit (AWS CDK) como ferramenta de infraestrutura como código (IaC), o Amazon API Gateway como API REST e o Amazon DynamoDB como camada de persistência. A arquitetura hexagonal segue os princípios de design orientados por domínio. Na arquitetura hexagonal, o software consiste em três componentes: domínio, portas e adaptadores. Para obter informações detalhadas sobre arquiteturas hexagonais e seus benefícios, consulte o guia Criação de arquiteturas hexagonais na AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Experiência em Python
- Familiaridade com AWS Lambda, AWS CDK, Amazon API Gateway e DynamoDB
- Uma GitHub conta (veja as instruções para se inscrever)
- Git (consulte as instruções de instalação)
- Um editor de código para fazer alterações e enviar seu código para GitHub (por exemplo, Visual Studio Code ou JetBrains PyCharm)
- Docker instalado e o daemon do Docker instalado e funcionando

Versões do produto

- Git versão 2.24.3 ou superior
- Python versão 3.7 ou superior
- AWS CDK v2
- Poetry versão 1.1.13 ou superior
- AWS Lambda Powertools para Python versão 1.25.6 ou superior
- pytest versão 7.1.1 ou superior

- Moto versão 3.1.9 ou superior
- pydantic versão 1.9.0 ou superior
- Boto3 versão 1.22.4 ou superior
- mypy-boto3-dynamodb versão 1.24.0 ou superior

Arquitetura

Pilha de tecnologias de destino

A pilha de tecnologia de destino consiste em um serviço em Python que usa o API Gateway, Lambda e DynamoDB. O serviço usa um adaptador do DynamoDB para manter os dados. Ele fornece uma função que usa o Lambda como ponto de entrada. O serviço usa o Amazon API Gateway para expor uma API REST. A API usa o AWS Identity and Access Management (IAM) para a autenticação de clientes.

Arquitetura de destino

Para ilustrar a implementação, esse padrão implanta uma arquitetura de destino com tecnologia sem servidor. Os clientes podem enviar solicitações para um endpoint do API Gateway. O API Gateway encaminha a solicitação para a função do Lambda de destino que implementa o padrão de arquitetura hexagonal. A função do Lambda executa operações de criação, leitura, atualização e exclusão (CRUD) em uma tabela do DynamoDB.

> **Important**
>
> Esse padrão foi testado em um ambiente PoC. Você deve realizar uma análise de segurança para identificar o modelo de ameaça e criar uma base de código segura antes de implantar qualquer arquitetura em um ambiente de produção.

A API oferece suporte a cinco operações em uma entidade de produto:

- `GET /products` devolve todos os produtos.
- `POST /products` cria um novo produto.
- `GET /products/{id}` retorna um produto específico.

- `PUT /products/{id}` atualiza um produto específico.
- `DELETE /products/{id}` exclui um produto específico.

Você pode usar a seguinte estrutura de pastas para organizar seu projeto de acordo com o padrão de arquitetura hexagonal:

```
app/  # application code
|--- adapters/  # implementation of the ports defined in the domain
     |--- tests/  # adapter unit tests
|--- entrypoints/  # primary adapters, entry points
     |--- api/  # api entry point
          |--- model/  # api model
          |--- tests/  # end to end api tests
|--- domain/  # domain to implement business logic using hexagonal architecture
     |--- command_handlers/  # handlers used to execute commands on the domain
     |--- commands/  # commands on the domain
     |--- events/  # events triggered via the domain
     |--- exceptions/  # exceptions defined on the domain
     |--- model/  # domain model
     |--- ports/  # abstractions used for external communication
     |--- tests/  # domain tests
|--- libraries/  # List of 3rd party libraries used by the Lambda function
infra/  # infrastructure code
simple-crud-app.py  # AWS CDK v2 app
```

Ferramentas

Serviços da AWS

- O Amazon API Gateway é um serviço totalmente gerenciado que facilita aos desenvolvedores criar, publicar, manter, monitorar e proteger APIs em qualquer escala.
- O Amazon DynamoDB é um banco de dados NoSQL totalmente gerenciado, de valor-chave e com tecnologia sem servidor, projetado para executar aplicativos de alto desempenho em qualquer escala.
- O AWS Lambda é um serviço computacional com tecnologia sem servidor e orientado a eventos que permite executar o código em virtualmente qualquer tipo de aplicação ou serviço de backend sem o provisionamento ou gerenciamento de servidores. Você pode iniciar funções do Lambda a partir de mais de 200 serviços da AWS e aplicativos de software como serviço (SaaS) e pagar somente pelo que usar.

Ferramentas

- O Git é usado como sistema de controle de versão para desenvolvimento de código nesse padrão.
- O Python é usado como linguagem de programação para esse padrão. O Python fornece estruturas de dados de alto nível e uma abordagem à programação orientada a objetos. O AWS Lambda fornece um runtime integrado do Python que simplifica a operação dos serviços do Python.
- O Visual Studio Code é usado como IDE para desenvolvimento e teste desse padrão. Você pode usar qualquer IDE que ofereça suporte ao desenvolvimento em Python (por exemplo, PyCharm).
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software de código aberto que permite definir recursos de aplicações em nuvem usando linguagens de programação conhecidas. Esse padrão usa o CDK para escrever e implantar a infraestrutura de nuvem como código.
- O Poetry é usado para gerenciar dependências no padrão.
- O Docker é usado pelo AWS CDK para criar o pacote e a camada do Lambda.

Código

O código desse padrão está disponível no repositório de amostras da arquitetura hexagonal GitHub Lambda.

Práticas recomendadas

Para usar esse padrão em um ambiente de produção, siga essas práticas recomendadas:

- Use chaves gerenciadas pelo cliente no AWS Key Management Service (AWS KMS) para criptografar grupos de log da Amazon e tabelas do CloudWatch Amazon DynamoDB.
- Configure o AWS WAF para o Amazon API Gateway para permitir acesso somente a partir da rede da sua organização.
- Considere outras opções para autorização do API Gateway se o IAM não atender às suas necessidades. Por exemplo, você pode usar grupos de usuários do Amazon Cognito ou autorizadores do Lambda do API Gateway.
- Use backups do DynamoDB.
- Configure as funções do Lambda com uma implantação de nuvem privada virtual (VPC) para manter o tráfego de rede dentro da nuvem.

- Atualize a configuração de origem permitida para o compartilhamento de recursos de origem cruzada (CORS) para restringir o acesso somente ao domínio de origem solicitante.
- Use cdk-nag para verificar as práticas recomendadas de segurança no código do AWS CDK.
- Considere o uso de ferramentas de digitalização de código para encontrar problemas de segurança comuns no código. Por exemplo, o Bandit é uma ferramenta projetada para encontrar problemas de segurança comuns no código Python. O PIP-Audit verifica os ambientes do Python em busca de pacotes que contenham tenham vulnerabilidades conhecidas.

Esse padrão usa o AWS X-Ray para rastrear solicitações por meio do ponto de entrada, domínio e adaptadores do aplicativo. O AWS X-Ray ajuda os desenvolvedores a identificar gargalos e determinar altas latências para melhorar o desempenho do aplicativo.

Épicos

Inicializar o projeto

Tarefa	Descrição	Habilidades necessárias
Crie seu próprio repositório.	1. Faça login em GitHub. 2. Crie um novo repositór io. Para obter instruçõe s, consulte a GitHub documentação. 3. Clone e envie o repositório de amostra desse padrão para o novo repositório em sua conta.	Desenvolvedor de aplicativos
Instale as dependências.	1. Instale o Poetry. `pip install poetry` 2. Instale pacotes do diretório raiz. O comando a seguir instala o aplicativo e os pacotes do AWS CDK. Ele também instala pacotes de	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	desenvolvimento necessários para a execução de testes de unidade. Todos os pacotes instalados são colocados em um novo ambiente virtual.
	`poetry install`
	3. Para visualizar uma representação gráfica dos pacotes instalados, execute o comando a seguir.
	`poetry show --tree`
	4. Atualizar todas as dependências.
	`poetry update`
	5. Abra um novo shell no ambiente virtual recém-criado. Ele contém todas as dependências instaladas.
	`poetry shell`	

Tarefa	Descrição	Habilidades necessárias
Configure seu IDE.	Recomendamos o Visual Studio Code, mas você pode usar qualquer IDE de sua escolha que ofereça suporte ao Python. As etapas a seguir são para o Visual Studio Code. 1. Atualize o arquivo `.vscode/settings` . `{ "python.testing.pytestArgs": [ "app/adapters/tests", "app/entrypoints/api/tests", "app/domain/tests" ], "python.testing.unittestEnabled": false, "python.testing.pytestEnabled": true, "python.envFile": "${workspaceFolder}/.env", }` 2. Crie um arquivo `.env` no diretório raiz do projeto. Isso garante que o diretório raiz do projeto seja incluído no `PYTHONPATH` para que `pytest` possa localizá-lo e	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	descobrir todos os pacotes adequadamente. `PYTHONPATH=.`	
Execute testes de unidade, opção 1: usando o Visual Studio Code.	1. Selecione o interpretador Python do ambiente virtual gerenciado pelo Poetry. 2. Execute testes no Test Explorer.	Desenvolvedor de aplicativos

Execute testes de unidade, opção 2: usando comandos shell.	1. Inicie um novo shell no ambiente virtual.
	`poetry shell`
	2. Execute o comando `pytest` no diretório raiz.
	`python -m pytest`
	Alternativamente, você pode executar o comando diretamente do Poetry.
	`poetry run python -m pytest`
		Desenvolvedor de aplicativos

Implante e teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Solicite credenciais temporárias.	Para obter credenciais da AWS no shell durante a execução do `cdk deploy`,	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	crie credenciais temporárias usando o Centro de Identidad e do AWS IAM (sucessor do AWS Single Sign-On). Para obter instruções, consulte a publicação Como recuperar credenciais de curto prazo para uso da CLI com o Centro de Identidade do AWS IAM.	

Implante o aplicativo .	1. Instale o AWS CDK v2.
	`npm install -g aws-cdk`
	Para obter mais informaçõ es, consulte a documenta ção do AWS CDK.
	2. Faça o bootstrap do AWS CDK na sua conta e região.
	`cdk bootstrap aws://12345678900/ us-east-1 --profile aws-profile-name`
	3. Implante o aplicativo como uma CloudFormation pilha da AWS usando um perfil da AWS.
	`cdk deploy --profile aws-profile-name`
		Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Teste a API, opção 1: usando o console.	Use o console do API Gateway para testar a API. Para obter mais informaçõ es sobre operações de API e mensagens de solicitação/ resposta, consulte a seção de uso da API do arquivo readme no repositório. GitHub	Desenvolvedor de aplicativos, AWS DevOps
Teste a API, opção 2: usando o Postman.	Se você quiser usar uma ferramenta como o Postman: 1. Instale o Postman como um aplicativo independente ou extensão do navegador. 2. Copie o URL do endpoint para o API Gateway. Ele estará no seguinte formato. `https://{api-id}.execute-api.{region}.amazonaws.com/{stage}/{path}` 3. Configure a assinatura da AWS na guia de autorizaç ão. Para obter instruções, consulte o artigo do AWS re:POST sobre a ativação da autenticação do IAM para o API Gateway REST. APIs 4. Use o Postman para enviar solicitações ao endpoint da API.	Desenvolvedor de aplicativos, AWS DevOps

Desenvolva o serviço

Tarefa	Descrição	Habilidades necessárias

Escreva testes de unidade para o domínio comercial.	1. Crie um arquivo Python na pasta `app/domain/tests` usando o prefixo do nome do arquivo `test_`.
	2. Crie um novo método de teste para testar a nova lógica de negócios usando o exemplo a seguir.
	
	`def test_create_product_should_store_in_repository():`
	`    # Arrange`
	`    command = create_product_command.CreateProductCommand(`
	`        name="Test Product",`
	`        description="Test Description",`
	`    )`
	`    # Act`
	`    create_product_command_handler.handle_create_product_command(`
	`        command=command, unit_of_work=mock_unit_of_work`
	`    )`
	`# Assert`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	3. Crie uma classe de comando na pasta `app/domain/commands` . 4. Caso seja uma funcionalidade nova, crie um stub para o manipulador de comandos na pasta `app/domain/command_handlers` . 5. Execute o teste de unidade para verificar se ela falha, porque ainda não há lógica de negócios. `python -m pytest`	

Tarefa	Descrição	Habilidades necessárias

Implemente comandos e manipuladores de comandos.	1. Implemente a lógica de negócios no arquivo manipulador de comandos recém-criado.
	2. Para cada dependência que interage com sistemas externos, declare uma classe abstrata na pasta `app/domain/ports` .
	`class ProductsRepository(ABC):`
	`  @abstractmethod`
	`  def add(self, product: product.Product) -> None:`
	`  ...`
	
	`class UnitOfWork(ABC):`
	`  products: ProductsRepository`
	
	`  @abstractmethod`
	`  def commit(self) -> None:`
	`  ...`
	
	`  @abstractmethod`
	`  def __enter__(self) -> typing.Any:`
	`  ...`
	
	`  @abstractmethod`
	`  def __exit__(self, *args) -> None:`
	`  ...`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	3. Atualize a assinatura do manipulador de comandos para aceitar as dependências recém-declaradas usando a classe de porta abstrata como anotação de tipo.
	
	`def handle_create_product_command(`
	`  command: create_product_command.CreateProductCommand,`
	`  unit_of_work: unit_of_work.UnitOfWork,`
	`) -> str:`
	`  ...`
	
	4. Atualize o teste de unidade para simular o comportamento de todas as dependências declaradas para o manipulador de comandos.
	
	`  # Arrange`
	`  mock_unit_of_work = unittest.mock.create_autospec(`
	`  spec=unit_of_work.UnitOfWork, instance=True`
	`  )`
	`  mock_unit_of_work.products = unittest.mock.create_autospec(`	

Tarefa	Descrição	Habilidades necessárias

	<pre>spec=unit
	_of_work.ProductsR
	epository, instance=
	True
	)</pre>
	5. Atualize a lógica de asserção no teste para verificar as invocações de dependência esperadas.
	<pre># Assert
	mock_unit
	_of_work.commit.as
	sert_called_once()
	product =
	mock_unit_of_work.
	products.add.call_
	args.args[0]
	
	assertpy.
	assert_that(produc
	t.name).is_equal_t
	o("Test Product")
	assertpy.
	assert_that(produc
	t.description).is_
	equal_to("Test
	Description")</pre>
	6. Execute o teste de unidade para verificar o sucesso.
	<pre>python -m pytest</pre>	

Tarefa	Descrição	Habilidades necessárias
Escreva testes de integração para adaptadores secundários.	1. Crie um arquivo de teste na pasta `app/adapters/tests` usando `test_` como prefixo do nome do arquivo. 2. Use a biblioteca Moto para simular os serviços da AWS. 3. Crie um novo método de teste para um teste de integração do adaptador.	Desenvolvedor de aplicativos

```
@pytest.fixture
def mock_dynamodb():
   with moto.mock
_dynamodb():
    yield boto3.res
ource("dynamodb",
 region_name="eu-ce
ntral-1")
```

```
def test_add_
and_commit_should_
store_product(mock
_dynamodb):
    # Arrange
    unit_of_work =
 dynamodb_unit_of_w
ork.DynamoDBUnitOf
Work(
        table_nam
e=TEST_TABLE_NAME,
 dynamodb_client=mo
ck_dynamodb.meta.c
lient
    )
    current_time =
 datetime.datetime.
```

Tarefa	Descrição	Habilidades necessárias

	now(datetime.timezone.utc).isoformat()
	
	    new_product_id = str(uuid.uuid4())
	    new_product = product.Product(
	        id=new_product_id,
	        name="test-name",
	        description="test-description",
	        createDate=current_time,
	        lastUpdateDate=current_time,
	    )
	
	    # Act
	    with unit_of_work:
	        unit_of_work.products.add(new_product)
	        unit_of_work.commit()
	
	    # Assert
	
	4. Crie uma classe de adaptador na pasta `app/adapters` . Use a classe abstrata da pasta ports como classe base.
	5. Execute o teste de unidade para verificar se ele falha, porque ainda não há lógica.	

Tarefa	Descrição	Habilidades necessárias
	`python -m pytest`	

Tarefa	Descrição	Habilidades necessárias

Implemente adaptadores secundários.	1. Implemente a lógica no arquivo do adaptador recém-criado.
	2. Atualize as afirmações do teste.
	
	`# Assert`
	`    with unit_of_work_readonly:`
	`        product_from_db = unit_of_work_readonly.products.get(new_product_id)`
	
	`    assertpy.assert_that(product_from_db).is_not_none()`
	`    assertpy.assert_that(product_from_db.dict()).is_equal_to(`
	`        {`
	`            "id": new_product_id,`
	`            "name": "test-name",`
	`            "description": "test-description",`
	`            "createDate": current_time,`
	`            "lastUpdateDate": current_time,`
	`        }`
	`    )`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	3. Execute o teste de unidade para verificar o sucesso. `python -m pytest`	

Tarefa	Descrição	Habilidades necessárias
Escreva end-to-end testes.	1. Crie um arquivo de teste na pasta `app/entry points/api/tests` usando `test_` como prefixo do nome do arquivo. 2. Crie uma configuração de contexto do Lambda que será usada pelo teste para chamar o Lambda. 3. Crie um método de teste para a invocação da API.	Desenvolvedor de aplicativos

```
@pytest.fixture
def lambda_co
ntext():
    @dataclass
    class LambdaCon
text:
        function_
name: str = "test"
        memory_li
mit_in_mb: int = 128
        invoked_f
unction_arn: str =
 "arn:aws:lambda:eu
-west-1:809313241:
function:test"
        aws_reque
st_id: str =
 "52fdfc07-2182-154
f-163f-5f0f9a621d7
2"

 return LambdaCon
text()
```

Tarefa	Descrição	Habilidades necessárias

	`def test_crea te_product(lambda_ context):`
	`    # Arrange`
	`    name = "TestName"`
	`    description =  "Test description"`
	`    request =  api_model.CreatePr oductRequest(name= name, descripti on=description)`
	
	`    minimal_event =  api_gateway_proxy_ event.APIGatewayPr oxyEvent(`
	`        {`
	`            "path": "/ products",`
	`            "httpMeth od": "POST",`
	`            "requestC ontext": {  #  correlation ID`
	
	`  "requestId":  "c6af9ac6-7b61-11e 6-9a41-93e8deadbee f"`
	`            },`
	`            "body":  json.dumps(request .dict()),`
	`        }`
	`    )`
	
	`    create_pr oduct_func_mock =  unittest.mock.crea te_autospec(`	

Tarefa	Descrição	Habilidades necessárias

	<pre>spec=crea
	te_product_command
	_handler.handle_cr
	eate_product_comma
	nd
	)
	handler.c
	reate_product_comm
	and_handler.handle
	_create_product_co
	mmand = (
	create_pr
	oduct_func_mock
	)
	
	# Act
	handler.h
	andler(minimal_eve
	nt, lambda_context)</pre>
	4. Execute o teste de unidade para verificar se ele falha, porque ainda não há lógica.
	<pre>python -m pytest</pre>	

Tarefa	Descrição	Habilidades necessárias

Implemente adaptadores primários.	1. Crie uma função para a lógica de negócios da API e declare-a como um recurso da API.
	
	`@tracer.capture_method`
	`@app.post("/products")`
	`@utils.parse_event(model=api_model.CreateProductRequest, app_context=app)`
	`def create_product(`
	`request: api_model.CreateProductRequest,`
	`) -> api_model.CreateProductResponse:`
	`"""Creates a product."""`
	`...`
	
	Note
	Todos os decoradores que você vê são recursos da biblioteca AWS Lambda Powertools for Python. Para obter detalhes, consulte o site Powertools do AWS Lambda para Python.
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	2. Implemente a lógica da API.
	
	`id=create_product_command_handler.handle_create_product_command(`
	`command=create_product_command.CreateProductCommand(`
	`name=request.name,`
	`description=request.description,`
	`),`
	`unit_of_work=unit_of_work,`
	`)`
	`response = api_model.CreateProductResponse(id=id)`
	`return response.dict()`
	
	3. Execute o teste de unidade para verificar o sucesso.
	
	`python -m pytest`	

Recursos relacionados

Guia do APG

- Criação de arquiteturas hexagonais na AWS

Referências da AWS

- Documentação do AWS Lambda
- Documentação do AWS CDK
  - Seu primeiro aplicativo AWS CDK
- Documentação do API Gateway
  - Controlar o acesso a uma API com permissões do IAM
  - Use o console do API Gateway para testar um método de API REST
- Documentação do Amazon DynamoDB

Ferramentas

- Site git-scm.com
- Como instalar o Git
- Criando um novo GitHub repositório
- Site em Python
- Powertools do AWS Lambda para Python
- Site do Postman
- Biblioteca de objetos simulados em Python
- Site do Poetry

IDEs

- Site do Visual Studio Code
- PyCharm site

Mais padrões

- Acesso Serviços da AWS a partir de um aplicativo ASP.NET Core usando grupos de identidade do Amazon Cognito
- Acesse aplicativos de contêineres de forma privada no Amazon ECS usando o AWS Fargate, a PrivateLink AWS e um Network Load Balancer
- Acesse aplicativos de contêineres de forma privada no Amazon ECS usando a AWS PrivateLink e um Network Load Balancer
- Associe um AWS CodeCommit repositório em um Conta da AWS com o Amazon SageMaker AI Studio Classic em outra conta
- Automatize a exclusão de AWS CloudFormation pilhas e recursos associados
- Restrinja o acesso com base no endereço IP ou geolocalização usando AWS WAF
- Crie uma arquitetura pouco acoplada com microsserviços usando DevOps práticas e o AWS Cloud9
- Crie um aplicativo móvel React Native de tecnologia sem servidor usando o AWS Amplify
- Crie e teste aplicativos iOS com AWS CodeCommit CodePipeline, AWS e AWS Device Farm
- Configure o registro em log para aplicativos.NET no Amazon CloudWatch Logs usando NLog
- Crie um pipeline e uma AMI usando CodePipeline um HashiCorp Packer
- Crie um pipeline e implante atualizações de artefatos em instâncias locais usando EC2 CodePipeline
- Crie uma definição de tarefa do Amazon ECS e monte um sistema de arquivos em EC2 instâncias usando o Amazon EFS
- Implemente um aplicativo baseado em gRPC em um cluster Amazon EKS e acesse-o com um Application Load Balancer
- Implemente uma ChatOps solução para gerenciar os resultados do escaneamento SAST usando o Amazon Q Developer em aplicativos de bate-papo, ações personalizadas e AWS CloudFormation
- Implante canários CloudWatch Synthetics usando o Terraform
- Implante microsserviços Java no Amazon ECS usando o AWS Fargate
- Implemente um caso de uso do RAG AWS usando o Terraform e o Amazon Bedrock
- Implante recursos em uma AWS Wavelength zona usando o Terraform
- Implemente o controle de versão de API baseado em caminhos usando domínios personalizados no Amazon API Gateway

- Migrar uma fila de mensagens do Microsoft Azure Service Bus para o Amazon SQS
- Migre uma aplicação .NET do Microsoft Azure App Service para o AWS Elastic Beanstalk
- Migrar um aplicativo web do Go on-premises para AWS Elastic Beanstalk usando o método binário
- Migrar um servidor SFTP local para usar AWSAWS Transfer for SFTP
- Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2
- Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2 com o Auto Scaling
- Migre da Oracle GlassFish para o AWS Elastic Beanstalk
- Migrar aplicações Java on-premises para a AWS usando o App2Container da AWS
- Migre OpenText TeamSite cargas de trabalho para a nuvem da AWS
- Migrar certificados SSL do Windows para um Application Load Balancer usando o ACM
- Modernize aplicativos ASP.NET Web Forms na AWS
- Monitore a atividade do aplicativo usando o CloudWatch Logs Insights
- Execute um contêiner Docker da API web ASP.NET Core em uma instância Amazon Linux EC2
- Ofereça conteúdo estático em um bucket do Amazon S3 por meio de uma VPC usando a Amazon CloudFront
- Configure uma PeopleSoft arquitetura altamente disponível na AWS
- Simplifique o desenvolvimento e a implantação de bots do Amazon Lex usando um fluxo de trabalho automatizado
- Solucione problemas de estados AWS Step Functions usando o Amazon Bedrock
- Use o Network Firewall para capturar os nomes de domínio DNS da Indicação de Nome do Servidor para tráfego de saída
- Visualize os resultados do modelo de IA/ML usando o Flask e o AWS Elastic Beanstalk

IoT

Tópicos

- Configure o registro e o monitoramento de eventos de segurança em seu AWS IoT ambiente
- Extraia e consulte atributos de AWS IoT SiteWise metadados em um data lake
- Configure e solucione problemas do AWS IoT Greengrass com dispositivos clientes
- Mais padrões

Configure o registro e o monitoramento de eventos de segurança em seu AWS IoT ambiente

Criado por Prateek Prakash (AWS)

Resumo

Garantir que seus ambientes de Internet das Coisas (IoT) estejam seguros é uma prioridade importante, principalmente porque as organizações estão conectando bilhões de dispositivos aos seus ambientes de TI. Esse padrão fornece uma arquitetura de referência que você pode usar para implementar o registro e o monitoramento de eventos de segurança em seu ambiente de IoT no. Nuvem AWS Normalmente, um ambiente de IoT no Nuvem AWS tem as três camadas a seguir:

- Dispositivos de IoT que geram dados de telemetria relevantes.
- AWS IoT serviços (por exemplo,, AWS IoT CoreAWS IoT Device Management, ou AWS IoT Device Defender) que conectam seus dispositivos de IoT a outros dispositivos e. Serviços da AWS
- Back-end Serviços da AWS que ajuda a processar dados de telemetria e fornece informações úteis para seus diferentes casos de uso comercial.

As melhores práticas fornecidas pelo whitepaper AWS IoT Lens - AWS Well-Architected Framework podem ajudar você a analisar e melhorar sua arquitetura baseada em nuvem e a entender melhor o impacto comercial de suas decisões de design. Uma recomendação importante é que você analise os registros e métricas do aplicativo em seus dispositivos e no Nuvem AWS. Você pode conseguir isso aproveitando diferentes abordagens e técnicas (por exemplo, modelagem de ameaças) para identificar métricas e eventos que devem ser monitorados para detectar possíveis problemas de segurança.

Esse padrão descreve como usar AWS IoT serviços de segurança para projetar e implementar uma arquitetura de referência de monitoramento e registro de segurança para um ambiente de IoT no. Nuvem AWS Essa arquitetura se baseia nas melhores práticas AWS de segurança existentes e as aplica ao seu ambiente de IoT.

Pré-requisitos e limitações

Pré-requisitos

- Um ambiente de zona de pouso existente. Para obter mais informações sobre isso, consulte o guia Configurando um AWS ambiente seguro e escalável com várias contas no site de Orientação AWS Prescritiva.
- As seguintes contas devem estar disponíveis em sua zona de pouso:
  - Conta do Log Archive — Essa conta é para usuários que precisam acessar as informações de registro das contas nas unidades organizacionais da sua zona de destino (OUs). Para obter mais informações sobre isso, consulte a seção da conta Security OU — Log Archive do guia Arquitetura de referência de AWS segurança no site de orientação AWS prescritiva.
  - Conta de segurança: suas equipes de segurança e conformidade usam essa conta para auditoria ou para realizar operações de segurança de emergência. Essa conta também é designada como a conta de administrador da Amazon GuardDuty. Os usuários da conta de administrador podem configurar GuardDuty, além de visualizar e gerenciar GuardDuty as descobertas de sua própria conta e de todas as contas dos membros. Para obter mais informações sobre isso, consulte Gerenciamento de várias contas GuardDuty na GuardDuty documentação.
  - Conta de IoT: essa conta é para seu ambiente de IoT.

Arquitetura

Esse padrão estende a solução de registro centralizado da Biblioteca de AWS soluções para coletar e processar eventos de IoT relacionados à segurança. A solução de registro centralizado é implantada na conta de segurança e ajuda a coletar, analisar e exibir CloudWatch os registros da Amazon em um único painel. Essa solução consolida, gerencia e analisa arquivos de log de várias fontes. Por fim, a solução de registro centralizado também usa o Amazon OpenSearch Service e os OpenSearch painéis para mostrar uma visão unificada de todos os eventos de log.

O diagrama de arquitetura a seguir mostra os principais componentes de um registro de segurança de IoT e uma arquitetura de referência no. Nuvem AWS

O diagrama mostra o seguinte fluxo de trabalho:

1. As coisas da IoT são os dispositivos que devem ser monitorados em busca de eventos de segurança anômalos. Esses dispositivos executam um agente para publicar eventos ou métricas de segurança em AWS IoT Core AWS IoT Device Defender e.

2. Quando o AWS IoT registro está ativado, AWS IoT envia eventos de progresso sobre cada mensagem à medida que ela passa de seus dispositivos por meio do agente de mensagens e do mecanismo de regras para o Amazon CloudWatch Logs. Você pode usar CloudWatch as assinaturas do Logs para enviar eventos para uma solução de registro centralizado. Para obter mais informações sobre isso, consulte AWS IoT métricas e dimensões na AWS IoT Core documentação.
3. AWS IoT Device Defender ajuda a monitorar configurações e métricas de segurança inseguras para seus dispositivos de IoT. Quando uma anomalia é detectada, os alarmes notificam o Amazon Simple Notification Service (Amazon SNS), que tem AWS Lambda a função de assinante. A função Lambda envia o alarme como uma mensagem para CloudWatch o Logs. Você pode usar assinaturas de CloudWatch registros para enviar eventos para sua solução de registro centralizado. Para obter mais informações sobre isso, consulte Verificações de auditoria, Carregar registros do lado do dispositivo e Configurar o AWS IoT registro na documentação. CloudWatch AWS IoT Core
4. AWS CloudTrail registra as ações do plano de AWS IoT Core controle que fazem alterações (por exemplo, criar, atualizar ou anexar APIs). Quando CloudTrail configurado como parte da implementação de uma landing zone, ele envia eventos para o CloudWatch Logs. Você pode usar assinaturas para enviar eventos para sua solução de registro centralizado.
5. AWS Config regras gerenciadas ou regras personalizadas avaliam os recursos que fazem parte do seu ambiente de IoT. Monitore suas notificações de alteração de conformidade usando CloudWatch Eventos com CloudWatch registros como alvo. Depois que as notificações de alteração de conformidade forem enviadas ao CloudWatch Logs, você poderá usar assinaturas para enviar eventos para sua solução de registro centralizado.
6. A Amazon analisa GuardDuty continuamente os eventos CloudTrail de gerenciamento e ajuda a identificar chamadas de API feitas para AWS IoT Core endpoints a partir de endereços IP maliciosos conhecidos, geolocalizações incomuns ou proxies anônimos. Monitore GuardDuty as notificações usando CloudWatch Eventos com grupos de CloudWatch registros no Logs como destino. Quando GuardDuty as notificações são enviadas para o CloudWatch Logs, você pode usar assinaturas para enviar eventos para sua solução de monitoramento centralizado ou usar o GuardDuty console em sua conta de segurança para visualizar as notificações.
7. AWS Security Hub monitora sua conta de IoT usando as melhores práticas de segurança. Monitore as notificações do Security Hub usando CloudWatch Eventos com grupos de CloudWatch registros em Logs como destino. Quando as notificações do Security Hub são enviadas para o CloudWatch Logs, use assinaturas para enviar eventos para sua solução de

monitoramento centralizado ou use o console do Security Hub em sua conta de segurança para visualizar as notificações.

8. O Amazon Detective avalia e analisa informações para isolar a causa raiz e tomar medidas com base nas descobertas de segurança de chamadas incomuns para AWS IoT endpoints ou outros serviços em sua arquitetura de IoT.
9. O Amazon Athena consulta os logs armazenados em sua conta do Log Archive para melhorar sua compreensão das descobertas de segurança e identificar tendências e atividades maliciosas.

Ferramentas

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon Simple Storage Service (Amazon S3) usando SQL padrão.
- AWS CloudTrailajuda você a viabilizar a governança, a conformidade e a auditoria operacional e de risco do seu Conta da AWS.
- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. Você pode usar CloudWatch para coletar e monitorar métricas, que são variáveis que você pode medir para seus recursos e aplicativos.
- O Amazon CloudWatch Logs centraliza os registros de todos os seus sistemas, aplicativos e os Serviços da AWS que você usa. Você pode visualizar e monitorar os logs em busca de códigos de erro ou padrões específicos, filtrá-los com base em campos específicos ou arquivá-los com segurança para análise futura.
- AWS Configfornece uma visão detalhada da configuração dos AWS recursos em seu Conta da AWS.
- O Amazon Detective torna fácil analisar, investigar e identificar rapidamente a causa raiz de descobertas de segurança ou atividades suspeitas.
- AWS Glueé um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado que torna simples e econômico categorizar seus dados, limpá-los, enriquecê-los e movê-los de forma confiável entre vários armazenamentos de dados e fluxos de dados.
- A Amazon GuardDuty é um serviço contínuo de monitoramento de segurança.
- AWS IoT Corefornece comunicação segura e bidirecional para dispositivos conectados à Internet (como sensores, atuadores, dispositivos incorporados, dispositivos sem fio e dispositivos inteligentes) para conexão via MQTT, Nuvem AWS HTTPS e WAN. LoRa

- O AWS IoT Device Defender é um serviço de segurança que permite auditar a configuração de seus dispositivos, monitorar dispositivos conectados para detectar comportamentos anormais e reduzir os riscos à segurança.
- O Amazon OpenSearch Service é um serviço gerenciado que facilita a implantação, a operação e a escalabilidade de OpenSearch clusters no Nuvem AWS.
- AWS Organizationsé um serviço de gerenciamento de contas que permite consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança AWS e ajuda você a verificar seu ambiente de acordo com os padrões e as melhores práticas do setor de segurança.
- A Amazon Virtual Private Cloud (Amazon VPC) provisiona uma seção logicamente isolada da Nuvem AWS qual você pode lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu data center, com os benefícios de usar a infraestrutura dimensionável da AWS.

Épicos

Configure uma conta de IoT em seu ambiente de zona de pouso

Tarefa	Descrição	Habilidades necessárias
Valide as barreiras de proteção da segurança na conta de IoT.	Valide se as grades de proteção de CloudTrail, AWS Config GuardDuty, e do Security Hub estão habilitadas em sua conta de IoT.	Administrador da AWS
Validar se sua conta de IoT está configurada como uma conta membro da sua conta de segurança.	Valide se sua conta de IoT está configurada e associada como conta GuardDuty membro e Security Hub em sua conta de segurança. Para obter mais informaçõ es sobre isso, consulte Gerenciando GuardDuty contas AWS Organizations	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	na GuardDuty documentação e Gerenciando contas de administrador e membro na documentação do Security Hub.	
Validar o arquivamento de logs.	Valide isso CloudTrail AWS Config, e os registros de fluxo da VPC serão armazenados na conta do Log Archive.	Administrador da AWS

Configurar a solução de registro em log centralizado

Tarefa	Descrição	Habilidades necessárias
Configurar a solução de registro em log centralizado em sua conta de segurança.	Faça login na sua conta AWS Management Console de segurança e configure a solução de registro centralizado da Biblioteca de AWS soluções para coletar, analisar e exibir CloudWatch registros no Amazon OpenSearch Service and OpenSearch Dashboards. Para obter mais informações sobre isso, consulte Coletar, analisar e exibir Amazon CloudWatch Logs em um único painel com a solução de registro centralizado do guia de implementação do registro centralizado na Biblioteca de AWS soluções.	Administrador da AWS

Configurar e configurar AWS recursos em sua conta de IoT

Tarefa	Descrição	Habilidades necessárias
Configure o AWS IoT registro.	Faça login no AWS Management Console para sua conta de IoT. Configure e configure AWS IoT Core para enviar registros para o CloudWatch Logs. Para obter mais informaçõ es sobre isso, consulte Configurar AWS IoT registros e Monitorar AWS IoT usando CloudWatch registros na AWS IoT Core documentação.	Administrador da AWS
Configurar AWS IoT Device Defender.	Configure AWS IoT Device Defender para auditar seus recursos de IoT e detectar anomalias. Para obter mais informações sobre isso, consulte Introduçã o AWS IoT Device Defender na AWS IoT Core documenta ção.	Administrador da AWS
Configurar CloudTrail.	Configure CloudTrail para enviar eventos para o CloudWatch Logs. Para obter mais informaçõ es sobre isso, consulte Envio de eventos para CloudWatc h registros na CloudTrail documentação.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Configuração AWS Config e AWS Config regras.	Configuração AWS Config e as AWS Config regras necessárias. Para obter mais informações sobre isso, consulte Configuração AWS Config com o console e Adição de AWS Config regras na AWS Config documentação.	Administrador da AWS
Configurar GuardDuty.	Configure e configure GuardDuty para enviar descobertas para a Amazon CloudWatch Events com grupos de CloudWatch registros em Logs como destino. Para obter mais informações sobre isso, consulte Criação de respostas personalizadas às GuardDuty descobertas com o Amazon CloudWatch Events na GuardDuty documentação.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Configurar o Security Hub.	Configure o Security Hub e habilite os padrões CIS AWS Foundations Benchmark e AWS Foundational Security Best Practices. Para obter mais informações sobre isso, consulte Resposta e remediação automatizadas na documentação do Security Hub.	Administrador da AWS
Configurar o Amazon Detective.	Configure o Detective para facilitar a análise das descobertas de segurança. Para obter mais informações sobre isso, consulte Introdução ao Amazon Detective na documentação do Amazon Detective.	Administrador da AWS
Configure o Amazon Athena e. AWS Glue	Configure o Athena e consulte AWS Glue os AWS service (Serviço da AWS) registros que conduzem investigações de incidentes de segurança. Para obter mais informaçõ es sobre isso, consulte Como consultar AWS service (Serviço da AWS) registros na documentação do Amazon Athena.	Administrador da AWS

Recursos relacionados

- O que é uma zona de pouso?

Extraia e consulte atributos de AWS IoT SiteWise metadados em um data lake

Criado por Ambarish Dongaonkar (AWS)

Resumo

AWS IoT SiteWise usa modelos e hierarquias de ativos para representar seus equipamentos, processos e instalações industriais. Cada modelo ou ativo pode ter vários atributos específicos do seu ambiente. Exemplos de atributos de metadados incluem o local ou a localização física do ativo, detalhes da planta e identificadores do equipamento. Esses valores de atributos complementam os dados de medição de ativos para maximizar o valor comercial. O machine learning (ML) pode fornecer informações adicionais sobre esses metadados e simplificar as tarefas de engenharia.

No entanto, os atributos de metadados não podem ser consultados diretamente do AWS IoT SiteWise serviço. Para tornar os atributos consultáveis, você deve extraí-los e ingeri-los em um data lake. Esse padrão usa um script Python para extrair os atributos de todos os AWS IoT SiteWise ativos e ingeri-los em um data lake em um bucket do Amazon Simple Storage Service (Amazon S3). Ao concluir esse processo, você pode usar consultas SQL no Amazon Athena para acessar AWS IoT SiteWise os atributos de metadados e outros conjuntos de dados, como conjuntos de dados de medição. As informações do atributo de metadados também são úteis ao trabalhar com AWS IoT SiteWise monitores ou painéis. Você também pode criar um QuickSight painel da Amazon usando os atributos extraídos no bucket do Amazon S3.

O padrão tem código de referência, e você pode implementar o código usando os melhores serviços de computação para seu caso de uso, como AWS Lambda ou AWS Glue.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Permissões para configurar AWS Lambda funções ou AWS Glue trabalhos.
- Um bucket do Amazon S3.
- Os modelos e hierarquias de ativos são configurados em. AWS IoT SiteWise Para obter mais informações, consulte Criação de modelos de ativos na AWS IoT SiteWise documentação.

Arquitetura

Você pode usar uma função Lambda ou um AWS Glue trabalho para concluir esse processo. Recomendamos usar o Lambda se você tiver menos de 100 modelos e cada modelo tiver uma média de 15 ou menos atributos. Para todos os outros casos de uso, recomendamos usar AWS Glue.

A arquitetura da solução e o fluxo de trabalho são mostrados no diagrama a seguir.

1. O AWS Glue trabalho agendado ou a função Lambda é executada. Ele extrai os atributos de metadados do ativo AWS IoT SiteWise e os ingere em um bucket do Amazon S3.
2. Um AWS Glue rastreador rastreia os dados extraídos no bucket do Amazon S3 e cria tabelas em um. AWS Glue Data Catalog
3. Usando SQL padrão, o Amazon Athena consulta as tabelas no. AWS Glue Data Catalog

Automação e escala

Você pode programar a função ou o AWS Glue trabalho do Lambda para execução diária ou semanal, de acordo com a frequência de atualização das configurações de seus AWS IoT SiteWise ativos.

Não há limite para o número de AWS IoT SiteWise ativos que o código de amostra pode processar, mas um grande número de ativos pode aumentar o tempo necessário para concluir o processo.

Ferramentas

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão.
- AWS Glueé um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS IoT SiteWiseajuda você a coletar, modelar, analisar e visualizar dados de equipamentos industriais em grande escala.

- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS

Épicos

Configurar o trabalho ou a função

Tarefa	Descrição	Habilidades necessárias
Configurar permissões do IAM.	No console do IAM, conceda permissões à função do IAM assumida pela função ou AWS Glue trabalho do Lambda para fazer o seguinte: • Leia do AWS IoT SiteWise serviço • Grave no bucket do Amazon S3 Para obter mais informaçõ es, consulte Criação de uma função para um AWS service (Serviço da AWS) na documentação do IAM.	AWS geral
Crie a função ou AWS Glue o trabalho do Lambda.	Se você estiver usando o Lambda, crie uma nova função do Lambda. Em	AWS geral

Tarefa	Descrição	Habilidades necessárias
	Runtime, selecione Python. Para obter mais informações, consulte Como criar funções do Lambda com Python na documentação do Lambda. Se você estiver usando AWS Glue, crie um novo trabalho de shell do Python no AWS Glue console. Para obter mais informações, consulte Adicionar trabalhos de shell do Python na AWS Glue documentação.	
Atualize a função ou AWS Glue o trabalho do Lambda.	Modifique a nova função ou AWS Glue tarefa do Lambda e insira o exemplo de código na seção Informações adicionais. Modifique o código conforme necessário para seu caso de uso. Para obter mais informações, consulte Editar código usando o editor do console na documentação do Lambda e consulte Trabalho com scripts na AWS Glue documentação.	AWS geral

Executar o trabalho ou função

Tarefa	Descrição	Habilidades necessárias
Execute a função ou AWS Glue o trabalho do Lambda.	Execute a função ou AWS Glue o trabalho do Lambda.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es, consulte Invocar a função Lambda na documentação do Lambda ou consulte Iniciar trabalhos usando acionador es na documentação. AWS Glue Isso extrai os atributos de metadados dos ativos e modelos na AWS IoT SiteWise hierarquia e os armazena no bucket do Amazon S3 especificado.	
Configure um AWS Glue rastreador.	Configure um AWS Glue rastreador com o classificador de formato necessário para um arquivo no formato CSV. Use os detalhes do bucket e do prefixo do Amazon S3 usados na função ou no trabalho do Lambda. AWS Glue Para obter mais informações, consulte Definição de rastreadores na AWS Glue documentação.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Execute o AWS Glue rastreador.	Execute o rastreador para processar o arquivo de dados criado pela função ou trabalho do Lambda. AWS Glue O rastreador cria uma tabela no especificado. AWS Glue Data Catalog Para obter mais informações, consulte Iniciando rastreadores usando gatilhos na documentação. AWS Glue	AWS geral
Consulte os atributos dos metadados.	Usando o Amazon Athena, use o SQL padrão para consultá-los AWS Glue Data Catalog conforme necessári o para seu caso de uso. Você pode unir a tabela de atributos de metadados com outros bancos de dados e tabelas. Para obter mais informações, consulte Conceitos básicos na documentação do Amazon Athena.	AWS geral

Recursos relacionados

- Documentação do Amazon Athena
- AWS Glue documentação
- AWS IoT SiteWise Referência de API
- AWS IoT SiteWise guia do usuário
  - Conceitos básicos
  - Modelagem de ativos industriais

  - Como definir relacionamentos entre modelos de ativos (hierarquias)
  - Associar e desassociar ativos
  - Criando a AWS IoT SiteWise demonstração
- IOTSiteWise (documentação do SDK para Python)
- Documentação do Lambda

Mais informações

Código

O código de amostra fornecido é para referência, e você pode personalizar esse código conforme necessário para seu caso de uso.

```
# Following code can be used in an AWS Lambda function or in an AWS Glue Python shell
 job.
# IAM roles used for this job need read access to the AWS IoT SiteWise service and
 write access to the S3 bucket.
sw_client = boto3.client('iotsitewise')
s3_client = boto3.client('s3')
output = io.StringIO()

attribute_list=[]
bucket = '{3_bucket name}'
prefix = '{s3_bucket prefix}'
output.write("model_id,model_name,asset_id,asset_name,attribuet_id,attribute_name,attribute_val
\n")

m_resp = sw_client.list_asset_models()
for m_rec in m_resp['assetModelSummaries']:
     model_id = m_rec['id']
     model_name = m_rec['name']

     attribute_list.clear()
     dam_response = sw_client.describe_asset_model(assetModelId=model_id)
     for rec in dam_response['assetModelProperties']:
         if 'attribute' in rec['type']:
            attribute_list.append(rec['name'])

     response = sw_client.list_assets(assetModelId=model_id, filter='ALL')
     for asset in response['assetSummaries']:
```

```
         asset_id = asset['id']
         asset_name = asset['name']
         resp = sw_client.describe_asset(assetId=asset_id)
         for rec in resp['assetProperties']:
            if rec['name'] in attribute_list:
                p_resp = sw_client.get_asset_property_value(assetId=asset_id,
 propertyId=rec['id'])
                if 'propertyValue' in p_resp:
                    if p_resp['propertyValue']['value']:
                        if 'stringValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['stringValue']) + "\n")

                        if 'doubleValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['doubleValue']) + "\n")
                        if 'integerValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['integerValue']) + "\n")
                         if 'booleanValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['booleanValue']) + "\n")

output.seek(0)
s3_client.put_object(Bucket=bucket, Key= prefix + '/data.csv', Body=output.getvalue())
output.close()
```

Configure e solucione problemas do AWS IoT Greengrass com dispositivos clientes

Criado por Marouane Sefiani e Akalanka De Silva (AWS)

Resumo

O AWS IoT Greengrass é um serviço de nuvem e runtime de borda de código aberto para criar, implantar e gerenciar software de Internet das Coisas (IoT) em dispositivos periféricos. Os casos de uso do AWS IoT Greengrass incluem:

- Casas inteligentes em que um gateway do AWS IoT Greengrass é usado como um hub para automação residencial
- Fábricas inteligentes nas quais o AWS IoT Greengrass pode facilitar a ingestão e o processamento local de dados do chão de fábrica

O AWS IoT Greengrass pode atuar como um endpoint de conexão MQTT seguro e autenticado para outros dispositivos de borda (também conhecidos como dispositivos clientes) que, de outra forma, normalmente se conectariam diretamente ao AWS IoT Core. Esse recurso é útil quando os dispositivos do cliente não têm acesso direto à rede ao endpoint do AWS IoT Core.

Você pode configurar o AWS IoT Greengrass para uso com dispositivos clientes nos seguintes casos de uso:

- Para dispositivos clientes enviarem dados para o AWS IoT Greengrass
- Para que o AWS IoT Greengrass encaminhe dados para o AWS IoT Core
- Para aproveitar os recursos avançados do mecanismo de regras do AWS IoT Core

Esses recursos exigem a instalação e a configuração dos seguintes componentes no dispositivo AWS IoT Greengrass:

- Operador MQTT
- Ponte MQTT
- Autenticação do dispositivo cliente
- Detector IP

Além disso, as mensagens publicadas pelos dispositivos clientes devem estar no formato JSON ou no formato Protocol Buffers (protobuf).

Esse padrão descreve como instalar e configurar esses componentes necessários e fornece dicas de solução de problemas e práticas recomendadas.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) versão 2
- Dois dispositivos clientes executando o Python 3.7 ou superior
- Um dispositivo principal executando o Ambiente de Execução Java (JRE) versão 8 ou superior e o Amazon Corretto 11 ou OpenJDK 11

Limitações

- Você deve escolher uma região da AWS onde o AWS IoT Core esteja disponível. Para ver a lista atual de regiões do AWS IoT Core, consulte Serviços da AWS por região.
- O dispositivo principal deve ter pelo menos 172 MB de RAM e 512 MB de espaço em disco.

Arquitetura

O diagrama a seguir mostra a arquitetura da solução desse padrão.

A arquitetura inclui:

- Dois dispositivos clientes. Cada dispositivo contém uma chave privada, um certificado de dispositivo e um certificado de autoridade de certificação (CA - certificate authority) raiz. O AWS IoT Device SDK, que contém um cliente MQTT, também é instalado em cada dispositivo cliente.
- Um dispositivo principal que tem o AWS IoT Greengrass implantado com os seguintes componentes:
  - Operador MQTT
  - Ponte MQTT

- Autenticação do dispositivo cliente
- Detector IP

Essa arquitetura oferece suporte aos seguintes cenários:

- Os dispositivos clientes podem usar seu cliente MQTT para se comunicarem uns com os outros por meio do agente MQTT do dispositivo principal.
- Os dispositivos clientes também podem se comunicar com o AWS IoT Core na nuvem por meio do agente MQTT do dispositivo principal e da ponte MQTT.
- O AWS IoT Core na nuvem pode enviar mensagens para dispositivos clientes por meio do cliente de teste MQTT e da ponte MQTT e do agente MQTT do dispositivo principal.

Para obter mais informações sobre as comunicações entre dispositivos cliente e o dispositivo principal, consulte a seção Informações adicionais.

Ferramentas

Serviços da AWS

- O AWS IoT Greengrass é um serviço de nuvem e de runtime de borda e de Internet das coisas (IoT) que ajuda você a criar, implantar e gerenciar aplicativos de IoT em seus dispositivos.
- O AWS IoT Core fornece comunicação segura e bidirecional para dispositivos conectados à Internet se conectarem à Nuvem AWS.
- O SDK de dispositivo da AWS IoT é um kit de desenvolvimento de software que inclui bibliotecas de código aberto, guias de desenvolvedor com amostras e guias de portabilidade para que você possa criar produtos ou soluções inovadoras da IoT nas plataformas de hardware de sua preferência.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

Práticas recomendadas

- A carga útil das mensagens dos dispositivos do cliente deve estar no formato JSON ou Protobuf para aproveitar os recursos avançados do mecanismo de regras do AWS IoT Core, como transformação e ações condicionais.

- Configure a ponte MQTT para permitir a comunicação bidirecional.
- Configure e implante o componente detector de IP no AWS IoT Greengrass para garantir que os endereços IP do dispositivo principal sejam incluídos no campo de nome alternativo do assunto (SAN) do certificado do agente MQTT.

Épicos

Configure um dispositivo de núcleo

Tarefa	Descrição	Habilidades necessárias
Configure o AWS IoT Greengrass em seu dispositivo principal.	Instale o software AWS IoT Greengrass Core seguindo as instruções no guia do desenvolvedor.	AWS IoT Greengrass

Verifique o status da sua instalação.	Use o seguinte comando para conferir o estado do AWS IoT Greengrass no seu dispositivo principal:
	`sudo systemctl status greengrass.service`
	A saída esperada do comando é:
	`Launched Nucleus successfully`
		AWS geral

Configure uma política do IAM e a anexe ao perfil de serviço do Greengrass.	1. Crie uma política do IAM para permitir comunicações de e para a ponte MQTT. Veja a seguir um exemplo de política do: `{`	AWS geral

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	"Version":
	"2012-10-17",
	"Statement": [
	
	{
	"Effect":
	"Allow",
	"Action":
	[
	
	"iot:*"
	],
	"Resource
	": "*"
	},
	{
	"Sid":
	"GreengrassActions
	",
	"Effect":
	"Allow",
	"Action":
	[
	
	"greengrass:*"
	],
	"Resource
	": "*"
	}
	]
	}</pre>	

	2. Anexe a política ao perfil de serviço do Greengrass. Para obter o perfil de serviço, use o comando:
	
	<pre>aws greengrassv2
	get-service-role-f</pre>	

Tarefa	Descrição	Habilidades necessárias
	`or-account --region <region>` onde `<region>` se refere à sua região da AWS.	
Configure e implante os componentes necessários no dispositivo principal do AWS IoT Greengrass.	Configure e implante os seguintes componentes: • `greengrass.clientdevices.mqtt.Moquette` (veja os detalhes da configuração) • `greengrass.clientdevices.mqtt.Bridge` (veja os detalhes da configuração e a próxima tarefa) • `greengrass.clientdevices.Auth` (veja os detalhes da configuração e a tarefa após a próxima) • `aws.greengrass.clientdevices.IPDetector` (veja os detalhes da configuração)	AWS IoT Greengrass

Tarefa	Descrição	Habilidades necessárias
Confirme se a ponte MQTT permite comunicação bidirecional.	Para retransmitir mensagens MQTT entre dispositivos clientes e o AWS IoT Core, configure e implante o componente de ponte MQTT e especifique os tópicos a serem retransmitidos. Veja um exemplo abaixo: `{ "mqttTopicMapping": { "ClientDevicesToCloud": { "topic": "dt/#", "source": "LocalMqtt", "target": "IotCore" }, "CloudToClientDevices": { "topic": "cmd/#", "source": "IotCore", "target": "LocalMqtt" } } }`	AWS IoT Greengrass

Tarefa	Descrição	Habilidades necessárias
Confirme se o componente de autenticação permite que os dispositivos cliente se conectem e publiquem ou assinem tópicos.	A `aws.greengrass.clientdevices.Auth` configuração a seguir permite que todos os dispositivos cliente se conectem, publiquem mensagens e assinem todos os tópicos. `{ "deviceGroups": { "formatVersion": "2021-03-05", "definitions": { "MyPermissiveDeviceGroup": { "selectionRule": "thingName: *", "policyName": "MyPermissivePolicy" } }, "policies": { "MyPermissivePolicy": { "AllowAll": { "statementDescription": "Allow client devices to perform all actions.", "operations": ["*"], "resources": ["*"] } }`	AWS IoT Greengrass

Tarefa	Descrição	Habilidades necessárias
	<pre> } } }</pre>	

Configurar dispositivos cliente

Tarefa	Descrição	Habilidades necessárias
Instale o SDK de dispositivos do AWS IoT.	Instale o AWS IoT Device SDK nos dispositivos do cliente. Para obter uma lista completa das linguagens suportadas e das associadas SDKs, consulte a documenta ção do AWS IoT Core. Por exemplo, o SDK do AWS IoT Device para Python está localizado em. GitHub Para instalar esse SDK: 1. Confirme se o Python 3.7 ou posterior está instalado , conforme as instruções na página de pré-requisitos do repositório. GitHub 2. Use o comando pip para instalar o SDK. Para macOS e Linux: <pre>python3 -m pip install awsiotsdk</pre> Para Windows:	AWS IoT Geral

Tarefa	Descrição	Habilidades necessárias

	`python -m pip install awsiotsdk`
	
	Como alternativa, você pode instalar o SDK do repositório de origem:
	
	`# Create a workspace directory to hold all the SDK files`
	`mkdir sdk-workspace`
	`cd sdk-workspace`
	`# Clone the repository`
	`git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git`
	`# Install using Pip (use 'python' instead of 'python3' on Windows)`
	`python3 -m pip install ./aws-iot-device-sdk-python-v2`	

Tarefa	Descrição	Habilidades necessárias
Crie uma coisa.	1. No console do AWS IoT, se um botão Começar for exibido, selecione-o. Caso contrário, no painel de navegação, escolha Segurança, Políticas. 2. Se a caixa de diálogo Você ainda não tem políticas , selecione Criar uma política. Caso contrário, escolha Criar. 3. Insira um nome para a política do AWS IoT (por exemplo, `ClientDevicePolicy`). 4. Na seção Adicionar instruções, substitua a política existente pelo código JSON a seguir. Substitua `<region>` e `<account>` por sua região da AWS e número da conta da AWS. `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "iot:Connect", "Resource": "arn:aws:iot:region:account:client/*" },`	AWS IoT Core

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	"Effect": "Allow",
	"Action": "iot:Publish",
	"Resource": "*"
	},
	{
	"Effect": "Allow",
	"Action": "iot:Receive",
	"Resource": "*"
	},
	{
	"Effect": "Allow",
	"Action": "iot:Subscribe",
	"Resource": "*"
	},
	{
	"Effect": "Allow",
	"Action": [
	"iot:GetThingShadow",
	"iot:UpdateThingShadow",
	"iot:DeleteThingShadow"
	],
	"Resource": "arn:aws:iot:region:account:thing/*"
	
	}
	]</pre>	

Tarefa	Descrição	Habilidades necessárias
	`}` 5. Escolha Criar. 6. No console do AWS IoT, no painel de navegação, escolha Gerenciar, Things. 7. Se uma caixa de diálogo Você ainda não tem coisas for exibida, selecione Registrar uma coisa. Caso contrário, escolha Criar. 8. Na página Creating AWS IoT things (Criar coisas para AWS IoT), selecione Create a single thing (Criar uma única coisa). 9. Na página Adicionar o dispositivo ao registro do dispositivo, insira um nome para o objeto de IoT (por exemplo, `ClientDevice1`) e selecione Próximo. **Note** Você não pode alterar o nome de um objeto depois de criá-lo. Para alterar o nome, é necessário criar uma coisa nova, fornecer o novo nome e,	

Tarefa	Descrição	Habilidades necessárias
	depois, excluir a coisa antiga. 10. Na página Adicionar um certificado ao objeto, escolha Criar certificado. 11. Escolha os links Download para fazer download do certificado, da chave privada e do certificado CA raiz. ⚠ Important Essa é sua única oportunidade de baixar seu certificado e sua chave privada. 12. Selecione Ativar para ativar o certificado. O certificado deve estar ativo para que um dispositivo se conecte ao AWS IoT. 13. Selecione a opção Anexar uma política. 14. Em Adicionar uma política para sua coisa ClientDevicePolicy, escolha Registrar coisa.	

Tarefa	Descrição	Habilidades necessárias
Baixe o certificado CA do dispositivo principal do Greengrass.	Se você espera que o dispositivo principal do Greengrass funcione em ambientes off-line, você precisa disponibilizar o certificado CA principal do Greengrass para que o dispositivo cliente possa verificar o certificado do agente MQTT (que é emitido pela CA principal do Greengrass). Portanto, é importante obter uma cópia desse certificado. Use uma das abordagens a seguir: • Se você tiver acesso à rede ao dispositivo AWS IoT Greengrass a partir do seu PC, insira `https://<device IP>:8883` seu navegador da web e visualize o certificado do agente MQTT e o certifica do CA. Você também pode salvar o certificado CA no dispositivo cliente. • Como alternativa, é possível usar a linha de comandos do OpenSSL: `openssl s_client -showcerts -connect <device IP>:8883`	AWS geral

Tarefa	Descrição	Habilidades necessárias
Copie as credenciais nos dispositivos do cliente.	Copie o certificado CA principal do Greengrass, o certificado do dispositivo e a chave privada nos dispositivos do cliente.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Associe dispositivos cliente ao dispositivo principal.	Associe dispositivos clientes a um dispositivo principal para que eles possam descobrir o dispositivo principal. Os dispositivos cliente podem então usar a API de descoberta do Greengrass para recuperar informações de conectividade e certificados para seus dispositivos principais associados. Para obter mais informações, consulte Associar dispositivos clientes na documentação do AWS IoT Greengrass. 1. No console do AWS IoT Greengrass, escolha dispositivos principais. 2. Escolha o dispositivo principal a ser gerenciado. 3. Na página de detalhes do dispositivo principal, escolha a guia Dispositivos clientes. 4. Na seção Dispositivos cliente associados, escolha Associar dispositivos cliente. 5. No modal Associar dispositivos cliente ao dispositivo principal, faça o seguinte para cada dispositivo cliente a ser associado:	AWS IoT Greengrass

Tarefa	Descrição	Habilidades necessárias
	a. Para associar o dispositivo do AWS IoT, insira o nome do AWS IoT. b. Escolha Adicionar. 6. Selecione Associar . Os dispositivos cliente que você associou agora podem usar a API de descoberta do Greengrass para descobrir esse dispositivo principal.	

Enviar e receber dados

Tarefa	Descrição	Habilidades necessárias
Envie dados de um dispositivo cliente para outro dispositivo cliente.	Use o cliente MQTT em seu dispositivo para publicar uma mensagem sobre o tópico `dt/client1/sensor` .	AWS geral
Envie dados do dispositivo cliente para o AWS IoT Core.	Use o cliente MQTT em seu dispositivo para publicar uma mensagem sobre o tópico `dt/client1/sensor` . No cliente de teste MQTT, inscreva-se no tópico para o qual o dispositivo está enviando mensagens ou inscreva-se em # para todos os tópicos (veja detalhes).	AWS geral

Tarefa	Descrição	Habilidades necessárias
Envie mensagens do AWS IoT Core para dispositivos clientes.	Na página do cliente de teste do MQTT, na guia Publicar em um tópico, no campo Nome do tópico, insira o nome do tópico da sua mensagem. Neste exemplo, use `cmd/client1` para o tópico.	AWS geral

Solução de problemas

Problema	Solução
Não foi possível verificar o erro do certificado do servidor	Esse erro ocorre quando o cliente MQTT não consegue verificar o certificado apresentado pelo agente MQTT durante o handshake TLS. O motivo mais comum é que o cliente MQTT não tem o certificado CA. Siga estas etapas para garantir que o certificado CA seja fornecido ao cliente MQTT. 1. Se você tiver acesso à rede ao dispositivo AWS IoT Greengrass a partir do seu PC, insira `https://<device IP>:8883` na janela do navegador para ver o certificado do agente MQTT e o certificado CA. Você também pode salvar o certificado CA no dispositivo cliente. Como alternativa, use a linha de comando do OpenSSL: `openssl s_client -showcerts -connect <device IP>:8883`

Problema	Solução

	2. Salve o conteúdo dos certificados Moquette CA e Greengrass Core CA em arquivos e, em seguida, visualize o conteúdo decodificado usando o comando:
	
	`openssl x509 -in <Name of CA>.pem -text`
	
	O certificado CA do Moquette deve mostrar o campo SAN como neste exemplo:
	
	`X509v3 Subject Alternative Name:`
	`IP Address:XXX.XXX.XXX.XXX, IP Address:127.0.0.1, DNS:localhost`

Não foi possível verificar o erro do nome do servidor	Esses erros ocorrem quando o cliente MQTT não consegue verificar se está se conectando ao servidor correto. O motivo mais comum é que o endereço IP do dispositivo Greengrass não está listado no campo SAN do certificado. Siga as instruções na solução anterior para obter o certificado do agente MQTT e verificar se o campo SAN contém o endereço IP do dispositivo AWS IoT Greengrass, conforme explicado na seção Informações adicionais. Caso contrário, confirme se o componente do detector de IP está instalado corretamente e reinicie o dispositivo principal.

Problema	Solução
Não é possível verificar o nome do servidor somente ao se conectar a partir de um dispositivo cliente incorporado	O Mbed TLS, que é uma biblioteca TLS popular usada em dispositivos incorporados, atualmente oferece suporte à verificação de nomes DNS somente no campo SAN do certificado, conforme mostrado no código da biblioteca Mbed TLS. Como o dispositivo principal não tem seu próprio nome de domínio e depende do endereço IP, os clientes TLS que usam o Mbed TLS falharão na verificação do nome do servidor durante o handshake TLS, causando uma falha na conexão. Recomendamos que você adicione a verificação do endereço IP da SAN à sua biblioteca Mbed TLS na função x509_crt_check_san function.

Recursos relacionados

- Documentação do AWS IoT Greengrass
- Documentação do AWS IoT Core
- Componente de corretor MQTT
- Componente de ponte MQTT
- Componente de autenticação do dispositivo cliente
- Componente detector IP
- SDKs de dispositivos do AWS IoT
- Implementação de dispositivos clientes locais com o AWS IoT Greengrass (publicação no blog da AWS)
- RFC 5280 – Certificado de infraestrutura de chave pública X.509 da Internet e perfil da lista de revogação de certificados (CRL)

Mais informações

Esta seção fornece informações adicionais sobre as comunicações entre os dispositivos clientes e o dispositivo principal.

O agente MQTT escuta na porta 8883 do dispositivo principal uma tentativa de conexão com o cliente TLS. A ilustração a seguir mostra um exemplo de certificado de servidor do agente MQTT.

O exemplo de certificado exibe os seguintes detalhes:

- O certificado é emitido pela CA do AWS IoT Greengrass Core, que é local e específica para o dispositivo principal; ou seja, ele atua como uma CA local.
- Esse certificado é alternado automaticamente toda semana pelo componente de autenticação do cliente, conforme mostrado na ilustração a seguir. Você pode definir esse intervalo na configuração do componente de autenticação do cliente.

- O nome alternativo do assunto (SAN) desempenha um papel fundamental na verificação do nome do servidor na extremidade do cliente TLS. Isso ajuda o cliente TLS a garantir que ele se conecte ao servidor correto e ajuda a evitar man-in-the-middle ataques durante a configuração da sessão TLS. No exemplo de certificado, o campo SAN indica que esse servidor está escutando no localhost (o soquete de domínio Unix local) e que a interface de rede tem o endereço IP 192.168.1.12.

O cliente TLS usa o campo SAN no certificado para verificar se está se conectando a um servidor legítimo durante a verificação do servidor. Por outro lado, durante um handshake TLS típico entre um servidor HTTP e um navegador, o nome de domínio no campo nome comum (CN - common name) ou no campo SAN é usado para verificar o domínio ao qual o navegador está realmente se conectando durante o processo de verificação do servidor. Se o dispositivo principal não tiver um nome de domínio, o endereço IP incluído no campo SAN tem a mesma finalidade. Para obter mais informações, consulte a seção Nome alternativo do assunto da RFC 5280 – Certificado de infraestrutura de chave pública X.509 da Internet e perfil da Lista de Revogação de Certificados(CRL).

O componente detector de IP no AWS IoT Greengrass garante que os endereços IP corretos sejam incluídos no campo SAN do certificado.

O certificado no exemplo é assinado pelo dispositivo AWS IoT Greengrass que atua como uma CA local. O cliente TLS (cliente MQTT) não conhece essa CA, portanto, devemos fornecer um certificado de CA semelhante ao seguinte.

Mais padrões

- Ingerir dados de IoT de forma econômica diretamente no Amazon S3 usando o AWS IoT Greengrass

Migração e modernização

Tópicos

- Migração
- Modernização
- Mainframes

Migração

Tópicos

- Crie CloudFormation modelos da AWS para tarefas do AWS DMS usando Microsoft Excel e Python
- Conceitos básicos de descoberta automatizada de portfólio
- Migre workloads on-premises da Cloudera para a Cloudera Data Platform na AWS
- Resolva erros de conexão após migrar o Microsoft SQL Server para a Nuvem AWS
- Reinicie o AWS Replication Agent automaticamente sem desativá-lo SELinux após a reinicialização de um servidor de origem RHEL
- Redefinir arquitetura
- Redefinir a hospedagem
- Realocar
- Redefinir a plataforma
- Padrões de migração por workload
- Mais padrões

Crie CloudFormation modelos da AWS para tarefas do AWS DMS usando Microsoft Excel e Python

Criado por Venkata Naveen Koppula (AWS)

Resumo

Esse padrão descreve as etapas para criar automaticamente CloudFormation modelos da AWS para o AWS Database Migration Service (AWS DMS) usando Microsoft Excel e Python.

A migração de bancos de dados usando o AWS DMS geralmente envolve a criação de CloudFormation modelos da AWS para provisionar tarefas do AWS DMS. Anteriormente, a criação CloudFormation de modelos da AWS exigia conhecimento da linguagem de programação JSON ou YAML. Com essa ferramenta, você só precisa de conhecimentos básicos do Excel e de como executar um script Python usando um terminal ou janela de comando.

Como entrada, a ferramenta usa uma pasta de trabalho do Excel que inclui os nomes das tabelas a serem migradas, os Amazon Resource Names (ARNs) dos endpoints do AWS DMS e as instâncias de replicação do AWS DMS. Em seguida, a ferramenta gera CloudFormation modelos da AWS para as tarefas necessárias do AWS DMS.

Para obter etapas detalhadas e informações básicas, consulte a postagem do blog Crie CloudFormation modelos da AWS para tarefas do AWS DMS usando o Microsoft Excel no blog do banco de dados da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Microsoft Excel versão 2016 ou superior
- Python (versão 2.7 ou superior)
- O módulo xlrd Python (instalado em um prompt de comando com o comando: pip install xlrd)
- Endpoints de origem e destino do AWS DMS e instância de replicação do AWS DMS

Limitações

- Os nomes dos esquemas, tabelas e colunas associadas são transformados em caracteres em minúsculas nos endpoints de destino.

- Essa ferramenta não trata da criação de endpoints e instâncias de replicação do AWS DMS.
- Atualmente, a ferramenta oferece suporte a apenas um esquema para cada tarefa do AWS DMS.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados on-premises
- Microsoft Excel

Pilha de tecnologias de destino

- CloudFormation Modelos da AWS
- Um banco de dados na Nuvem AWS

Arquitetura

Ferramentas

- Pycharm IDE ou qualquer ambiente de desenvolvimento integrado (IDE) que suporte Python versão 3.6
- Microsoft Office 2016 (para Microsoft Excel)

Épicos

Configure a rede, a instância de replicação do AWS DMS e os endpoints

Tarefa	Descrição	Habilidades necessárias
Se necessário, solicite um aumento da Service Quota.	Solicite um aumento de service quota para as tarefas do AWS DMS, se necessário.	AWS geral
Configure a região da AWS, as nuvens privadas virtuais (VPCs), os intervalos de		AWS geral

Tarefa	Descrição	Habilidades necessárias
CIDR, as zonas de disponibilidade e as sub-redes.		
Configure a instância de replicação do AWS DMS.	A instância de replicação do AWS DMS pode se conectar a bancos de dados locais e da AWS.	AWS geral
Configure endpoints do AWS DMS.	Configure endpoints para ambos os bancos de dados, de origem e de destino.	AWS geral

Prepare as planilhas para tarefas e tags do AWS DMS

Tarefa	Descrição	Habilidades necessárias
Configure a lista de tabelas.	Liste todas as tabelas envolvidas na migração.	Banco de dados
Prepare a planilha de tarefas.	Prepare a planilha do Excel usando a lista de tabelas que você configurou.	AWS geral, Microsoft Excel
Prepare a planilha de tags.	Detalhe as tags de recursos da AWS a serem anexadas às tarefas do AWS DMS.	AWS geral, Microsoft Excel

Baixe e execute a ferramenta

Tarefa	Descrição	Habilidades necessárias
Baixe e extraia a ferramenta de geração de modelos do GitHub repositório.	GitHub repositório:/ https://github.com/aws-samples/dms-cloudformation-templates-generator	

Tarefa	Descrição	Habilidades necessárias
Execute a ferramenta.	Siga as instruções detalhadas na postagem do blog listada em “Referências e ajuda”.	

Recursos relacionados

- Crie CloudFormation modelos da AWS para tarefas do AWS DMS usando o Microsoft Excel (publicação no blog)
- Gerador de CloudFormation modelos DMS (GitHub repositório)
- Documentação do Python
- descrição e download do xlrd
- Documentação do AWS DMS
- CloudFormation Documentação da AWS

Conceitos básicos de descoberta automatizada de portfólio

Criado por Pratik Chunawala (AWS) e Rodolfo Jr. Cerrada (AWS)

Resumo

Avaliar o portfólio e coletar metadados é um desafio fundamental ao migrar aplicativos e servidores para a nuvem da Amazon Web Services (AWS), especialmente para grandes migrações que têm mais de 300 servidores. O uso de uma ferramenta automatizada de descoberta de portfólio pode ajudá-lo a coletar informações sobre seus aplicativos, como número de usuários, frequência de uso, dependências e informações sobre a infraestrutura do aplicativo. Essas informações são essenciais ao planejar ondas em migração para que você possa priorizar e agrupar adequadamente aplicativos com características semelhantes. O uso de uma ferramenta de descoberta simplifica a comunicação entre a equipe do portfólio e os proprietários do aplicativo, pois a equipe do portfólio pode validar os resultados da ferramenta de descoberta em vez de coletar manualmente os metadados. Esse padrão discute as principais considerações para selecionar uma ferramenta de descoberta automatizada e informações sobre como implantá-la e testá-la em seu ambiente.

Esse padrão inclui um modelo, que é um ponto de partida para criar sua própria lista de verificação de atividades de alto nível. Ao lado da lista de verificação está o modelo para uma matriz responsável, confiável, consultada e informada (RACI). Você pode usar essa matriz RACI para determinar quem é responsável por cada tarefa em sua lista de verificação.

Épicos

Selecionar uma ferramenta de descoberta

Tarefa	Descrição	Habilidades necessárias
Determinar se uma ferrament a de descoberta é apropriada para o seu caso de uso.	Uma ferramenta de descobert a pode não ser a melhor solução para seu caso de uso. Considere o tempo necessári o para selecionar, adquirir, preparar e implantar uma ferramenta de descoberta. Pode levar de 4 a 8 semanas para configurar o dispositi	Líder de migração, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	vo de digitalização para uma ferramenta de descoberta sem agente em seu ambiente ou para instalar agentes em todas as workloads dentro do escopo. Depois de implantad a, você deve esperar de 4 a 12 semanas para que a ferramenta de descoberta colete metadados examinand o as workloads do aplicativ o e realizando a análise da pilha de aplicativos. Se você estiver migrando menos de 100 servidores, poderá coletar manualmente os metadados e analisar as dependências mais rápido do que o tempo necessário para implantar e coletar metadados com uma ferramenta de descoberta automatizada.	

Tarefa	Descrição	Habilidades necessárias
Selecionar uma ferramenta de descoberta.	Revise as Considerações para selecionar uma ferramenta de descoberta automatizada na seção Informações adicionais. Determine os critérios apropriados para selecionar uma ferramenta de descoberta para seu caso de uso e, em seguida, avalie cada ferramenta em relação a esses critérios. Para obter uma lista abrangente de ferramentas automatizadas de descoberta, consulte Ferramentas de migração de descoberta, planejamento e recomendação.	Líder de migração, engenheiro de migração

Preparar a instalação

Tarefa	Descrição	Habilidades necessárias
Preparar a lista de verificação de pré-implantação.	Crie uma lista de verificação das tarefas que você deve concluir antes de implantar a ferramenta. Por exemplo, consulte a Lista de verificação de pré-implantação no site de documentação do Flexera.	Líder de compilação, engenheiro de migração, líder de migração, administrador de rede
Preparar os requisitos de rede.	Provisione as portas, protocolos, endereços IP e roteamento necessários para que a ferramenta execute	Engenheiro de migração, administrador de rede, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	e acesse os servidores de destino. Para obter mais informações, consulte o guia de instalação da sua ferramenta de descobert a. Para obter um exemplo, consulte Requisitos de implantação no site de documentação do Flexera.	
Preparar os requisitos de conta e credencial.	Identifique as credenciais necessárias para acessar os servidores de destino e instalar todos os componentes da ferramenta.	Administrador de nuvem, AWS geral, engenheiro de migração, líder de migração, administrador de rede, administrador da AWS
Preparar os dispositivos nos quais você instalará a ferramenta.	Certifique-se de que os dispositivos nos quais você instalará os componentes da ferramenta atendam às especificações e aos requisito s da plataforma da ferramenta.	Engenheiro de migração, líder de migração, administrador de rede
Preparar os pedidos de alteração.	De acordo com o processo de gerenciamento de mudanças em sua organização, prepare todos os pedidos de alteração necessários e garanta que esses pedidos de alteração sejam aprovados.	Líder de criação, líder de migração

Tarefa	Descrição	Habilidades necessárias
Enviar os requisitos às partes interessadas.	Envie a lista de verificação de pré-implantação e os requisitos de rede às partes interessadas. As partes interessadas devem revisar, avaliar e preparar os requisitos necessários antes de prosseguir com a implantação.	Líder de criação, líder de migração

Implantar a ferramenta

Tarefa	Descrição	Habilidades necessárias
Fazer download do instalador.	Faça download do instalador ou da imagem da máquina virtual. As imagens de máquinas virtuais geralmente vêm no formato OVF (Open Virtualization Format).	Líder de criação, líder de migração
Extrair os arquivos.	Se você estiver usando um instalador, deverá baixar e executar o instalador em um servidor on-premises.	Líder de criação, líder de migração
Implantar a ferramenta nos servidores.	Implante a ferramenta de descoberta nos servidores on-premises de destino da seguinte forma: • Se o arquivo de origem for uma imagem de máquina virtual, implante-o em seu	Líder de criação, líder de migração, administrador de rede

Tarefa	Descrição	Habilidades necessárias
	ambiente de máquina virtual, como VMware. • Se o arquivo de origem for um instalador, execute o instalador para instalar e configurar a ferramenta.	
Iniciar sessão na ferramenta de descoberta.	Siga as mensagens na tela e faça login para começar a usar a ferramenta.	Líder de criação, líder de compilação
Habilitar o produto.	Insira sua chave de licença.	Líder de criação, líder de migração
Configurar a ferramenta.	Insira todas as credenciais necessárias para acessar os servidores de destino, como credenciais para Windows VMware, Simple Network Management Protocol (SNMP) e Secure Shell Protocol (SSH) ou bancos de dados.	Líder de criação, líder de migração

Testar a ferramenta

Tarefa	Descrição	Habilidades necessárias
Selecionar servidores de teste.	Identifique um pequeno conjunto de sub-redes ou endereços IP que não sejam de produção que você possa usar para testar a ferrament a de descoberta. Isso ajuda você a validar os escaneame ntos rapidamente, identific	Líder de criação, líder de migração, administrador de rede

Tarefa	Descrição	Habilidades necessárias
	ar e solucionar quaisquer erros rapidamente e isolar seus testes dos ambientes de produção.	
Começar a escanear os servidores de teste seleciona dos.	Para uma ferramenta de descoberta sem agente, insira as sub-redes ou endereços IP dos servidores de teste selecionados no console da ferramenta de descoberta e inicie a verificação. Para uma ferramenta de descoberta baseada em agente, instale o agente nos servidores de teste seleciona dos.	Líder de criação, líder de migração, administrador de rede
Revisar os resultados da verificação.	Revisar os resultados da verificação dos servidores de teste. Se algum erro for encontrado, solucione e corrija os erros. Documente os erros e as soluções. Você consultar á essas informações no futuro e poderá adicioná-las ao runbook do seu portfólio.	Líder de criação, líder de migração, administrador de rede
Examinar novamente os servidores de teste.	Quando a nova verificação for concluída, repita a verificação até que não haja erros.	Líder de criação, líder de migração, administrador de rede

Recursos relacionados

AWS recursos

- Guia de avaliação do portfólio de aplicativos para Nuvem AWS migração
- Ferramentas de migração de descoberta, planejamento e recomendação

Guias de implantação para ferramentas de descoberta comumente selecionadas

- Implante o dispositivo virtual RN15 0 (documentação do Flexera)
- Instalação do Gatherer (documentação do ModelizeIt)
- Instalação do Analysis Server on-premises (documentação do ModelizeIt)

Mais informações

Considerações para selecionar uma ferramenta de descoberta automatizada

Cada ferramenta de descoberta tem benefícios e limitações. Ao selecionar a ferramenta apropriada para o seu caso de uso, considere o seguinte:

- Selecione uma ferramenta de descoberta que possa coletar a maioria, se não todos, dos metadados necessários para atingir sua meta de avaliação de portfólio.
- Identifique os metadados que você precisa coletar manualmente porque a ferramenta não oferece suporte a eles.
- Forneça os requisitos da ferramenta de descoberta às partes interessadas para que elas possam analisar e avaliar a ferramenta com base em seus requisitos internos de segurança e conformidade, como requisitos de servidor, rede e credencial.
  - A ferramenta exige que você instale um agente na workload dentro do escopo?
  - A ferramenta exige que você configure um dispositivo virtual em seu ambiente?
- Determine seus requisitos de residência de dados. Algumas organizações não querem armazenar seus dados fora do ambiente. Para resolver isso, talvez seja necessário instalar alguns componentes da ferramenta no ambiente on-premises.
- Verifique se a ferramenta oferece suporte ao sistema operacional (SO) e à versão do SO da workload dentro do escopo.
- Determine se seu portfólio inclui servidores mainframe, intermediários e legados. A maioria das ferramentas de descoberta pode detectar essas workloads como dependências, mas algumas ferramentas podem não conseguir obter detalhes do dispositivo, como utilização e dependências do servidor. As ferramentas de descoberta Device42 e ModernizeIT oferecem suporte a servidores de mainframe e de médio porte.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre workloads on-premises da Cloudera para a Cloudera Data Platform na AWS

Criado por Battulga Purevragchaa (AWS), Nijjwol Lamsal (parceiro) e Nidhi Gupta (AWS)

Resumo

Esse padrão descreve as etapas de alto nível para migrar suas workloads on-premises do Cloudera Distributed Hadoop (CDH), da Hortonworks Data Platform (HDP) e do Cloudera Data Platform (CDP) para o CDP Public Cloud na AWS. Recomendamos que você faça parceria com o Cloudera Professional Services e um integrador de sistemas (SI) para implementar essas etapas.

Há muitos motivos pelos quais os clientes da Cloudera desejam mover suas workloads on-premises de CDH, HDP e CDP para a nuvem. Alguns motivos típicos incluem:

- Simplificar a adoção de novos paradigmas de plataforma de dados, como data lakehouse ou data mesh
- Aumentar a agilidade dos negócios, democratizar o acesso e a inferência sobre os ativos de dados existentes
- Reduzir o custo total de propriedade (TCO)
- Melhorar a elasticidade da workload
- Permitir maior escalabilidade; reduzir drasticamente o tempo de provisionamento de serviços de dados em comparação com a base de instalação legada no on-premises
- Remover o hardware antigo; reduzir significativamente os ciclos de atualização de hardware
- Aproveite os pay-as-you-go preços, que são estendidos às cargas de trabalho da Cloudera na AWS com o modelo de licenciamento da Cloudera (CCU)
- Aproveite a implantação mais rápida e a integração aprimorada com plataformas de integração contínua e entrega contínua (CI/CD)
- Usar uma única plataforma unificada (CDP) para várias workloads

A Cloudera suporta todas as principais workloads, incluindo Machine Learning, Engenharia de Dados, Data Warehouse, Banco de Dados Operacional, Processamento de Stream (CSP) e segurança e governança de dados. A Cloudera oferece essas workloads on-premises há muitos anos, e você pode migrar essas workloads para a Nuvem AWS usando o CDP Public Cloud com o Workload Manager e o Replication Manager.

O Cloudera Shared Data Experience (SDX) fornece um catálogo compartilhado de metadados entre essas workloads para facilitar o gerenciamento e as operações consistentes de dados. O SDX também inclui segurança abrangente e granular para proteção contra ameaças e governança unificada para recursos de auditoria e pesquisa para conformidade com padrões como o Payment Card Industry Data Security Standard (PCI DSS) e o GDPR.

Visão geral da migração do CDP

Workload	Workload de origem	Nuvem privada CDH, HDP e CDP
	Ambiente de origem	• Windows, Linux • On-premises, colocalização ou em qualquer ambiente que não seja da AWS
	Workload de destino	Nuvem pública CDP na AWS
	Ambiente do destino	• Modelo de implantação: conta de cliente • Modelo operacional: ambiente de gerenciamento Cliente/Cloudera
Migração	Estratégia de migração (7Rs)	Redefinir a hospedagem, redefinir a plataforma ou refatorar
	Isso é um upgrade na versão da workload?	Sim
	Duração da migração	• Implantação: cerca de uma semana para criar uma conta de cliente, uma nuvem privada virtual (VPC) e um ambiente gerenciado pelo cliente da CDP Public Cloud.

- Duração da migração: de 1 a 4 meses, dependendo da complexidade e do tamanho da workload.

Custos	Custo da execução da workload na AWS	• Em um alto nível, o custo de uma migração da workload da CDH para a AWS pressupõe que você estabelecerá um novo ambiente na AWS. Isso inclui a contabilização do tempo e do esforço da equipe, bem como o provisionamento de recursos de computação e software de licenciamento para o novo ambiente. • O modelo de preços baseado no consumo de nuvem Cloudera oferece a flexibilidade de aproveita r os recursos de escalabil idade automática e de intermitência. Para obter mais informações, consulte as taxas de serviço do CDP Public Cloud no site da Cloudera. • O Cloudera Enterprise Data Hub é baseado no Amazon Elastic Compute Cloud (Amazon EC2) e modela de perto os clusters tradicion ais. O Data Hub pode ser personalizado, mas isso afetará os custos. • O CDP Public Cloud Data Warehouse, o Cloudera Machine Learning e o Cloudera Data Engineeri

		ng (CDE) são baseados em contêineres e podem ser configurados para escalar automaticamente.
Acordos e estrutura de infraestrutura	Requisitos do sistema	Consulte a seção Pré-requisitos.
	SLA	Consulte o Acordo de Nível de Serviço da Cloudera para CDP Public Cloud.
	DR	Consulte Recuperação de desastres na documentação da Cloudera.
	Modelo operacional e de licenciamento (para a conta de destino da AWS)	Modelo “Traga a sua própria licença” (BYOL)
Conformidade	Requisitos de segurança	Consulte Visão geral da segurança da Cloudera na documentação da Cloudera.
	Outras certificações de conformidade	Veja as informações no site da Cloudera sobre a conformidade com o Regulamento Geral de Proteção de Dados (GDPR) e o CDP Trust Center.

Pré-requisitos e limitações

Pré-requisitos

- Requisitos de conta da AWS, incluindo contas, recursos, serviços e permissões, como a configuração de políticas e perfis do (IAM) do AWS Identity and Access Management
- Pré-requisitos para implantar o CDP a partir do site da Cloudera

A migração exige as seguintes funções e conhecimentos:

Função	Habilidades e responsabilidades
Líder de migração	Garante suporte executivo, colaboração em equipe, planejamento, implementação e avaliação
Cloudera PME	Habilidades especializadas em administr ação de CDH, HDP e CDP, administração de sistemas e arquitetura
Arquiteto da AWS	Habilidades em serviços, redes, segurança e arquiteturas da AWS

Arquitetura

Desenvolver a arquitetura adequada é uma etapa essencial para garantir que a migração e o desempenho atendam às suas expectativas. Para que seu esforço de migração atenda às suposições desse manual, seu ambiente de dados de destino na Nuvem AWS, seja em instâncias hospedadas em nuvem privada virtual (VPC) ou CDP, deve ser equivalente ao seu ambiente de origem em termos de sistema operacional e versões de software, bem como das principais especificações da máquina.

O diagrama a seguir (reproduzido com permissão da planilha de dados do Cloudera Shared Data Experience) mostra os componentes de infraestrutura para o ambiente de CDP e como os níveis ou componentes da infraestrutura interagem.

Essa arquitetura inclui os seguintes componentes CDP:

- O Data Hub é um serviço para lançar e gerenciar clusters de workload desenvolvido pelo Cloudera Runtime. Você pode usar as definições de cluster no Data Hub para provisionar e acessar clusters de workload para casos de uso personalizados e definir configurações de cluster personalizadas. ,Para obter mais informações, consulte o site da Cloudera.
- O fluxo e o streaming de dados abordam os principais desafios que as empresas enfrentam com os dados em movimento. Ele gerencia o seguinte:
  - Processamento de fluxo de dados em tempo real em alto volume e alta escala

  - Rastreando a proveniência dos dados e a linhagem dos dados de streaming
  - Gerenciando e monitorando aplicativos periféricos e fontes de streaming

  Para obter mais informações, consulte Cloudera DataFlow e CSP no site da Cloudera.
- A engenharia de dados inclui integração de dados, qualidade de dados e governança de dados, que ajudam as organizações a criar e manter fluxos de trabalho e pipelines de dados. ,Para obter mais informações, consulte o site da Cloudera. Saiba mais sobre o suporte para instâncias spot para facilitar a redução de custos na AWS para workloads de engenharia de dados da Cloudera.
- O Data Warehouse permite que você crie data warehouses e data marts independentes que se escalam automaticamente para atender às demandas de workload. Esse serviço fornece instâncias de computação isoladas e otimização automatizada para cada data warehouse e data mart, além de ajudar você a economizar custos durante as reuniões SLAs. ,Para obter mais informações, consulte o site da Cloudera. Saiba mais sobre o gerenciamento de custos e o ajuste de escala automático do Cloudera Data Warehouse na AWS.
- O banco de dados operacional no CDP fornece uma base confiável e flexível para aplicativos escaláveis e de alto desempenho. Ele fornece um banco de dados escalável, sempre disponível e em tempo real, que serve dados estruturados tradicionais, juntamente com dados novos e não estruturados, em uma plataforma operacional e de armazenamento unificada. ,Para obter mais informações, consulte o site da Cloudera.
- O Machine Learning é uma plataforma de machine learning nativa de nuvem que combina recursos de autoatendimento de ciência de dados e engenharia de dados em um único serviço portátil em uma nuvem de dados corporativa. Ele permite a implantação escalável de machine learning e inteligência artificial (IA) em dados em qualquer lugar. ,Para obter mais informações, consulte o site da Cloudera.

CDP na AWS

O diagrama a seguir (adaptado com permissão do site da Cloudera) mostra a arquitetura de alto nível do CDP na AWS. O CDP implementa seu próprio modelo de segurança para gerenciar contas e fluxo de dados. Eles são integrados ao IAM por meio do uso de funções entre contas.

O ambiente de gerenciamento do CDP reside em uma conta principal da Cloudera em sua própria VPC. Cada conta de cliente tem sua própria subconta e uma VPC exclusiva. Os perfis do IAM entre contas e as tecnologias SSL direcionam o tráfego de gerenciamento de e para o ambiente de gerenciamento para os serviços ao cliente que residem em sub-redes públicas roteáveis pela

Internet dentro de cada VPC do cliente. Na VPC do cliente, a Cloudera Shared Data Experience (SDX) fornece segurança corporativa com governança e conformidade unificadas para que você possa obter insights de seus dados com mais rapidez. A SDX é uma filosofia de design incorporada a todos os produtos da Cloudera. Para obter mais informações sobre SDX e a arquitetura de rede CDP Public Cloud para AWS, consulte a documentação da Cloudera.

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o Kubernetes na AWS sem precisar instalar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Automação e ferramentas

- Para obter ferramentas adicionais, você pode usar o Cloudera Backup Data Recovery (BDR), o AWS Snowball e o AWS Snowmobile para ajudar a migrar dados da CDH, HDP e CDP on-premises para a CDP hospedada pela AWS.
- Para novas implantações, recomendamos que você use a solução de parceiros da AWS para CDP.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Envolva a equipe da Cloudera.	A Cloudera busca um modelo padronizado de engajamento com seus clientes e pode trabalhar com seu integrador de sistemas (SI) para promover a mesma abordagem. Entre em contato com a equipe de clientes da Cloudera para que eles possam fornecer orientações e os recursos técnicos necessários para iniciar o projeto. Entrar em contato com a equipe da Cloudera garante que todas as equipes necessárias possam se preparar para a migração à medida que a data se aproxima. Você pode entrar em contato com os Serviços Profissionais da Cloudera para mover sua implantação do Cloudera do piloto para a produção rapidamente, a um custo menor e com desempenho máximo. Para obter uma lista completa de ofertas, consulte o site da Cloudera.	Líder de migração

Tarefa	Descrição	Habilidades necessárias
Crie um ambiente de nuvem pública CDP na AWS para sua VPC.	Trabalhe com o Cloudera Professional Services ou com seu SI para planejar e implantar a nuvem pública CDP em uma VPC na AWS.	Arquiteto de nuvem, Cloudera SME

Tarefa	Descrição	Habilidades necessárias
Priorize e avalie as workloads para migração.	Avalie todas as suas workloads on-premises para determinar as workloads mais fáceis de migrar. Os aplicativos que não são essenciais são os melhores a serem implantados primeiro, pois terão um impacto mínimo em seus clientes. Guarde as workloads essenciais para o final, depois de migrar com sucesso outras workloads. **Note** Cargas de trabalho transitórias (CDP Data Engineering) são mais fáceis de migrar do que cargas de trabalho persistentes (CDP Data Warehouse). Também é importante considerar o volume e os locais dos dados ao migrar. Os desafios podem incluir a replicação contínua de dados de um ambiente on-premises para a nuvem e a alteração dos canais de ingestão de dados para importar dados	Líder de migração

Tarefa	Descrição	Habilidades necessárias
	diretamente para a nuvem.	
Discuta as atividades de CDH, HDP, CDP e migração de aplicativos legados.	Considere e comece a planejar as seguintes atividades com o Cloudera Workload Manager: • Dados e workloads para copiar para seu ambiente da AWS • Dados prontos para a nuvem • Vizinhos barulhentos, que consomem recursos e criam problemas para outros inquilinos • workloads elásticas • Clusters pequenos com alta sobrecarga operacional	Líder de migração

Tarefa	Descrição	Habilidades necessárias
Preencha os requisitos e recomendações do Cloudera Replication Manager.	Trabalhe com o Cloudera Professional Services e seu SI para se preparar para migrar workloads para seu ambiente de nuvem pública CDP na AWS. Compreender os requisitos e recomendações a seguir pode ajudá-lo a evitar problemas comuns durante e após a instalação do serviço Replication Manager. • Analise os documentos de suporte do Replication Manager para confirmar se você atende aos requisitos do ambiente e do sistema. Para obter mais informações, consulte a matriz de suporte do CDP Public Cloud Replication Manager no site da Cloudera. • Você não precisa de acesso root aos nós nos quais o aplicativo Replication Manager e o mecanismo Data Lifecycle Manager (DLM) serão instalados. • Instale o Apache Hive durante a instalação inicial do Replication Manager, a menos que tenha certeza de que não usará a replicação do Hive no futuro. Se	Líder de migração

Tarefa	Descrição	Habilidades necessárias
	você decidir instalar o Hive depois de criar políticas de replicação do HDFS no Replication Manager, precisará excluir e recriar todas as políticas de replicação do HDFS depois de adicionar o Hive. • Os clusters usados no Replication Manager devem ter configurações simétricas. Cada cluster em uma relação de replicaçã o deve ser configurado exatamente da mesma forma para segurança (Kerberos), gerenciamento de usuários (LDAP/AD) e Knox Proxy. Serviços de cluster, como Sistema de Arquivos Distribuí do do Hadoop (HDFS), Apache Hive, Apache Knox, Apache Ranger e Apache Atlas, podem ter configura ções diferentes para alta disponibilidade (HA). Por exemplo, os clusters de origem e de destino podem ter configurações separadas de HA e não HA.	

Migre a CDP para a AWS

Tarefa	Descrição	Habilidades necessárias
Migre a primeira workload para ambientes de dev/teste usando o Cloudera Workload Manager.	Seu SI pode ajudá-lo a migrar sua primeira workload para a nuvem AWS. Esse deve ser um aplicativo que não seja voltado para o cliente nem essencial. Os candidatos ideais para a migração de dev/teste são aplicativos que têm dados que a nuvem pode ingerir facilmente, como workloads de engenharia de dados do CDP. Essa é uma workload transitória que geralmente tem menos usuários acessando-a, em comparação com uma workload persistente, como uma workload do CDP Data Warehouse, que pode ter muitos usuários que precisam de acesso ininterrupto. As workloads de engenharia de dados não são persistentes, o que minimiza o impacto nos negócios se algo der errado. No entanto, esses trabalhos podem ser essenciais para a geração de relatórios de produção, portanto, priorize as workloads de engenharia de dados de baixo impacto.	Líder de migração

Tarefa	Descrição	Habilidades necessárias
Repita as etapas de migração conforme necessário.	O Cloudera Workload Manager ajuda a identificar as workloads mais adequadas para a nuvem. Ele fornece métricas como classific ações de desempenho da nuvem, planos de tamanho/c apacidade para o ambiente de destino e planos de replicaçã o. Os melhores candidatos para migração são workloads sazonais, relatórios ad hoc e trabalhos intermitentes que não consomem muitos recursos. O Cloudera Replication Manager move dados on-premises para a nuvem e da nuvem para on-premises. Otimize proativamente workloads, aplicativos, desempenho e capacidad e de infraestrutura para armazenamento de dados, engenharia de dados e machine learning usando o Workload Manager. Para obter um guia completo sobre como modernizar um data warehouse, consulte o site da Cloudera.	Cloudera PME

Recursos relacionados

Documentação da Cloudera:

- Registrar clusters clássicos com CDP, Cloudera Manager e Replication Manager:
  - Console de Gerenciamento
  - Replicação de hive do Replication Manager
- Replicação do Sentry
- Permissões do Sentry
- Lista de verificação de planejamento de clusters do Data Hub
- Arquitetura do Workload Manager
- Requisitos do Replication Manager
- Observabilidade da plataforma de dados Cloudera
- Requisitos do AWS

Documentação da AWS:

- Migração de dados para nuvem

Resolva erros de conexão após migrar o Microsoft SQL Server para a Nuvem AWS

Criado por Premkumar Chelladurai (AWS)

Resumo

Depois de migrar o Microsoft SQL Server executado no Windows Server 2008 R2, 2012 ou 2012 R2 para instâncias do Amazon Elastic Compute Cloud (Amazon EC2) na Amazon Web Services (AWS) Cloud, a conexão com o SQL Server falha e os seguintes erros aparecem:

- `[Microsoft][ODBC SQL Server Driver][DBNETLIB] General Network error`
- `ERROR [08S01] [Microsoft][SQL Native Client]Communication link failure. System.Data.SqlClient.SqlException: A transport-level error has occurred when sending the request to the server. (provider: TCP Provider, error: 0 - An existing connection was forcibly closed by the remote host.)`
- `TCP Provider: The semaphore timeout period has expired`

Esse padrão descreve como você pode resolver esses erros desativando os recursos do Windows Scalable Networking Pack (SNP) no nível do sistema operacional (SO) e da interface de rede para o SQL Server executado no Windows Server 2008 R2, 2012 ou 2012 R2.

Pré-requisitos e limitações

Pré-requisitos

- Privilégios de administrador para Windows Server.
- Se você usou o AWS Application Migration Service como sua ferramenta de migração, precisará de uma das seguintes versões do Windows Server:
  - Windows Server 2008 R2 Service Pack 1, 2012 ou 2012 R2
- Se você usou a CloudEndure migração como sua ferramenta de migração, precisará de uma das seguintes versões do Windows Server:
  - Windows Server 2003 R2 Service Pack 3, 2008, 2008 R2 Service Pack 1, 2012 ou 2012 R2

Ferramentas

- Amazon EC2 — A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode usar EC2 a Amazon para lançar quantos servidores virtuais precisar e pode expandir ou aumentar a escala.
- Windows Server: o Windows Server é uma plataforma para criar uma infraestrutura de aplicativos, redes e serviços web conectados.

Épicos

Desative os recursos SNP nos níveis do sistema operacional e da interface de rede elástica

Tarefa	Descrição	Habilidades necessárias
Desative os recursos SNP no nível do sistema operacional.	1. Entre no Windows Server e abra um prompt de comando como um administrador. 2. Execute o comando `netsh int tcp show global`. 3. Na saída, verifique se um `Receive-Side Scaling` ou `Chimney Offload` está no modo `enabled`. Se algum for `enabled`, execute um dos comandos a seguir: • `netsh int tcp set global chimney=disabled` • `netsh int tcp set global rss=disabled`	Administrador da AWS, administrador de sistemas da AWS, engenheiro de migração, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
Desative os recursos do SNP no nível da interface de rede elástica.	1. Escolha Iniciar, insira `encpa.cpl`, em seguida, pressione Enter. 2. Clique com o botão direito em Elastic Network Adapter. 3. No menu pop-up, escolha Propriedades. 4. Na janela Propriedades do adaptador Ethernet, escolha Configurar. 5. Na janela pop-up Proprieda des do Adaptador de Rede Elástica da Amazon escolha a guia Avançado. 6. Na seção Propriedade, desative todos os descarreg amentos e RSS.	Administrador da AWS, administrador da nuvem, administrador de sistemas da AWS

Recursos relacionados

- Como solucionar problemas de atributos avançados de desempenho de rede, como RSS e NetDMA

Reinicie o AWS Replication Agent automaticamente sem desativá-lo SELinux após a reinicialização de um servidor de origem RHEL

Criado por Anil Kunapareddy (AWS), Shanmugam Shanker (AWS) e Venkatramana Chintha (AWS)

Resumo

O AWS Application Migration Service ajuda a simplificar, agilizar e automatizar a migração da sua workload do Red Hat Enterprise Linux (RHEL) para a nuvem da Amazon web Services (AWS). Para adicionar servidores de origem ao Application Migration Service, você instala o AWS Replication Agent nos servidores.

O Application Migration Service fornece replicação em tempo real, assíncrona e em nível de bloco. Isso significa que você pode continuar com as operações normais de TI durante todo o processo de replicação. Essas operações de TI podem exigir que você reinicie ou reinicie o servidor de origem do RHEL durante a migração. Se isso acontecer, o AWS Replication Agent não será reiniciado automaticamente e sua replicação de dados será interrompida. Normalmente, você pode definir o Security-Enhanced Linux (SELinux) para o modo desativado ou permissivo para reiniciar automaticamente o AWS Replication Agent. No entanto, as políticas de segurança da sua organização podem proibir a desativação SELinux e talvez você também precise renomear seus arquivos.

Esse padrão descreve como reiniciar automaticamente o AWS Replication Agent sem desligá-lo SELinux quando o servidor de origem do RHEL é reinicializado ou reiniciado durante uma migração.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma workload on-premises do RHEL que você deseja migrar para a Nuvem AWS.
- Serviço de migração de aplicativos inicializado a partir do console do Application Migration Service. A inicialização é necessária somente na primeira vez que você usa esse serviço. Para obter instruções, consulte a documentação do Application Migration Service.
- Uma política do IAM do AWS Identity and Access Management (IAM) existente para o Application Migration Service. Para saber mais, consulte a documentação do Serviço de Migração de Aplicativos.

Versões

- RHEL versão 7 ou superior

Ferramentas

Serviços da AWS

- O AWS Application Migration Service é uma solução altamente automatizada lift-and-shift (rehospedagem) que simplifica, agiliza e reduz o custo da migração de aplicativos para a AWS.

Comandos Linux

A tabela a seguir fornece uma lista dos comandos Linux que você executará no seu servidor de origem RHEL. Eles também são descritos nos épicos e nas histórias desse padrão.

Comando	Descrição
`#systemctl –version`	Identifica a versão do sistema.
`#systemctl list-units --type=service`	Lista todos os serviços ativos que estão disponíveis no servidor RHEL.
`#systemctl list-units --type=service | grep running`	Lista todos os serviços atualmente em execução no servidor RHEL.
`#systemctl list-units --type=service | grep failed`	Lista todos os serviços que falharam ao carregar após a reinicialização ou reinicialização do servidor RHEL.
`restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Muda o contexto para `aws-replication-service` .
`yum install policycoreutils*`	Instala os principais utilitários da política necessários para a operação do SELinux sistema.
`ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Pesquisa o registro de auditoria e cria um módulo para políticas.

`semodule -i my-modprobe.pp`	Ativa a política.
`cat my-modprobe.te`	Visualiza o conteúdo do `my-modprobe.te` arquivo.
`semodule -l | grep my-modprobe`	Verifica se a política foi carregada no SELinux módulo.

Épicos

Instale o AWS Replication Agent e reinicie o servidor de origem do RHEL

Tarefa	Descrição	Habilidades necessárias
Crie um usuário do Application Migration Service com uma chave de acesso e uma chave de acesso secreta.	Para instalar o AWS Replication Agent, você deve criar um usuário do Application Migration Service com as credenciais necessárias da AWS. Para obter instruções, consulte a documentação do Application Migration Service.	Engenheiro de migração
Instale o AWS Replication Agent.	1. Faça login no AWS Management Console e abra o console do AWS Migration Service em https://console.aws.amazon.com/mgn/casa. 2. Defina as configurações de replicação seguindo as instruções na documentação do Application Migration Service. 3. Instale o AWS Replication Agent seguindo as	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	instruções na documentação do Application Migration Service. 4. Na página Servidores de origem, escolha o servidor de origem RHEL e, em seguida, escolha Replicação para iniciar a replicação inicial. Para saber mais, consulte a documentação do Serviço de Migração de Aplicativos.	
Reinicie ou reinicialize o servidor de origem do RHEL.	Reinicie ou reinicie seu servidor de origem RHEL quando o status de replicação de dados for exibido Paradono painel de migração.	Engenheiro de migração
Verifique o status da replicação de dados.	Aguarde uma hora e verifique novamente o status da replicação de dados no painel de migração. Deve estar no estado saudável.	Engenheiro de migração

Verifique o status do AWS Replication Agent no servidor de origem do RHEL

Tarefa	Descrição	Habilidades necessárias
Identifique a versão do sistema.	Abra a interface de linha de comando do seu servidor de origem RHEL e execute o seguinte comando para identificar a versão do sistema:	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	`#systemctl –version`	
Liste todos os serviços ativos.	Para listar todos os serviços ativos disponíveis no servidor RHEL, execute o comando: `#systemctl list-units --type=service`	Engenheiro de migração
Liste todos os serviços em execução.	Para listar todos os serviços atualmente em execução no servidor RHEL, use o comando: `#systemctl list-units --type=service | grep running`	Engenheiro de migração
Liste todos os serviços que falharam ao carregar.	Para listar todos os serviços que falharam ao carregar após a reinicialização ou reinicialização do servidor RHEL, execute o comando: `#systemctl list-units --type=service | grep failed`	Engenheiro de migração

Crie e execute o SELinux módulo

Tarefa	Descrição	Habilidades necessárias
Alterar o contexto de segurança.	Na interface de linha de comando do seu servidor de origem do RHEL, execute o seguinte comando para alterar	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	o contexto de segurança do serviço de replicação da AWS: `restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	
Instale os principais utilitários.	Para instalar os principais utilitários necessários para a operação do SELinux sistema e suas políticas, execute o comando: `yum install policycoreutils*`	Engenheiro de migração
Pesquise o registro de auditoria e crie um módulo para políticas.	Execute o comando : `ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Engenheiro de migração
Exiba o conteúdo do my-modprobe-te arquivo.	O arquivo `my-modprobe.te` é gerado pelo comando audit2allow. Ele inclui os SELinux domínios, o diretório de origem da política e os subdiretórios e especifica as regras e transições do vetor de acesso associada s aos domínios. Execute os seguintes comandos para exibir o conteúdo do arquivo. `cat my modprobe.te`	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Ativa a política.	Para inserir o módulo e ativar o pacote de políticas, execute o comando: `semodule -i my-modprobe.pp`	Engenheiro de migração
Verifique se o módulo foi carregado.	Execute o comando : `semodule -l | grep my-modprobe` Depois que o SELinux módulo for carregado, você não precisará mais configurar SELinux o modo desativado ou permissivo durante a migração.	Engenheiro de migração
Reinicialize ou reinicie o servidor de origem do RHEL e verifique o status da replicação de dados.	Abra o console do AWS Migration Service, navegue até o Andamento da replicação de dados e, em seguida, reinicie ou reinicie seu servidor de origem RHEL. A replicação de dados agora deve ser retomada automaticamente após a reinicialização do servidor de origem do RHEL.	Engenheiro de migração

Recursos relacionados

- Documentação do serviço de migração de aplicativos
- Materiais de treinamento técnico

- Solução de problemas do AWS Replication Agent
- Políticas do Application Migration Service

Redefinir arquitetura

Tópicos

- Converter VARCHAR2 (1) tipo de dados para Oracle para tipo de dados booleano para Amazon Aurora PostgreSQL
- Crie usuários e funções do aplicativo no Aurora compatível com PostgreSQL
- Emule o Oracle DR usando um banco de dados global Aurora compatível com PostgreSQL
- Implemente SHA1 o hashing para dados de PII ao migrar do SQL Server para o PostgreSQL
- Migre incrementalmente do Amazon RDS para Oracle para o Amazon RDS para PostgreSQL usando o Oracle SQL Developer e o AWS SCT
- Faça o upload de arquivos BLOB em TEXT usando a codificação de arquivos no Aurora PostgreSQL-Compatible
- Migre o Amazon RDS for Oracle para o Amazon AWS SCT RDS for PostgreSQL com e usando e AWS DMSAWS CLIAWS CloudFormation
- Migre o Amazon RDS para Oracle para o Amazon RDS para PostgreSQL no modo SSL usando o AWS DMS
- Migrar os pacotes de pragma Oracle SERIALLY_REUSABLE para o PostgreSQL
- Migre tabelas externas da Oracle para a compatibilidade com o Amazon Aurora PostgreSQL
- Migre índices baseados em funções do Oracle para o PostgreSQL
- Migre funções nativas do Oracle para o PostgreSQL usando extensões
- Migre um banco de dados Db2 da Amazon para o EC2 Aurora MySQL compatível usando o AWS DMS
- Migre um banco de dados Microsoft SQL Server da Amazon EC2 para o Amazon DocumentDB usando o AWS DMS
- Migre um banco de dados ThoughtSpot Falcon local para o Amazon Redshift
- Migrar um banco de dados Oracle para o Amazon DynamoDB usando AWS DMS
- Migre uma tabela particionada do Oracle para o PostgreSQL usando o AWS DMS
- Migre do Amazon RDS para Oracle para o Amazon RDS para MySQL
- Migre do IBM Db2 na Amazon para o EC2 Aurora compatível com PostgreSQL usando o AWS DMS e o AWS SCT
- Migre do Oracle 8i ou 9i para o Amazon RDS for PostgreSQL usando o AWS DMS SharePlex

- Migre do Oracle 8i ou 9i para o Amazon RDS para PostgreSQL usando visões materializadas e o AWS DMS
- Migre do Oracle na Amazon EC2 para o Amazon RDS for MySQL usando o AWS DMS e o AWS SCT
- Migrar do Oracle para o Amazon DocumentDB usando o AWS DMS
- Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for MariaDB usando o AWS DMS e o AWS SCT
- Migre um banco de dados Oracle on-premises para o Amazon RDS para MySQL, usando o AWS DMS e o AWS SCT.
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para PostgreSQL usando um Oracle bystander e o AWS DMS
- Migre do banco de dados Oracle para o Amazon RDS for PostgreSQL usando o Oracle GoldenGate
- Migre um banco de dados Oracle para o Amazon Redshift usando o AWS DMS e o AWS SCT
- Migrar um banco de dados Oracle para o Aurora PostgreSQL usando AWS DMS e AWS SCT
- Migrar dados de um banco de dados Oracle on-premises para o Aurora PostgreSQL
- Migre do SAP ASE para o Amazon RDS para SQL Server usando o AWS DMS
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift utilizando o AWS DMS
- Migre um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift usando agentes de extração de dados da AWS SCT
- Migre um banco de dados Teradata para o Amazon Redshift usando agentes de extração de dados do AWS SCT
- Migre um banco de dados Vertica on-premises para o Amazon Redshift usando agentes de extração de dados do AWS SCT
- Migre aplicativos legados do Oracle Pro*C para o ECPG
- Migre colunas geradas virtualmente do Oracle para o PostgreSQL
- Configure a funcionalidade Oracle UTL_FILE no Aurora compatível com PostgreSQL
- Valide objetos de banco de dados após migrar do Oracle para o Amazon Aurora PostgreSQL

Converter VARCHAR2 (1) tipo de dados para Oracle para tipo de dados booleano para Amazon Aurora PostgreSQL

Criado por Naresh Damera (AWS)

Resumo

Durante uma migração do Amazon Relational Database Service (Amazon RDS) para Oracle para a edição compatível com o Amazon Aurora PostgreSQL, você pode encontrar uma incompatibilidade de dados ao validar a migração em (). AWS Database Migration Service AWS DMS Para evitar essa incompatibilidade, você pode converter o tipo de dados VARCHAR2 (1) em tipo de dados booleano.

VARCHAR2 o tipo de dados armazena cadeias de texto de tamanho variável e VARCHAR2 (1) indica que a sequência tem 1 caractere de comprimento ou 1 byte. Para obter mais informações sobre VARCHAR2, consulte os tipos de dados integrados da Oracle (documentação da Oracle).

Nesse padrão, na coluna da tabela de dados da fonte de amostra, os dados VARCHAR2 (1) são Y, para Sim, ou N, para Não. Esse padrão inclui instruções para usar AWS DMS e AWS Schema Conversion Tool (AWS SCT) para converter esse tipo de dados dos valores Y e N em VARCHAR2 (1) para valores verdadeiros ou falsos em booleano.

Público-alvo

Esse padrão é recomendado para aqueles que têm experiência em migrar bancos de dados Oracle para o Aurora, compatível com PostgreSQL, usando o. AWS DMS Ao concluir a migração, siga as recomendações em Converter Oracle em Amazon RDS for PostgreSQL ou Amazon Aurora PostgreSQL (documentação).AWS SCT

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Confirme se seu ambiente está preparado para o Aurora, incluindo a configuração de credenciais, permissões e um grupo de segurança. Para obter mais informações, consulte Configuração de seu ambiente para o Amazon Aurora (documentação do Aurora).
- Um banco de dados de origem do Amazon RDS for Oracle que contém uma coluna de tabela VARCHAR2 com (1) dados.

- Uma instância de banco de dados de destino compatível com o Amazon Aurora PostgreSQL. Para obter mais informações, consulte Criação de um cluster de banco de dados e conexão a um banco de dados em um cluster de banco de dados Aurora PostgreSQL (documentação do Aurora).

Versões do produto

- Amazon RDS para Oracle versão 12.1.0.2 ou superior.
- AWS DMS versão 3.1.4 ou posterior. Para obter mais informações, consulte Usando um banco de dados Oracle como fonte AWS DMS e Usando um banco de dados PostgreSQL como destino AWS DMS para AWS DMS (documentação). Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e recursos.
- AWS Schema Conversion Tool (AWS SCT) versão 1.0.632 ou posterior. Recomendamos que você use a versão mais recente do AWS SCT para obter o suporte mais abrangente de versões e recursos.
- O Aurora é compatível com as versões do PostgreSQL listadas em Versões do mecanismo do banco de dados para Aurora PostgreSQL-Compatible (documentação do Aurora).

Arquitetura

Pilha de tecnologia de origem

Instância de banco de dados do Amazon RDS para Oracle

Pilha de tecnologias de destino

Instância de banco de dados Amazon Aurora PostgreSQL-Compatible

Arquitetura de origem e destino

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e compatível com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL.
- AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para Nuvem AWS ou entre combinações de configurações na nuvem e no local.

- O Amazon Relational Database Service (Amazon RDS) para Oracle ajuda você a configurar, operar e escalar um banco de dados relacional Oracle no. Nuvem AWS
- AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de banco de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.

Outros serviços

- O Oracle SQL Developer é um ambiente de desenvolvimento integrado que simplifica o desenvolvimento e o gerenciamento de bancos de dados Oracle em implantações tradicionais e baseadas em nuvem. Nesse padrão, você usa essa ferramenta para se conectar à instância do banco de dados Amazon RDS para Oracle e consultar os dados.
- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados. Neste padrão, você usa essa ferramenta para se conectar à instância do banco de dados Aurora e consulta os dados.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Crie um relatório de migração do banco de dados.	1. Em AWS SCT, crie um relatório de avaliação da migração do banco de dados. Para obter mais informações, consulte Criação de relatórios de avaliação da migração. 2. Revise e execute as ações indicadas no relatório de avaliação da migração. Para obter mais, consulte o https://docs.aws.amazon.com/SchemaConversio	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	nTool/latest/userguide/CHAP_AssessmentReport.ActionItems.html Ítens de ação do relatório de avaliação.	
Elimine restrições de chave externa no banco de dados de destino.	No PostgreSQL, as chaves estrangeiras são implementadas usando gatilhos. Durante a fase de carga total, AWS DMS carrega cada tabela uma de cada vez. Recomendamos que você desative as restrições de chave externa durante um carregamento total, usando um dos seguintes métodos: • Desative temporariamente todos os triggers da instância e conclua o carregamento total. • Use o parâmetro `session_replication_role` no PostgreSQL. Se não for possível desativar as restrições de chave estrangeira, crie uma tarefa de AWS DMS migração para os dados primários que seja específica da tabela principal e da tabela secundária.	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias

Coloque chaves primárias e chaves exclusivas no banco de dados de destino.	Usando os comandos a seguir, desative as chaves primárias e as restrições no banco de dados de destino. Isso ajuda a melhorar o desempenho da tarefa de carregamento inicial.
	`ALTER TABLE <table> DISABLE PRIMARY KEY;`
	`ALTER TABLE <table> DISABLE CONSTRAINT <constraint_name>;`
		DBA, Desenvolvedor

Crie a tarefa de carregamento inicial.	Em AWS DMS, crie a tarefa de migração para a carga inicial. Para obter instruções, consulte Criação de uma tarefa. Para método de migração, escolha Migrar dados existentes. Esse método de migração é chamado `Full Load` na API. Não inicie essa tarefa ainda.	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Edite as configurações da tarefa de carregamento inicial.	Edite as configurações da tarefa para adicionar a validação de dados. Essas configurações de validação devem ser criadas em um arquivo JSON. Para obter instruções e exemplos, consulte Especificação das configurações da tarefa. Adicione as seguintes validações: • Para validar se os dados VARCHAR2 (1) foram convertidos com precisão em booleanos no banco de dados de destino, adicione o código no script de validação de dados na seção Informações adicionais desse padrão. O script de validação converte os valores booleanos de 1 para Y e de 0 para N na tabela de destino e, em seguida, compara os valores na tabela de destino com a tabela de origem. Para validar o restante da migração de dados, habilite a validação de dados na tarefa. Para obter mais informaçõ	Administrador da AWS, DBA

Tarefa	Descrição	Habilidades necessárias
	es, consulte Configuração da tarefa de validação de dados.	
Criar uma tarefa de replicação contínua.	Em AWS DMS, crie a tarefa de migração que mantém o banco de dados de destino sincronizado com o banco de dados de origem. Para obter instruções, consulte Criação de uma tarefa. Em método de migração, escolha Replicar somente alterações de dados. Não inicie essa tarefa ainda.	DBA

Teste a tarefa de migração

Tarefa	Descrição	Habilidades necessárias
Crie dados de amostra para testes.	No banco de dados de origem, crie uma tabela de amostra com dados para fins de teste.	Desenvolvedor
Confirme se não há atividades conflitantes.	Use `pg_stat_activity` para verificar se há alguma atividade no servidor que possa afetar a migração. Para obter mais informaçõ es, consulte Coletor de estatísticas (documentação do PostgreSQL).	Administrador da AWS
Inicie as tarefas de AWS DMS migração.	No AWS DMS console, na página Painel, inicie o carregamento inicial e as tarefas de replicação	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	contínuas que você criou no épico anterior.	
Monitore as tarefas e os estados de carregamento da tabela.	Durante a migração, monitore o status da tarefa e os estados da tabela. Quando a tarefa de carregamento inicial estiver concluída, na guia Estatísticas da tabela: • O Estado de carregamento deve ser Tabela concluída. • O Estado de validação deve ser Validado.	Administrador da AWS
Verifique os resultados da migração.	Usando pgAdmin, consulte a tabela no banco de dados de destino. Uma consulta bem-sucedida indica que os dados foram migrados com êxito.	Desenvolvedor
Adicione as chaves primárias e estrangeiras ao banco de dados de destino.	Crie as chaves primárias e estrangeiras ao banco de dados de destino. Para obter mais informações, consulte ALTER TABLE (site do PostgreSQL).	DBA
Limpe os dados do teste.	Nos bancos de dados de origem e destino, limpe os dados que foram criados para teste de unidade.	Desenvolvedor

Substituir

Tarefa	Descrição	Habilidades necessárias
Concluir a migração.	Repita o tópico anterior, Testar as tarefas de migração, usando os dados de origem reais. Essa ação migra os dados do banco de dados de origem para o banco de dados de destino.	Desenvolvedor
Valide se os bancos de dados de origem e de destino estão em sincronia.	Valide se os bancos de dados de origem e de destino estão em sincronia. Para obter mais informações e instruções, consulte validação AWS DMS de dados.	Desenvolvedor
Interrompa o banco de dados de origem.	Interrompa o banco de dados Amazon RDS para Oracle. Para instruções, consulte Interrupção temporária de uma instância de banco de dados do Amazon RDS. Quando você interrompe o banco de dados de origem, a carga inicial e as tarefas de replicação em andamento AWS DMS são automatic amente interrompidas. Nenhuma ação adicional é necessária para interromper essas tarefas.	Desenvolvedor

Recursos relacionados

AWS referências

- Migre um banco de dados Oracle para o Aurora PostgreSQL usando e (orientação AWS DMSAWS SCT prescritiva)AWS
- Conversão do Oracle para o Amazon RDS for PostgreSQL ou Amazon Aurora PostgreSQL (documentação)AWS SCT
- Como AWS DMS funciona (AWS DMS documentação)

Outras referências

- Tipo de dados booleano (documentação do PostgreSQL)
- Tipos de dados integrados da Oracle (documentação da Oracle)
- pgAdmin (site do pgAdmin)
- SQL Developer (site da Oracle)

Tutoriais e vídeos

- Começando com AWS DMS
- Conceitos básicos do Amazon RDS
- Introdução a AWS DMS (Vídeo)
- Noções básicas sobre o Amazon RDS (vídeo)

Mais informações

Script de validação de dados

O script de validação de dados a seguir converte 1 em Y e 0 em N. Isso ajuda a AWS DMS tarefa a ser concluída com êxito e a passar pela validação da tabela.

```
{
"rule-type": "validation",
"rule-id": "5",
"rule-name": "5",
"rule-target": "column",
"object-locator": {
```

```
"schema-name": "ADMIN",
"table-name": "TEMP_CHRA_BOOL",
"column-name": "GRADE"
},
"rule-action": "override-validation-function",
"target-function": "case grade when '1' then 'Y' else 'N' end"
        }
```

A instrução `case` no script executa a validação. Se a validação falhar, AWS DMS insere um registro na tabela public.awsdms_validation_failures_v1 na instância do banco de dados de destino. Esse registro inclui o nome da tabela, o horário do erro e detalhes sobre os valores incompatíveis nas tabelas de origem e de destino.

Se você não adicionar esse script de validação de dados à AWS DMS tarefa e os dados forem inseridos na tabela de destino, a AWS DMS tarefa mostrará o estado de validação como Registros incompatíveis.

Durante a AWS SCT conversão, a tarefa de AWS DMS migração altera o tipo de dados do tipo de dados VARCHAR2 (1) para booleano e adiciona uma restrição de chave primária na `''N0''` coluna.

Crie usuários e funções do aplicativo no Aurora compatível com PostgreSQL

Criado por Abhishek Verma (AWS)

Resumo

Quando você migra para o Amazon Aurora Edição Compatível com PostgreSQL, os usuários e funções do banco de dados que existem no banco de dados de origem devem ser criados no banco de dados do Aurora compatível com PostgreSQL. Você pode criar usuários e funções no Aurora compatíveis com PostgreSQL usando duas abordagens diferentes:

- Use usuários e funções semelhantes no banco de dados de destino e no banco de dados de origem. Nessa abordagem, as linguagens de definição de dados (DDLs) são extraídas para usuários e funções do banco de dados de origem. Em seguida, eles são transformados e aplicados ao banco de dados Aurora de destino compatível com PostgreSQL. Por exemplo, a postagem do blog Use SQL para mapear usuários, funções e concessões do Oracle para o PostgreSQL aborda o uso da extração de um mecanismo de banco de dados de origem Oracle.
- Use usuários e funções padronizados que são comumente usados durante o desenvolvimento, a administração e para realizar outras operações relacionadas no banco de dados. Isso inclui operações somente de leitura, leitura/gravação, desenvolvimento, administração e implantação realizadas pelos respectivos usuários.

Esse padrão contém as concessões necessárias para a criação de usuários e funções no Aurora, compatível com o PostgreSQL, necessárias para a abordagem padronizada de usuários e funções. As etapas de criação do usuário e da função estão alinhadas à política de segurança de conceder privilégio mínimo aos usuários do banco de dados. A tabela a seguir lista os usuários, suas funções correspondentes e seus detalhes no banco de dados.

Usuários	Funções	Finalidade
`APP_read`	`APP_RO`	Usado para acesso somente de leitura no esquema `APP`
`APP_WRITE`	`APP_RW`	Usado para as operações de gravação e leitura no esquema `APP`

APP_dev_user	APP_DEV	Usado para fins de desenvolvimento no esquema APP_DEV, com acesso somente para leitura no esquema APP
Admin_User	rds_superuser	Usado para realizar operações de administrador no banco de dados
APP	APP_DEP	Usado para criar os objetos sob o esquema APP e para a implantação de objetos no esquema APP

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS)
- Um banco de dados PostgreSQL, banco de dados Amazon Aurora Edição Compatível com PostgreSQL ou Amazon Relational Database Service (Amazon RDS) para banco de dados PostgreSQL

Versões do produto

- Todas as versões do PostgreSQL

Arquitetura

Pilha de tecnologia de origem

- Qualquer banco de dados

Pilha de tecnologias de destino

- Amazon Aurora compatível com PostgreSQL

Arquitetura de destino

O diagrama a seguir mostra as funções do usuário e a arquitetura do esquema no banco de dados do Aurora compatível com PostgreSQL.

Automação e escala

Esse padrão contém os usuários, as funções e o script de criação do esquema, que você pode executar várias vezes sem afetar os usuários existentes do banco de dados de origem ou de destino.

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID, que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.

Outros serviços

- O psql é uma ferramenta frontend baseada em terminal que é instalada com cada instalação do banco de dados PostgreSQL. Ele tem uma interface da linha de comando para executar comandos SQL, PL-PGSQL e do sistema operacional.
- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.

Épicos

Criar os usuários e perfis

Tarefa	Descrição	Habilidades necessárias
Criar o usuário de implantação.	O usuário de implantação APP será usado para criar e modificar os objetos do banco de dados durante as	DBA

Tarefa	Descrição	Habilidades necessárias

	implantações. Use os scripts a seguir para criar a função de usuário de implantação APP_DEP no esquema APP. Valide os direitos de acesso para garantir que esse usuário tenha apenas o privilégio de criar objetos no esquema APP necessário.
	
	1. Conecte-se ao usuário administrador e crie o esquema.
	
	`CREATE SCHEMA APP;`
	
	2. Crie o usuário.
	
	`CREATE USER APP WITH PASSWORD <password> ;`
	
	3. Crie a função.
	
	`CREATE ROLE APP_DEP ;`
	`GRANT all on schema APP to APP_DEP ;`
	`GRANT USAGE ON SCHEMA APP to APP_DEP ;`
	`GRANT connect on database <db_name> to APP_DEP ;`
	`GRANT APP_DEP to APP;`
	
	4. Para testar os privilégios, conecte-se ao APP e crie as tabelas.	

Tarefa	Descrição	Habilidades necessárias

	`set search_path to APP;`
	`SET`
	`CREATE TABLE test(id integer ) ;`
	`CREATE TABLE`
	5. Verifique os privilégios.
	`select schemaname , tablename , tableowner from pg_tables where tablename like 'test' ;`
	`schemaname | tablename | tableowner`
	`APP | test | APP`	

Tarefa	Descrição	Habilidades necessárias

Crie o usuário somente para leitura.	O usuário de somente leitura `APP_read` será usado para realizar a operação somente leitura no esquema. APP
	Use os scripts a seguir para criar o usuário somente para leitura. Valide os direitos de acesso para garantir que esse usuário tenha privilégi os somente para ler os objetos no esquema APP e para conceder automatic amente acesso de leitura a qualquer novo objeto criado no esquema APP.
	
	1. Crie o usuário `APP_read`.
	
	`create user APP_read ;`
	`alter user APP_read with password 'your_password' ;`
	
	2. Crie a função.
	
	`CREATE ROLE APP_ro ;`
	`GRANT SELECT ON ALL TABLES IN SCHEMA APP TO APP_RO ;`
	`GRANT USAGE ON SCHEMA APP TO APP_RO`
	`GRANT CONNECT ON DATABASE testdb TO APP_RO ;`
	`GRANT APP_RO TO APP_read;`
		DBA

Tarefa	Descrição	Habilidades necessárias

	3. Para testar os privilégios, faça login usando o usuário `APP_read`.
	
	`set search_path to APP ;`
	`create table test1( id integer) ;`
	`ERROR: permission denied for schema APP`
	`LINE 1: create table test1( id integer) ;`
	`insert into test values (34) ;`
	`ERROR: permission denied for table test`
	`SQL state: 42501`
	`select from test`
	`no rows selected`	

Tarefa	Descrição	Habilidades necessárias

Crie o usuário de leitura/gravação.	O usuário de leitura/gravação `APP_WRITE` será usado para realizar operações de leitura e gravação no esquema APP. Use os scripts a seguir para criar o usuário de leitura/gravação e conceder a ele a função `APP_RW`. Valide os direitos de acesso para garantir que esse usuário tenha privilégios de leitura e gravação somente nos objetos do esquema APP e para conceder automaticamente acesso de leitura e gravação a qualquer novo objeto criado no esquema APP.
	
	1. Crie o usuário.
	
	`CREATE USER APP_WRITE ; alter user APP_WRITE with password 'your_password' ;`
	
	2. Crie a função.
	
	`CREATE ROLE APP_RW; GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA APP TO APP_RW ; GRANT CONNECT ON DATABASE postgres to APP_RW ; GRANT USAGE ON SCHEMA APP to APP_RW ;`	

Tarefa	Descrição	Habilidades necessárias

	<pre>ALTER DEFAULT
	 PRIVILEGES IN SCHEMA
	 APP
	GRANT SELECT, INSERT,
	 UPDATE, DELETE ON
	 TABLES TO APP_RW ;
	GRANT APP_RW to
	 APP_WRITE</pre>
	3. Para testar os privilégios, faça login usando o usuário `APP_WRITE` .
	
	<pre>SET SEARCH_PATH to
	 APP;
	CREATE TABLE
	 test1(id integer) ;
	ERROR: permission
	 denied for schema APP
	LINE 1: create table
	 test1(id integer) ;
	SELECT * FROM test ;
	id
	---- 	
	12
	INSERT INTO test
	 values (31) ;
	INSERT 0 1</pre>	

Tarefa	Descrição	Habilidades necessárias

Crie o usuário administrador.	O usuário administrador `Admin_User` será usado para realizar operações administrativas no banco de dados. Exemplos dessas operações são `CREATE ROLE` e `CREATE DATABASE`. O `Admin_User` usa a função integrada `rds_superuser` para realizar operações administrativas no banco de dados. Use os scripts a seguir para criar e testar o privilégio do usuário administrador `Admin_User` no banco de dados.
	1. Crie o usuário e conceda a função.
	`create user Admin_User WITH PASSWORD ‘Your password’ ALTER user Admin_user CREATEDB; ALTER user Admin_user CREATEROLE;`
	2. Para testar o privilégio, faça login com o usuário `Admin_User` .
	`SELECT * FROM APP.test ; id ---- 31`
		DBA

Tarefa	Descrição	Habilidades necessárias

	`CREATE ROLE TEST ;`
	`CREATE DATABASE`
	`test123 ;`	

Tarefa	Descrição	Habilidades necessárias

Crie o usuário de desenvolvimento.	O usuário de desenvolvimento `APP_dev_user` terá direitos para criar os objetos em seu esquema local `APP_DEV` e acesso de leitura no esquema APP. Use os scripts a seguir para criar e testar os privilégios do usuário `APP_dev_user` no banco de dados.
	1. Crie o usuário.
	`CREATE USER APP1_dev_user with password 'your password';`
	2. Crie o esquema `APP_DEV` para o `App_dev_user` .
	`CREATE SCHEMA APP1_DEV ;`
	3. Crie a função do APP_DEV.
	`CREATE ROLE APP1_DEV ;`
	`GRANT APP1_RO to APP1_DEV ;`
	`GRANT SELECT ON ALL TABLES IN SCHEMA APP1_DEV to APP1_dev_user`
	`GRANT USAGE, CREATE ON SCHEMA APP1_DEV to APP1_DEV_USER`
	`GRANT APP1_DEV to APP1_DEV_USER ;`
		DBA

Tarefa	Descrição	Habilidades necessárias

	4. Para testar os privilégios, faça login em `APP_dev_user`.
	
	`CREATE TABLE APP1_dev.test1( id integer ) ;`
	`CREATE TABLE`
	`INSERT into APP1_dev.test1 ( select * from APP1.test );`
	`INSERT 0 1`
	`CREATE TABLE APP1.test4 ( id int) ;`
	`ERROR: permission denied for schema APP1`
	`LINE 1: create table APP1.test4 ( id int) ;`	

Recursos relacionados

Documentação do PostgreSQL

- CRIAR PERFIL
- CRIAR USUÁRIO
- Perfis predefinidos

Mais informações

Aprimoramento do PostgreSQL 14

O PostgreSQL 14 fornece um conjunto de funções predefinidas que dão acesso a determinadas capacidades e informações privilegiadas comumente necessárias. Os administradores (incluindo funções que têm o privilégio de `CREATE ROLE`) podem conceder essas funções ou outras funções em seu ambiente aos usuários, fornecendo-lhes acesso aos recursos e informações especificados.

Os administradores podem conceder aos usuários acesso a essas funções usando o comando `GRANT`. Por exemplo, para conceder a função `pg_signal_backend` a `Admin_User`, você pode executar o comando a seguir.

```
GRANT pg_signal_backend TO Admin_User;
```

A função `pg_signal_backend` tem como objetivo permitir que os administradores habilitem funções confiáveis e não de superusuário para enviar sinais para outros backends. Para obter mais informações, consulte Aprimoramentos do PostgreSQL 14.

Ajustando o acesso

Em alguns casos, pode ser necessário fornecer acesso mais granular aos usuários (por exemplo, acesso baseado em tabela ou acesso baseado em colunas). Nesses casos, funções adicionais podem ser criadas para conceder esses privilégios aos usuários. Para obter mais informações, consulte Concessões do PostgreSQL.

Emule o Oracle DR usando um banco de dados global Aurora compatível com PostgreSQL

Criado por HariKrishna Boorgadda (AWS)

Resumo

As práticas recomendadas para recuperação de desastres (DR) empresarial consistem basicamente em projetar e implementar sistemas de hardware e software tolerantes a falhas que possam sobreviver a um desastre (continuidade dos negócios) e retomar as operações normais (retomada dos negócios), com intervenção mínima e, idealmente, sem perda de dados. Criar ambientes tolerantes a falhas para satisfazer os objetivos corporativos de DR pode ser caro e demorado, além de exigir um forte comprometimento da empresa.

O Oracle Database fornece três abordagens diferentes para DR que fornecem o mais alto nível de proteção e disponibilidade de dados em comparação com qualquer outra abordagem para proteger dados do Oracle.

- Dispositivo Oracle Zero Data Loss Recovery
- Oracle Active Data Guard
- Oráculo GoldenGate

Esse padrão fornece uma forma de emular o Oracle GoldenGate DR usando um banco de dados global Amazon Aurora. A arquitetura de referência usa o Oracle GoldenGate para DR em três regiões da AWS. O padrão percorre a redefinição da plataforma de origem para o banco de dados global Aurora nativo de nuvem, baseado na edição do Amazon Aurora compatível com PostgreSQL.

O banco de dados global Aurora foi criado para aplicações com uma presença mundial. Um único banco de dados Aurora abrange várias regiões da AWS com até cinco regiões secundárias. Os bancos de dados globais do Aurora fornecem os seguintes atributos:

- Replicação física em nível de armazenamento
- Leituras globais de baixa latência
- Recuperação de desastres rápida após interrupções em toda a região
- Migrações rápidas entre regiões
- Baixo atraso de replicação em todas as regiões

- Little-to-no impacto no desempenho do seu banco de dados

Para obter mais informações sobre os atributos e vantagens do banco de dados global Aurora, consulte Usar o Amazon Aurora Global Database. Para obter mais informações sobre failovers não planejados e gerenciados, consulte Uso de failover em um Amazon Aurora Global Database.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um driver PostgreSQL Java Database Connectivity (JDBC) para conectividade de aplicativos
- Um banco de dados global do Aurora baseado no Amazon Aurora Edição Compatível com PostgreSQL
- Um banco de dados do Oracle Real Application Clusters (RAC) migrou para o banco de dados global Aurora baseado em compatibilidade com o Aurora PostgreSQL

Limitações dos bancos de dados globais do Aurora

- Os bancos de dados globais Aurora não estão disponíveis em todas as regiões da AWS. Para obter uma lista de regiões compatíveis, consulte Bancos de dados globais do Aurora PostgreSQL.
- Para obter informações sobre atributos que não são compatíveis e outras limitações dos bancos de dados globais do Aurora, consulte as Limitações do Amazon Aurora Global Database.

Versões do produto

- Edição do Amazon Aurora compatível com PostgreSQL versão 10.14 ou superior

Arquitetura

Pilha de tecnologia de origem

- Banco de dados de quatro nós do Oracle RAC
- Oráculo GoldenGate

Arquitetura de origem

O diagrama a seguir mostra três clusters com Oracle RAC de quatro nós em diferentes regiões da AWS replicados usando o Oracle. GoldenGate

Pilha de tecnologias de destino

- Um Amazon Aurora Global Database de três clusters baseado no Aurora PostgreSQL, compatível com um cluster na região primária e dois clusters em diferentes regiões secundárias

Arquitetura de destino

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e compatível com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL.
- Os Amazon Aurora Global Database abrangem várias regiões da AWS, fornecendo leituras globais de baixa latência e recuperação rápida de interrupções raras que podem afetar uma região inteira da AWS.

Épicos

Adicionar regiões com instâncias de banco de dados de leitor

Tarefa	Descrição	Habilidades necessárias
Conecte um ou mais clusters secundários do Aurora.	No menu Console de Gerenciamento da AWS, selecione Amazon Aurora. Selecione o cluster primário, selecione Actions e Adicionar região na lista suspensa.	DBA
Selecione a classe da instância.	Você pode alterar a classe da instância do cluster secundári o. No entanto, recomendamos	DBA

Tarefa	Descrição	Habilidades necessárias
	mantê-la igual à classe de instância do cluster primário.	
Adicione a terceira região.	Repita as etapas desse épico para adicionar um cluster na terceira região.	DBA

Fazer failover do banco de dados global Aurora

Tarefa	Descrição	Habilidades necessárias
Remova o cluster primário do banco de dados Aurora global.	1. Na página Bancos de dados, selecione o cluster primário. 2. Selecione Remover do global para seguir para o failover de um cluster secundário.	DBA
Reconfigure o aplicativo a fim de desviar o tráfego de gravação para o cluster recém-promovido.	Modifique o endpoint no aplicativo usando o do cluster recém-promovido.	DBA
Pare de emitir qualquer operação de gravação para o cluster indisponível.	Interrompa o aplicativo e qualquer atividade de data manipulation language (DML – linguagem de manipulação de dados) no cluster que você removeu.	DBA
Crie um novo banco de dados global Aurora.	Agora você pode criar um banco de dados Aurora global com o cluster recém-pro movido como cluster primário.	DBA

Inicie o cluster primário

Tarefa	Descrição	Habilidades necessárias
Selecione o cluster primário a ser iniciado a partir do banco de dados global.	No console do Amazon Aurora, selecione o cluster primário na configuração do banco de dados global.	DBA
Inicie o cluster.	Na lista suspensa Ações, selecione Iniciar. Esse processo pode levar algum tempo. Atualize a tela para ver o status ou verifique na coluna Status o estado atual do cluster após a conclusão da operação.	DBA

Limpe os recursos

Tarefa	Descrição	Habilidades necessárias
Exclua os clusters secundári os restantes.	Após a conclusão do piloto de failover, remova os clusters secundários do banco de dados global.	DBA
Exclua o cluster primário.	Remova o cluster.	DBA

Recursos relacionados

- Usar o Amazon Aurora Global Database
- Soluções de recuperação de desastres do Aurora PostgreSQL usando o Amazon Aurora Global Database (publicação do blog)

Implemente SHA1 o hashing para dados de PII ao migrar do SQL Server para o PostgreSQL

Criado por Rajkumar Raghuwanshi (AWS) e Jagadish Kantubugata (AWS)

Resumo

Esse padrão descreve como implementar o hashing do Secure Hash Algorithm 1 (SHA1) para endereços de e-mail ao migrar do SQL Server para o Amazon RDS for PostgreSQL ou compatível com o Amazon Aurora PostgreSQL. Um endereço de e-mail é um exemplo de informações de identificação pessoal (PII). PII são informações que, quando visualizadas diretamente ou combinadas com outros dados relacionados, podem ser usadas para inferir razoavelmente a identidade de um indivíduo.

Esse padrão abrange os desafios de manter valores de hash consistentes em diferentes agrupamentos de bancos de dados e codificações de caracteres e fornece uma solução usando funções e gatilhos do PostgreSQL. Embora esse padrão se concentre no SHA1 hashing, ele pode ser adaptado para outros algoritmos de hash suportados pelo módulo do PostgreSQL. `pgcrypto` Sempre considere as implicações de segurança de sua estratégia de hashing e consulte especialistas em segurança ao lidar com dados confidenciais.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Banco de dados SQL Server de origem
- Banco de dados PostgreSQL de destino (compatível com Amazon RDS for PostgreSQL ou Aurora PostgreSQL)
- Experiência em codificação PL/pgSQL

Limitações

- Esse padrão exige alterações de agrupamento em nível de banco de dados com base em casos de uso.
- O impacto no desempenho em grandes conjuntos de dados não foi avaliado.

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Versões do produto

- Microsoft SQL Server 2012 ou posterior

Arquitetura

Pilha de tecnologia de origem

- SQL Server
- NET Framework

Pilha de tecnologias de destino

- PostgreSQL
- `pgcrypto`extensão

Automação e escala

- Considere implementar a função de hashing como um procedimento armazenado para facilitar a manutenção.
- Para grandes conjuntos de dados, avalie o desempenho e considere estratégias de indexação ou processamento em lote.

Ferramentas

Serviços da AWS

- Compatível com o Amazon Aurora PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e compatível com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL.
- AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para Nuvem AWS ou entre combinações de configurações na nuvem e no local.

- Amazon Relational Database Service Amazon RDS for PostgreSQL O Amazon RDS for PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL no. Nuvem AWS
- AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.

Outras ferramentas

- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.
- O SQL Server Management Studio (SSMS) é um ambiente integrado para gerenciar qualquer infraestrutura SQL.

Práticas recomendadas

- Use as configurações de agrupamento apropriadas para lidar com caracteres especiais no lado do banco de dados de destino.
- Teste minuciosamente com uma variedade de endereços de e-mail, incluindo endereços com caracteres não ASCII.
- Mantenha a consistência na manipulação de maiúsculas e minúsculas entre as camadas do aplicativo e do banco de dados.
- Compare o desempenho das consultas usando os valores em hash.

Épicos

Analise a implementação do hashing de origem

Tarefa	Descrição	Habilidades necessárias
Analise o código do SQL Server.	Para revisar o código do SQL Server que gera SHA1 hashes, faça o seguinte:	Engenheiro de dados, DBA, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	• Analise a implementação existente do SHA1 hashing no SQL Server. • Identifique os métodos exatos usados para geração de hash. • Documente os parâmetros de entrada e o formato de saída. • Analise todas as conversões ou transformações de tipos de dados. • Examine as configurações de agrupamento e seu impacto.	
Documente o algoritmo de hashing e as transformações de dados.	Para documentar o algoritmo de hash exato e as transformações de dados, faça o seguinte: • Crie documentação técnica detalhada do processo de hashing. • Documente a lógica de step-by-step transformação. • Especifique os formatos de entrada e saída e os tipos de dados. • Inclua casos extremos e tratamento de caracteres especiais.	Desenvolvedor de aplicativos, engenheiro de dados, DBA

Crie a função de hashing do PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Crie uma `pgcrypto` extensão.	Para criar a `pgcrypto` extensão, use `pgAdmin/psql` para executar o seguinte comando: `CREATE EXTENSION pgcrypto;`	DBA, engenheiro de dados
Implemente uma função do PostgreSQL.	Implemente a função PostgreSQL a seguir para replicar a lógica de hash do SQL Server. Em um alto nível, essa função usa as seguintes etapas: 1. Opcionalmente, converte a entrada em maiúsculas. 2. Cria um SHA1 hash da entrada. 3. Obtém os últimos 10 bytes (80 bits) desse hash. 4. Converte esses bytes em um número inteiro de 64 bits. `CREATE OR REPLACE FUNCTION utility.hex_to_bigint ( par_val character varying, par_upper character varying DEFAULT`	Engenheiro de dados, DBA, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	'lower'::character varying)
	RETURNS bigint
	LANGUAGE 'plpgsql'
	AS $BODY$
	DECLARE
	retnumber bigint;
	digest_bytes bytea;
	BEGIN
	if lower(par_upper) = 'upper'
	then
	digest_bytes := digest(upper(par_val), 'sha1');
	else
	digest_bytes := digest((par_val), 'sha1');
	end if;
	retnumber := ('x' || encode(substring(digest_bytes, length(digest_bytes)-10+1), 'hex'))::bit(64)::bigint;
	RETURN retnumber;
	END;
	$BODY$;	

Tarefa	Descrição	Habilidades necessárias

Testar a função.	Para testar a função, use dados de exemplo do SQL Server para verificar os valores de hash correspon dentes. Execute o seguinte comando:
	`select 'alejandr o_rosalez@example. com' as Email, utility.hex_to_big int('alejandro_ros alez@example.com', 'upper') as HashValue;`
	`--OUTPUT /* email hashvalue "alejandro_rosale z@example.com" 451 397011176045063 */`
		Desenvolvedor de aplicativos, DBA, engenheiro de dados

Implemente gatilhos para hashing automático

Tarefa	Descrição	Habilidades necessárias
Crie gatilhos em tabelas relevantes.	Para criar acionadores em tabelas relevantes para gerar automaticamente valores de hash na inserção ou atualizaç ão, execute o seguinte comando:	Desenvolvedor de aplicativos, engenheiro de dados, DBA

Tarefa	Descrição	Habilidades necessárias

	`CREATE OR REPLACE FUNCTION update_email_hash() RETURNS TRIGGER AS $$ BEGIN NEW.email_hash = utility.hex_to_bigint(NEW.email, 'upper'); RETURN NEW; END; $$ LANGUAGE plpgsql;`
	
	`CREATE TRIGGER email_hash_trigger BEFORE INSERT OR UPDATE ON users FOR EACH ROW EXECUTE FUNCTION update_email_hash();`	

Migrar dados existentes

Tarefa	Descrição	Habilidades necessárias
Desenvolva ou use um script de migração AWS DMS.	Desenvolva um script de migração ou use AWS DMS para preencher valores de hash para dados existentes (incluindo valores de hash armazenados como `BIGINT` no sistema de origem). Complete as seguintes tarefas:	Engenheiro de dados, desenvolvedor de aplicativos, DBA

Tarefa	Descrição	Habilidades necessárias
	• Crie scripts de migração para transferência de dados com valores de hash. • Configure AWS DMS tarefas com as regras de transformação apropriadas. • Configure os endpoints de origem e destino em AWS DMS. • Implemente mecanismos de tratamento e registro de erros. • Crie uma estratégia de processamento em lote para grandes conjuntos de dados. • Crie consultas de validação para verificação de dados.	

Tarefa	Descrição	Habilidades necessárias
Use a nova função de hash do PostgreSQL.	Para usar a nova função de hash do PostgreSQL para garantir a consistência, faça o seguinte: • Implemente procedimentos de validação para verificar a consistência do hash. • Crie scripts de comparação entre os sistemas de origem e de destino. • Configure testes automatizados para verificação do valor de hash. • Documente quaisquer discrepâncias e etapas de resolução.	Desenvolvedor de aplicativos, DBA, engenheiro DevOps

Atualizar consultas de aplicativos

Tarefa	Descrição	Habilidades necessárias
Identifique as consultas do aplicativo.	Para identificar consultas de aplicativos que usam valores em hash, faça o seguinte: • Analise a base de código do aplicativo para consultas usando valores de hash. • Revise os procedimentos e funções armazenados que fazem referência às operações de hash.	Desenvolvedor de aplicativos, DBA, engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	• Documente as métricas de desempenho da consulta e os planos de execução. • Identifique dependências em pesquisas baseadas em hash. • Mapeie os componentes afetados do aplicativo.	
Modifique as consultas.	Se necessário, modifique as consultas para usar a nova função de hash do PostgreSQL. Faça o seguinte: • Refatore as consultas existentes para usar a função de hash do PostgreSQL. • Atualize os procedimentos e funções armazenados. • Implemente e teste novos padrões de consulta. • Otimize as consultas modificadas para melhorar o desempenho.	Desenvolvedor de aplicativos, DBA, engenheiro de dados

Teste e valide

Tarefa	Descrição	Habilidades necessárias
Realize testes.	Para realizar testes completos com um subconjunto de dados de produção, faça o seguinte:	Desenvolvedor de aplicativos, engenheiro de dados, DBA

Tarefa	Descrição	Habilidades necessárias
	• Crie um plano de teste para validação do subconjunto de dados. • Extraia uma amostra representativa dos dados de produção. • Configure um ambiente de teste com as configurações adequadas. • Execute testes de carregamento e transform ação de dados. • Realize testes de volume e estresse.	
Valide se os valores de hash coincidem.	Para validar a correspon dência dos valores de hash entre o SQL Server e o PostgreSQL, faça o seguinte: • Desenvolva scripts de comparação para valores de hash. • Crie relatórios de validação para correspondência de hash. • Implemente procedimentos de verificação automatiz ados. • Documente todas as discrepâncias encontradas. • Analise e resolva incompati bilidades de hash.	Desenvolvedor de aplicativos, engenheiro de dados, DBA

Tarefa	Descrição	Habilidades necessárias
Verifique a funcionalidade do aplicativo.	Para verificar a funcional idade do aplicativo usando os dados migrados e a nova implementação de hashing, faça o seguinte: • Execute testes de end-to-en d aplicativos. • Valide todos os recursos do aplicativo usando dados em hash. • Teste o desempenho do aplicativo com a nova implementação. • Verifique as integrações e dependências da API.	Desenvolvedor de aplicativos, DBA, engenheiro de dados

Solução de problemas

Problema	Solução
Os valores de hash não coincidem.	Verifique as codificações e agrupamentos de caracteres entre a origem e o destino. Para obter mais informações, consulte Gerenciar alterações de agrupamento no PostgreSQL no Amazon Aurora e no Amazon RDS (Blog).AWS

Recursos relacionados

AWS Blogs

- Gerencie alterações de agrupamento no PostgreSQL no Amazon Aurora e no Amazon RDS
- Migre o SQL Server para o Amazon Aurora PostgreSQL usando as melhores práticas e as lições aprendidas em campo

Outros recursos

- Módulo pgcrypto do PostgreSQL (documentação do PostgreSQL)
- Funções de gatilho do PostgreSQL (documentação do PostgreSQL)
- Função HASHBYTES do SQL Server (documentação da Microsoft)

Migre incrementalmente do Amazon RDS para Oracle para o Amazon RDS para PostgreSQL usando o Oracle SQL Developer e o AWS SCT

Criado por Pinesh Singal (AWS)

Resumo

Muitas estratégias e abordagens de migração são executadas em várias fases, que podem durar de algumas semanas a vários meses. Durante esse período, você pode enfrentar atrasos devido a patches ou atualizações nas instâncias de banco de dados Oracle de origem que você deseja migrar para instâncias de banco de dados PostgreSQL. Para evitar essa situação, recomendamos que você migre incrementalmente o código restante do banco de dados Oracle para o código do banco de dados PostgreSQL.

Esse padrão fornece uma estratégia de migração incremental sem tempo de inatividade para uma instância de banco de dados Oracle de vários terabytes que tem um grande número de transações realizadas após a migração inicial e que deve ser migrada para um banco de dados PostgreSQL. Você pode usar essa step-by-step abordagem padrão para migrar incrementalmente uma instância de banco de dados Amazon Relational Database Service (Amazon RDS) para Oracle para uma instância de banco de dados Amazon RDS for PostgreSQL sem entrar no console de gerenciamento da Amazon Web Services (AWS).

O padrão usa o Oracle SQL Developer para encontrar as diferenças entre dois esquemas no banco de dados Oracle de origem. Em seguida, você usa a AWS Schema Conversion Tool (AWS SCT) para converter os objetos do esquema do banco de dados do Amazon RDS para Oracle em objetos do esquema do banco de dados Amazon RDS para PostgreSQL. Então, você pode executar um script Python no prompt de comando do Windows para criar objetos do AWS SCT para as alterações incrementais nos objetos do banco de dados de origem.

> **Note**
>
> Antes de migrar suas cargas de trabalho de produção, recomendamos que você execute uma prova de conceito (PoC) para a abordagem desse padrão em um ambiente de teste ou de não produção.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Instância de banco de dados existente Amazon RDS para Oracle.
- Uma instância existente de banco de dados do Amazon RDS para PostgreSQL.
- AWS SCT, instalada e configurada com drivers JDBC para mecanismos de banco de dados Oracle e PostgreSQL. Para obter mais informações sobre isso, consulte Instalação do AWS SCT e Instalação dos drivers de banco de dados necessários na documentação da AWS SCT.
- Oracle SQL Developer, instalado e configurado. Para obter mais informações sobre isso, consulte a documentação do Oracle SQL Developer.
- O arquivo `incremental-migration-sct-sql.zip` (anexado), baixado no seu computador local.

Limitações

- Os requisitos mínimos para sua instância de banco de dados do Amazon RDS para Oracle de origem são:
  - Oracle versões 10.2 e posteriores (para versões 10.x), 11g (versões 11.2.0.3.v1 e posteriores) e até 12.2 e 18c para as edições Enterprise, Standard, Standard One e Standard Two
- Os requisitos mínimos para sua instância de banco de dados do Amazon RDS para PostgreSQL de origem são:
  - PostgreSQL versões 9.4 e posterior (para versões 9.x), 10.x e 11.x
- Esse padrão usa o Oracle SQL Developer. Seus resultados podem variar se você usar outras ferramentas para encontrar e exportar diferenças de esquema.
- Os scripts SQL gerados pelo Oracle SQL Developer podem gerar erros de transformação, o que significa que você precisa realizar uma migração manual.
- Se as conexões de teste de origem e destino do AWS SCT falharem, certifique-se de configurar as versões do driver JDBC e as regras de entrada para que o grupo de segurança da nuvem privada virtual (VPC) aceite o tráfego de entrada.

Versões do produto

- Instância do banco de dados Amazon RDS para Oracle versão 12.1.0.2 (versão 10.2 e posteriores)
- Instância do banco de dados Amazon RDS para PostgreSQL versão 11.5 (versão 9.4 e posteriores)
- Oracle SQL Developer versão 19.1 e posteriores

- AWS SCT versão 1.0.632 e posteriores

Arquitetura

Pilha de tecnologia de origem

- Instância do banco de dados Amazon RDS para Oracle

Pilha de tecnologias de destino

- instância do banco de dados Amazon RDS para PostgreSQL

Arquitetura de origem e destino

O diagrama a seguir mostra a migração de uma instância de banco de dados Amazon RDS para Oracle para uma instância de banco de dados Amazon RDS para PostgreSQL.

O diagrama mostra o seguinte fluxo de trabalho de migração:

1. Abra o Oracle SQL Developer e conecte-se aos bancos de dados de origem e destino.
2. Gere um relatório de diferença e, em seguida, gere o arquivo de scripts SQL para os objetos de diferença do esquema. Para obter mais informações sobre relatórios de diferença, consulte Relatórios de diferença detalhados na documentação da Oracle.
3. Configure o AWS SCT e execute o código Python.
4. O arquivo de scripts SQL é convertido do Oracle para o PostgreSQL.
5. Execute o arquivo de scripts SQL na instância do banco de dados PostgreSQL de destino.

Automação e escala

Você pode automatizar esta migração incluindo parâmetros adicionais e alterações relacionadas à segurança para várias funcionalidades em um único programa ao seu script do Python.

Ferramentas

- AWS SCT: o AWS Schema Conversion Tool (AWS SCT) converte seu esquema de banco de dados existente de um mecanismo de banco de dados para outro.

- Oracle SQL Developer: o Oracle SQL Developer é um ambiente de desenvolvimento integrado (IDE) que simplifica o desenvolvimento e o gerenciamento de bancos de dados Oracle em implantações tradicionais e baseadas em nuvem.

Código

O arquivo `incremental-migration-sct-sql.zip` (anexo) contém o código-fonte completo para esse padrão.

Épicos

Crie o arquivo de scripts SQL para as diferenças do esquema do banco de dados de origem

Tarefa	Descrição	Habilidades necessárias
Execute Database Diff no Oracle SQL Developer.	1. Faça login na sua instância de banco de dados Oracle de origem, escolha Ferramentas e, em seguida, escolha Relatório de diferenças. 2. Escolha seu banco de dados de origem em Conexão de origem. 3. Escolha o banco de dados de origem atualizado ou corrigido em Conexão de destino. 4. Configure as opções restantes de acordo com seus requisitos, escolha Avançar e, em seguida, escolha Concluir para gerar o relatório de diferença.	DBA

Tarefa	Descrição	Habilidades necessárias
Gere o arquivo de scripts SQL.	Escolha Gerar script para gerar as diferenças nos arquivos SQL. Isso gera o arquivo de scripts SQL que o AWS SCT usa para converter seu banco de dados do Oracle para o PostgreSQL.	DBA

Use o script Python para criar os objetos de banco de dados de destino no AWS SCT

Tarefa	Descrição	Habilidades necessárias
Configure o AWS SCT com o prompt de comando do Windows.	1. Copie o arquivo `AWSSchemaConversionToolBatch.jar` da sua pasta AWS SCT pré-instalada e cole-o em seu diretório de trabalho. 2. Implante o código Python do arquivo `run_aws_sct_sql.py` da pasta `incremental-migration-sct-sql.zip` (anexo). Isso cria arquivos .xml e arquivos .sct no diretório `projects` com os detalhes de configuração do ambiente de banco de dados de origem e de destino. Ele também lê o arquivo de scripts SQL que	DBA

Tarefa	Descrição	Habilidades necessárias

	você gerou no Oracle SQL Developer. Por fim, ele cria objetos de arquivo .sql no diretório `output`.
	3. Configure os detalhes da configuração do ambiente de origem e de destino no arquivo `database_migration.txt` usando o seguinte formato:
	`#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port`
	`ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432`
	4. Modifique os parâmetros de configuração do AWS SCT de acordo com seus requisitos e, em seguida,	

Tarefa	Descrição	Habilidades necessárias
	copie o arquivo de scripts SQL em seu diretório de trabalho no subdiretório `input`.	
Execute o script do Python.	1. Execute o script do Python usando o comando a seguir: `$ python run_aws_sct_sql.py database_migration .txt` 2. Isso cria o arquivo SQL dos objetos de banco de dados. Códigos não convertidos com erros de transform ação podem ser convertid os manualmente.	DBA
Crie os objetos no Amazon RDS para PostgreSQL	Execute os arquivos SQL e crie objetos na sua instância do banco de dados Amazon RDS para PostgreSQL.	DBA

Recursos relacionados

- Oracle no Amazon RDS
- PostgreSQL no Amazon RDS
- Usar a interface de usuário do AWS SCT
- Usar Oracle como origem para AWS SCT

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Faça o upload de arquivos BLOB em TEXT usando a codificação de arquivos no Aurora PostgreSQL-Compatible

Criado por Bhanu Ganesh Gudivada (AWS) e Jeevan Shetty (AWS)

Resumo

Muitas vezes, durante a migração, há casos em que você precisa processar dados estruturados e não estruturados que são carregados a partir de arquivos disponíveis em um sistema local. Os dados também podem estar em um conjunto de caracteres diferente do conjunto de caracteres do banco de dados.

Esses arquivos contêm os seguintes tipos de dados:

- Metadados: esses dados descrevem a estrutura do arquivo.
- Dados semiestruturados: são strings de texto em um formato específico, como JSON ou XML. Talvez você possa fazer afirmações sobre esses dados, como “sempre começará com '<'” ou “não contém nenhum caractere de nova linha”.
- Texto completo: esses dados geralmente contêm todos os tipos de caracteres, incluindo caracteres de nova linha e aspas. Também pode consistir em caracteres de vários bytes em UTF-8.
- Dados binários — esses dados podem conter bytes ou combinações de bytes, incluindo nulos e end-of-file marcadores.

Carregar uma mistura desses tipos de dados pode ser um desafio.

O padrão pode ser usado com bancos de dados Oracle locais, bancos de dados Oracle que estão em instâncias do Amazon Elastic Compute Cloud EC2 (Amazon) na Amazon Web Services (AWS) Cloud e Amazon Relational Database Service (Amazon RDS) para bancos de dados Oracle. Para fins de ilustração, esse padrão está usando o Amazon Aurora Edição Compatível com PostgreSQL.

No banco de dados Oracle, com a ajuda de um ponteiro `BFILE` (arquivo binário), do pacote `DBMS_LOB` e das funções do sistema Oracle, você pode carregar a partir do arquivo e convertê-lo em CLOB com codificação de caracteres. Como o PostgreSQL não fornece suporte para o tipo de dados BLOB ao migrar para um banco de dados Amazon Aurora Edição Compatível com PostgreSQL, essas funções devem ser convertidas em scripts compatíveis com o PostgreSQL.

Esse padrão fornece duas abordagens para carregar um arquivo em uma única coluna de um banco de dados Amazon Aurora compatível com PostgreSQL:

- Abordagem 1 – Você importa dados do bucket do Amazon Simple Storage Service (Amazon S3) usando a função `table_import_from_s3` da extensão `aws_s3` com a opção de codificação.
- Abordagem 2 – Você codifica em hexadecimal fora do banco de dados e, em seguida, decodifica para visualizar `TEXT` dentro do banco de dados.

Recomendamos usar a Abordagem 1 porque o Aurora compatível com PostgreSQL tem integração direta com a extensão `aws_s3`.

Esse padrão usa o exemplo de carregamento de um arquivo simples que contém um modelo de e-mail, caracteres de vários bytes e formatação distinta, em um banco de dados Amazon Aurora compatível com PostgreSQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância do Amazon RDS ou uma instância do Aurora compatível com PostgreSQL
- Uma compreensão básica do SQL e do sistema de gerenciamento de banco de dados relacional (RDBMS)
- Um bucket do Amazon Simple Storage Service (Amazon S3).
- Conhecimento das funções do sistema em Oracle e PostgreSQL
- Pacote RPM HexDump -XXD-0.1.1 (incluído no Amazon Linux 2)

> **Note**
>
> O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs.

Limitações

- Para o tipo de dados `TEXT`, o string de caracteres mais longo possível que pode ser armazenado é de cerca de 1 GB.

Versões do produto

- O Aurora oferece suporte às versões do PostgreSQL listadas nas atualizações do Amazon Aurora PostgreSQL.

Arquitetura

Pilha de tecnologias de destino

- Aurora compatível com PostgreSQL

Arquitetura de destino

Abordagem 1 – Usar aws_s3.table_import_from_s3

A partir de um servidor on-premises, um arquivo contendo um modelo de e-mail com caracteres de vários bytes e formatação personalizada é transferido para o Amazon S3. A função de banco de dados personalizada fornecida por esse padrão usa a função `aws_s3.table_import_from_s3` com `file_encoding` para carregar arquivos no banco de dados e retornar os resultados da consulta como o tipo de dados `TEXT`.

1. Os arquivos são transferidos para o bucket do S3 de preparação.
2. Os arquivos são carregados para o banco de dados Amazon Aurora PostgreSQL-Compatible.
3. Usando o cliente pGAdmin, a função personalizada `load_file_into_clob` é implantada no banco de dados Aurora.
4. A função personalizada usa `table_import_from_s3` internamente com file_encoding. O resultado da função é obtido usando `array_to_string` e `array_agg` como o resultado `TEXT`.

Abordagem 2 – Codificação em hexadecimal fora do banco de dados e, em seguida, decodifica para visualizar TEXT dentro do banco de dados

Um arquivo de um servidor on-premises ou de um sistema de arquivos local é convertido em um hex dump. Em seguida, o arquivo é importado para o PostgreSQL como um campo `TEXT`.

1. Converta o arquivo em um hex dump na linha de comando usando a opção `xxd -p`.
2. Faça upload dos arquivos hex dump no Aurora PostgreSQL-Compatible usando a opção `\copy` e, em seguida, decodifique os arquivos hex dump em binário.

3. Codifique os dados binários para que sejam retornados como TEXT.

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

Outras ferramentas

- O pgAdmin4 é uma plataforma de administração e desenvolvimento de código aberto para o PostgreSQL. O pgAdmin4 pode ser usado em Linux, Unix, mac OS e Windows para gerenciar o PostgreSQL.

Épicos

Abordagem 1: importar dados do Amazon S3 para o Aurora PostgreSQL-Compatible

Tarefa	Descrição	Habilidades necessárias
Execute uma EC2 instância.	Para obter instruções sobre como iniciar uma instância, consulte Executar sua instância.	DBA
Instale a ferramenta pgAdmin do cliente PostgreSQL.	Baixe e instale pgAdmin.	DBA
Crie uma política do IAM.	Crie uma política do AWS Identity and Access Management (IAM) chamada `aurora-s3-access-pol` que concede acesso ao bucket do S3 onde os	DBA

Tarefa	Descrição	Habilidades necessárias
	arquivos serão armazenados. Use o código a seguir, `<bucket-name>` para substituir pelo nome do bucket do S3. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject", "s3:AbortMultipartUpload", "s3:DeleteObject", "s3:ListMultipartUploadParts", "s3:PutObject", "s3:ListBucket" ], "Resource": [ "arn:aws:s3:::<bucket-name>/*", "arn:aws:s3:::<bucket-name>" ] } ]`	

Tarefa	Descrição	Habilidades necessárias
	`}`	
Crie um perfil do IAM para importação de objetos do Amazon S3 para o Aurora PostgreSQL-Compatible.	Use o código a seguir para criar uma função do IAM chamada `aurora-s3-import-role` com a relação de AssumeRole confiança. `AssumeRole` permite que a Aurora acesse outros serviços da AWS em seu nome. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow","Principal": { "Service": "rds.amazonaws.com" },"Action": "sts:AssumeRole" } ] }`	DBA

Tarefa	Descrição	Habilidades necessárias
Associe o perfil do IAM ao cluster.	Para associar o perfil do IAM ao cluster do banco de dados Aurora PostgreSQL-Compatible, execute o comando da AWS CLI a seguir. Altere `<Account-ID>` para o ID da conta da AWS que hospeda o banco de dados Aurora PostgreSQL-Compatible. Isso permite que o banco de dados Aurora PostgreSQL-Compatible acesse o bucket do S3. `aws rds add-role-to-db-cluster --db-cluster-identifier aurora-postgres-cl --feature-name s3Import --role-arn arn:aws:iam::<Account-ID>:role/aurora-s3-import-role`	DBA
Faça o upload do exemplo para o Amazon S3.	1. Na seção Informações adicionais desse padrão, copie o código do modelo de e-mail em um arquivo chamado `salary.event.notification.email.vm` . 2. Faça upload do arquivo no bucket do S3.	DBA, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Implante a função personalizada.	1. Na seção Informações adicionais, copie o conteúdo do arquivo SQL `load_file_into_clob` da função personalizada em uma tabela temporária. 2. Faça login no banco de dados Aurora PostgreSQL-Compatible e implante-o no esquema do banco de dados usando o cliente pgAdmin.	Proprietário do aplicativo, DBA

Tarefa	Descrição	Habilidades necessárias

Execute a função personalizada para importar os dados para o banco de dados.	Execute o comando SQL a seguir, substituindo os itens entre parênteses angulares pelos valores apropriados.
	`select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	Substitua os itens entre parênteses angulares pelos valores apropriados, conforme mostrado no exemplo a seguir, antes de executar o comando.
	`Select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	O comando carrega o arquivo do Amazon S3 e retorna o resultado como TEXT.
		Proprietário do aplicativo, DBA

Abordagem 2: converter o arquivo de modelo em um hex dump em um sistema Linux local

Tarefa	Descrição	Habilidades necessárias
Converta o arquivo do modelo em um hex dump.	**Note** O utilitário Hexdump exibe o conteúdo dos arquivos binários em hexadecimal, decimal, octal ou ASCII. O comando `hexdump` faz parte do pacote `util-linux` e vem pré-instalado nas distribuições Linux. O pacote Hexdump RPM também faz parte do Amazon Linux 2. (: O suporte do Amazon Linux 2 está chegando ao fim. Para obter mais informações, consulte o Amazon Linux 2 FAQs.) Para converter o conteúdo do arquivo em um hex dump, execute o seguinte comando shell. `xxd -p </path/file.vm> | tr -d '\n' > </path/file.hex>`	DBA

Tarefa	Descrição	Habilidades necessárias
	Substitua o caminho e o arquivo pelos valores apropriados, conforme mostrado no exemplo a seguir. `xxd -p employee.salary.event.notification.email.vm | tr -d '\n' > employee.salary.event.notification.email.vm.hex`	

Tarefa	Descrição	Habilidades necessárias
Carregue o arquivo hexdump no esquema do banco de dados.	Use os comandos a seguir para carregar o arquivo hexdump no banco de dados Aurora PostgreSQL-Compatible. 1. Faça login no banco de dados Aurora PostgreSQL e crie uma nova tabela chamada `email_template_hex` . ``` CREATE TABLE email_template_hex(hex_data TEXT); ``` 2. Carregue os arquivos do sistema de arquivos local no esquema do banco de dados usando o comando a seguir. ``` \copy email_template_hex FROM '/path/file.hex'; ``` Substitua o caminho pelo local em seu sistema de arquivos local. ``` \copy email_template_hex FROM '/tmp/employee.salary.event.notification.email.vm.hex'; ```	DBA

Tarefa	Descrição	Habilidades necessárias

	3. Crie mais uma tabela chamada `email_template_bytea` .
	`CREATE TABLE email_template_bytea(hex_data bytea);`
	4. Insira os dados de `email_template_hex` em `email_template_bytea` .
	`INSERT INTO email_template_bytea (hex_data)`
	`(SELECT decode(hex_data, 'hex') FROM email_template_hex limit 1);`
	5. Para retornar código hexadecimal bytea como dados TEXT, execute o comando a seguir.
	`SELECT encode(hex_data::bytea, 'escape') FROM email_template_bytea;`	

Recursos relacionados

Referências

- Uso do banco de dados PostgreSQL como origem para o AWS Database Migration Service

- Manual de migração do Oracle Database 19c para o Amazon Aurora com compatibilidade com PostgreSQL (12.4)
- Criação de políticas do IAM
- Associar um perfil do IAM a um cluster de banco de dados do Amazon Aurora MySQL
- pgAdmin

Tutoriais

- Conceitos básicos do Amazon RDS
- Migre do Oracle para o Amazon Aurora

Mais informações

função personalizada load_file_into_clob

```
CREATE OR REPLACE FUNCTION load_file_into_clob(
    s3_bucket_name text,
    s3_bucket_region text,
    file_name text,
    file_delimiter character DEFAULT '&'::bpchar,
    file_encoding text DEFAULT 'UTF8'::text)
    RETURNS text
    LANGUAGE 'plpgsql'
    COST 100
    VOLATILE PARALLEL UNSAFE
AS $BODY$
DECLARE
    blob_data BYTEA;
    clob_data TEXT;
    l_table_name CHARACTER VARYING(50) := 'file_upload_hex';
    l_column_name CHARACTER VARYING(50) := 'template';
    l_return_text TEXT;
    l_option_text CHARACTER VARYING(150);
    l_sql_stmt CHARACTER VARYING(500);

BEGIN

    EXECUTE format ('CREATE TEMPORARY TABLE %I (%I text, id_serial serial)',
 l_table_name, l_column_name);
```

```
    l_sql_stmt := 'select ''(format text, delimiter ''''' || file_delimiter || ''''',
 encoding ''''' || file_encoding ||  ''''')'' ';

    EXECUTE FORMAT(l_sql_stmt)
    INTO l_option_text;

    EXECUTE FORMAT('SELECT aws_s3.table_import_from_s3($1,$2,$6,
 aws_commons.create_s3_uri($3,$4,$5))')
    INTO l_return_text
    USING l_table_name, l_column_name, s3_bucket_name,
 file_name,s3_bucket_region,l_option_text;

    EXECUTE format('select array_to_string(array_agg(%I order by id_serial),E''\n'')
 from %I', l_column_name, l_table_name)
    INTO clob_data;

    drop table file_upload_hex;

    RETURN clob_data;
END;
$BODY$;
```

Modelo de e-mail

```
##############################################################################################
##
 ##
##    johndoe Template Type: email
 ##
##    File: johndoe.salary.event.notification.email.vm
 ##
##    Author: Aimée Étienne    Date 1/10/2021
      ##
##  Purpose: Email template used by EmplmanagerEJB to inform a johndoe they         ##
##        have been given access to a salary event
 ##
##    Template Attributes:
 ##
##        invitedUser - PersonDetails object for the invited user
  ##
##        salaryEvent - OfferDetails object for the event the user was given access
 ##
```

```
##        buyercollege - CompDetails object for the college owning the salary event
 ##
##        salaryCoordinator - PersonDetails of the salary coordinator for the event
 ##
##        idp - Identity Provider of the email recipient
 ##
##        httpWebRoot - HTTP address of the server
 ##
##
 ##
#################################################################################

$!invitedUser.firstname $!invitedUser.lastname,

Ce courriel confirme que vous avez ete invite par $!salaryCoordinator.firstname $!
salaryCoordinator.lastname de $buyercollege.collegeName a participer a l'evenement
 "$salaryEvent.offeringtitle" sur johndoeMaster Sourcing Intelligence.

Votre nom d'utilisateur est $!invitedUser.username

Veuillez suivre le lien ci-dessous pour acceder a l'evenement.

${httpWebRoot}/myDashboard.do?idp=$!{idp}

Si vous avez oublie votre mot de passe, utilisez le lien "Mot de passe oublie" situe
 sur l'ecran de connexion et entrez votre nom d'utilisateur ci-dessus.

Si vous avez des questions ou des preoccupations, nous vous invitons a
 communiquer avec le coordonnateur de l'evenement $!salaryCoordinator.firstname $!
salaryCoordinator.lastname au ${salaryCoordinator.workphone}.

*******

johndoeMaster Sourcing Intelligence est une plateforme de soumission en ligne pour les
 equipements, les materiaux et les services.

Si vous avez des difficultes ou des questions, envoyez un courriel a
 support@johndoeMaster.com pour obtenir de l'aide.
```

Migre o Amazon RDS for Oracle para o Amazon AWS SCT RDS for PostgreSQL com e usando e AWS DMSAWS CLIAWS CloudFormation

Criado por Pinesh Singal (AWS)

Resumo

Esse padrão mostra como migrar uma instância de banco de dados Amazon Relational Database Service (Amazon RDS) for Oracle de vários terabytes para uma instância de banco de dados Amazon RDS for PostgreSQL usando o (). AWS Command Line Interface AWS CLI A abordagem fornece um tempo de inatividade mínimo e não exige login no AWS Management Console.

Esse padrão ajuda a evitar configurações manuais e migrações individuais usando os consoles AWS Schema Conversion Tool (AWS SCT) e AWS Database Migration Service (AWS DMS). A solução configura uma configuração única para vários bancos de dados e executa as migrações usando AWS SCT e AWS DMS no. AWS CLI

O padrão é usado AWS SCT para converter objetos do esquema de banco de dados do Amazon RDS para Oracle para o Amazon RDS for PostgreSQL e, em seguida, é usado para migrar os dados. AWS DMS Usando scripts Python em AWS CLI, você cria AWS SCT objetos e AWS DMS tarefas com um AWS CloudFormation modelo.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Instância de banco de dados existente Amazon RDS para Oracle.
- Uma instância existente de banco de dados do Amazon RDS para PostgreSQL.
- Uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou máquina local com sistema operacional Windows ou Linux para execução de scripts.
- Uma compreensão dos seguintes tipos de tarefas de AWS DMS migração:`full-load`,`cdc`,`full-load-and-cdc`. Para obter mais informações, consulte Criação de uma tarefa na AWS DMS documentação.
- AWS SCT, instalado e configurado com drivers Java Database Connectivity (JDBC) para mecanismos de banco de dados Oracle e PostgreSQL. Para obter mais informações, consulte Instalação e configuração AWS SCT na AWS SCT documentação.
- O `AWSSchemaConversionToolBatch.jar` arquivo da AWS SCT pasta instalada, copiado para o seu diretório de trabalho.

- O arquivo `cli-sct-dms-cft.zip` (anexo), baixado e extraído em seu diretório de trabalho.
- A versão mais recente do mecanismo AWS DMS de instância de replicação. Para obter mais informações, consulte Como faço para criar uma instância de AWS DMS replicação na AWS Support documentação e nas notas de AWS DMS versão.
- AWS CLI versão 2, instalada e configurada com seu ID de chave de acesso, chave de acesso secreta e Região da AWS nome padrão para a EC2 instância ou sistema operacional em que os scripts são executados. Para obter mais informações, consulte Instalando ou atualizando para a versão mais recente do AWS CLI e Definindo as configurações do AWS CLI na AWS CLI documentação.
- Familiaridade com AWS CloudFormation modelos. Para obter mais informações, consulte Como AWS CloudFormation funciona na AWS CloudFormation documentação.
- Python versão 3, instalado e configurado na EC2 instância ou no sistema operacional em que os scripts são executados. Para obter mais informações, consulte a documentação do Python.

Limitações

- Os requisitos mínimos para sua instância de banco de dados do Amazon RDS para Oracle de origem são:
  - Versões 12c (12.1.0.2, 12.2.0.1), 18c (18.0.0.0) e 19c (19.0.0.0) da Oracle para as edições Enterprise, Standard, Standard One e Standard Two.
  - Embora o Amazon RDS ofereça suporte ao Oracle 18c (18.0.0.0), essa versão está em um caminho de descontinuação porque a Oracle não fornece mais patches para 18c após a data. end-of-support Para obter mais informações, consulte o Amazon RDS para Oracle na documentação do Amazon RDS.
  - O Amazon RDS para Oracle 11g não é mais compatível.
- Os requisitos mínimos para sua instância de banco de dados do Amazon RDS para PostgreSQL de origem são:
  - Versões 9 (9.5 e 9.6), 10.x, 11.x, 12.x e 13.x do PostgreSQL

Versões do produto

- Instância do banco de dados Amazon RDS para Oracle versão 12.1.0.2 e posteriores
- Instância do banco de dados Amazon RDS para PostgreSQL versão 11.5 e posteriores
- AWS CLI versão 2

- A versão mais recente do AWS SCT
- A versão mais recente do Python 3

Arquitetura

Pilha de tecnologia de origem

- Amazon RDS para Oracle

Pilha de tecnologias de destino

- Amazon RDS para PostgreSQL

Arquitetura de origem e destino

O diagrama a seguir mostra a migração de uma instância de banco de dados Amazon RDS for Oracle para uma instância de banco de dados Amazon RDS for PostgreSQL AWS DMS usando scripts Python.

O diagrama mostra o seguinte fluxo de trabalho de migração:

1. O script Python é usado AWS SCT para se conectar às instâncias de banco de dados de origem e de destino.
2. O usuário começa AWS SCT com o script Python, converte o código Oracle em código PostgreSQL e o executa na instância de banco de dados de destino.
3. O script Python cria tarefas de AWS DMS replicação para as instâncias de banco de dados de origem e de destino.
4. O usuário implanta scripts Python para iniciar as tarefas e, em seguida, interrompe AWS DMS as tarefas após a conclusão da migração de dados.

Automação e escala

Você pode automatizar essa migração adicionando parâmetros e alterações relacionadas à segurança ao seu script Python para fornecer funcionalidades adicionais.

Ferramentas

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir com os serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS CloudFormationajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los em todo o seu ciclo de vida em todas Contas da AWS as regiões. Esse padrão converte o arquivo `.csv` de entrada em um arquivo `.json` de entrada usando um script Python. O `.json` arquivo é usado em AWS CLI comandos para criar uma AWS CloudFormation pilha que cria várias tarefas de AWS DMS replicação com Amazon Resource Names (ARNs), tipos de migração, configurações de tarefas e mapeamentos de tabelas.
- AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para Nuvem AWS ou entre combinações de configurações na nuvem e no local. Esse padrão é usado AWS DMS para criar, iniciar e interromper tarefas com um script Python executado na linha de comando e para criar o AWS CloudFormation modelo.
- AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino. Esse padrão requer o `AWSSchemaConversionToolBatch.jar` arquivo do AWS SCT diretório instalado.

Código

O arquivo `cli-sct-dms-cft.zip` (anexo) contém o código-fonte completo para esse padrão.

Épicos

Configure AWS SCT e crie objetos de banco de dados no AWS CLI

Tarefa	Descrição	Habilidades necessárias
Configure AWS SCT para ser executado a partir do AWS CLI.	1. Configure os detalhes da configuração do ambiente de origem e de destino no arquivo `database_migration.txt` usando o seguinte formato:	DBA

Tarefa	Descrição	Habilidades necessárias

	<pre>#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port
	ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432</pre> 2. Modifique os parâmetros de AWS SCT configuração de acordo com seus requisitos nos seguintes arquivos: `project_settings.xml` `Oracle_PG_Test_Batch.xml` , `ORACLE-orcl-to-POSTGRESQL.xml` e.	

Tarefa	Descrição	Habilidades necessárias
Execute o `run_aws_sct.py` script Python.	Execute o script `run_aws_sct.py` do Python usando o comando a seguir: `$ python run_aws_sct.py database_migration.txt` O script do Python converte os objetos do banco de dados do Oracle para o PostgreSQL e cria arquivos SQL no formato PostgreSQL. O script também cria o arquivo PDF`Database migration assessment report` , que fornece recomendações detalhadas e estatísticas de conversão para objetos de banco de dados.	DBA
Crie objetos no Amazon RDS para PostgreSQL.	1. Modifique manualmente os arquivos SQL gerados pelo AWS SCT, se necessário. 2. Execute os arquivos SQL e crie objetos na sua instância do banco de dados Amazon RDS para PostgreSQL.	DBA

Configure e crie AWS DMS tarefas usando o AWS CLI e AWS CloudFormation

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de AWS DMS replicação.	Faça login no AWS Management Console, abra	DBA

Tarefa	Descrição	Habilidades necessárias
	o AWS DMS console e crie uma instância de replicação configurada de acordo com seus requisitos. Para obter mais informaçõ es, consulte Criação de uma instância de replicaçã o na AWS DMS documenta ção e Como faço para criar uma instância de AWS DMS replicação na AWS Support documentação.	
Crie um endpoint de origem.	No AWS DMS console, escolha Endpoints e, em seguida, crie um endpoint de origem para o banco de dados Oracle de acordo com seus requisitos. **Note** O atributo de conexão extra deve estar `numberDat aTypeScale` com um `-2` valor. Para obter mais informações, consulte Criação de endpoints de origem e destino na AWS DMS documentação.	DBA

Tarefa	Descrição	Habilidades necessárias
Crie um endpoint de destino.	No AWS DMS console, escolha Endpoints e, em seguida, crie um endpoint de destino para o banco de dados PostgreSQL de acordo com seus requisitos. Para obter mais informações, consulte Criação de endpoints de origem e destino na AWS DMS documentação.	DevOps engenheiro

Configure os detalhes da AWS DMS replicação para serem executados a partir do AWS CLI.	Configure os endpoints de AWS DMS origem e de destino e os detalhes da replicação no `dms-arn-list.txt` arquivo com o ARN do endpoint de origem, o ARN do endpoint de destino e o ARN da instância de replicação usando o seguinte formato:
	
	`#sourceARN,targetARN,repARN`
	`arn:aws:dms:us-east-1:123456789012:endpoint:EH7AINRUDZ5GOYIY6HVMXECMCQ`
	`arn:aws:dms:us-east-1:123456789012:endpoint:HHJVUV57N7O3CQF4PJZKGIOYY5`
	`arn:aws:dms:us-east-1:123456789012:rep:LL57N77AQQAHHJF4PJFHNEDZ5G`
		DBA

Tarefa	Descrição	Habilidades necessárias
Execute o script `dms-create-task.py` Python para criar as AWS DMS tarefas.	1. Execute o script `dms-create-task.py` do Python usando o comando a seguir: `$ python dms-create-task.py database_migration.txt dms-arn-list.txt <cft-stack-name> <migration-type>` em que: • `database_migration.txt` é o arquivo de texto de migração do banco de dados. • `dms-arn-list.txt` é a lista de ARN para. AWS DMS • `<cft-stack-name>` é o nome da AWS CloudFormation pilha definido pelo usuário. • `<migration-type>` é `full-load` , `cdc` ou `full-load-and-cdc` . 2. Dependendo do tipo de migração, você pode usar os seguintes comandos para criar três tipos de AWS DMS tarefas: • `$ python dms-create-task.py`	DBA

Tarefa	Descrição	Habilidades necessárias
	`database_migration .txt dms-arn-l ist.txt dms-cli-c ft-stack full-load` • `$ python dms- create-task.py database_migration .txt dms-arn-l ist.txt dms-cli-c ft-stack cdc` • `$ python dms- create-task.py database_migration .txt dms-arn-l ist.txt dms-cli-c ft-stack full-load -and-cdc`	
Verifique se as AWS DMS tarefas estão prontas.	No AWS DMS console, verifique se suas AWS DMS tarefas estão em `Ready` status na seção Status.	DBA

Inicie e interrompa as AWS DMS tarefas usando o AWS CLI

Tarefa	Descrição	Habilidades necessárias
Inicie as AWS DMS tarefas.	Execute o script `dms-start -task.py` do Python usando o comando a seguir:	DBA

Tarefa	Descrição	Habilidades necessárias
	`$ python dms-start-task.py start '<cdc-start-datetime>'` **Note** A data e a hora de início devem estar no `'YYYY-MM-DDTHH:MI:SS'` formato `'DD-MON-YYYY'` ou (por exemplo, `'01-Dec-2019'` ou `'2018-03-08T12:12:12'`). Você pode revisar o status da AWS DMS tarefa na guia Estatísticas da tabela na página Tarefas do AWS DMS console.	

Tarefa	Descrição	Habilidades necessárias
Valide os dados.	1. Após a conclusão da migração de carga total, a tarefa é mantida em execução contínua para o CDC. 2. Quando a CDC estiver concluída ou nenhuma outra alteração precisar ser migrada, revise e valide os resultados e os dados da tarefa de migração em seus bancos de dados Oracle e PostgreSQL. Você pode validar seus dados verificando o status e as colunas de contagem (`Validation state` ,`Validation pending` , `Validation failed` `Validation suspended` , `eValidation details`) na guia Estatísticas da tabela da tarefa de migração do banco de dados na página Tarefas do AWS DMS console. Para obter mais informações, consulte a validação de AWS DMS dados na AWS DMS documentação.	DBA

Tarefa	Descrição	Habilidades necessárias
Pare as AWS DMS tarefas.	Execute o script do Python usando o comando a seguir: `$ python dms-start-task.py stop` **Note** AWS DMS as tarefas podem parar com um `failed` status, dependendo do status de validação. Para obter mais informaçõ es, consulte a próxima seção.	DBA

Solução de problemas

Problema	Solução
AWS SCT as conexões de teste de origem e destino falham.	Configure as versões do driver JDBC e as regras de entrada do grupo de segurança da VPC para aceitar o tráfego de entrada.
Falha na execução do teste do endpoint de origem ou destino.	Verifique se as configurações do endpoint e a instância de replicação estão em `Available` status. Verifique se o status da conexão do endpoint é `Successful` . Para obter mais informações, consulte Como soluciono falhas de conectividade de endpoints do AWS DMS na documentação. AWS Support

Problema	Solução
Falha na execução com carga total.	Verifique se os bancos de dados de origem e de destino têm tipos e tamanhos de dados correspondentes. Para obter mais informações, consulte Solução de problemas de tarefas de migração AWS DMS na AWS DMS documentação.
Você encontra erros de execução de validação.	Verifique se a tabela tem uma chave primária porque as tabelas de chave não primária não estão validadas. Se a tabela tiver uma chave primária, mas retornar erros, verifique o atributo de conexão extra no endpoint de origem tem `numberDataTypeScale=-2` . Para obter mais informações, consulte Configurações do endpoint ao usar o Oracle como fonte e Solução de problemas na AWS DMS documentação. AWS DMSOracleSettings

Recursos relacionados

- Instalando e configurando AWS SCT
- Introdução ao AWS DMS (vídeo)
- Exemplos de comandos de operação de CloudFormation pilha para e AWS CLI PowerShell
- Navegando pela interface do usuário do AWS SCT
- Usando um banco de dados Oracle como fonte para AWS DMS
- Conectando-se aos bancos de dados Oracle com AWS SCT
- Usando um banco de dados PostgreSQL como alvo para AWS DMS
- Origens para a migração de dados
- Destinos para a migração de dados
- cloudformation (documentação)AWS CLI

- create-stack (documentação)AWS CLI
- dms (AWS CLI documentação)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre o Amazon RDS para Oracle para o Amazon RDS para PostgreSQL no modo SSL usando o AWS DMS

Criado por Pinesh Singal (AWS)

Resumo

Este padrão fornece orientação para migração de uma instância do banco de dados Amazon Relational Database Service (Amazon RDS) para Oracle para um banco de dados do Amazon RDS para PostgreSQL na nuvem da Amazon Web Services (AWS). Para criptografar conexões entre os bancos de dados, o padrão usa autoridade de certificação (CA) e modo SSL no Amazon RDS e no AWS Database Migration Service (AWS DMS).

O padrão descreve uma estratégia de migração on-line com pouco ou nenhum tempo de inatividade para um banco de dados de origem Oracle de vários terabytes com um grande número de transações. Visando à segurança dos dados, o padrão usa SSL ao transferir os dados.

Esse padrão usa o AWS Schema Conversion Tool (AWS SCT) para converter o esquema de banco de dados Amazon RDS para Oracle em um esquema do Amazon RDS para PostgreSQL. Em seguida, o padrão usa o AWS DMS para migrar dados do banco de dados Amazon RDS para Oracle para o banco de dados Amazon RDS para PostgreSQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Autoridade de certificação (CA) do banco de dados Amazon RDS configurada somente com rds-ca-rsa2048-g1
  - O certificado rds-ca-2019 expirou em agosto de 2024.
  - O certificado rds-ca-2015 expirou em 5 de março de 2020.
- AWS SCT
- AWS DMS
- pgAdmin
- Ferramentas SQL (por exemplo, SQL Developer ou SQL*Plus)

Limitações

- Banco de dados Amazon RDS para Oracle: o requisito mínimo é para as versões 19c da Oracle para as edições Enterprise e Standard Two.
- Banco de dados Amazon RDS para PostgreSQL: o requisito mínimo é para o PostgreSQL versão 12 e posterior (para versões 9.x e posteriores).

Versões do produto

- Instância do banco de dados Amazon RDS para Oracle versão 12.1.0.2
- Instância do banco de dados Amazon RDS para PostgreSQL versão 11.5

Arquitetura

Pilha de tecnologia de origem

- Instância de banco de dados Amazon RDS para Oracle versão 12.1.0.2.v18.

Pilha de tecnologias de destino

- AWS DMS
- Instância de banco de dados Amazon RDS para PostgreSQL versão 11.5.

Arquitetura de destino

O diagrama a seguir mostra a arquitetura da arquitetura de migração de dados entre os bancos de dados Oracle (origem) e PostgreSQL (destino). A arquitetura inclui o seguinte:

- Uma nuvem privada virtual (VPC)
- Uma zona de disponibilidade
- Uma sub-rede privada
- Um banco de dados Amazon RDS para Oracle
- Uma instância de replicação do AWS DMS
- Um banco de dados RDS para PostgreSQL

Para criptografar conexões para bancos de dados de origem e destino, os modos CA e SSL devem estar habilitados no Amazon RDS e no AWS DMS.

Ferramentas

Serviços da AWS

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O Amazon Relational Database Service (Amazon RDS) para Oracle ajuda você a configurar, operar e escalar um banco de dados relacional Oracle na Nuvem AWS.
- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.
- O AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.

Outros serviços

- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.

Práticas recomendadas

OAmazon RDS fornece novos certificados CA como uma prática recomendada de segurança daAWS. Para obter informações sobre os novos certificados e as regiões compatíveis da AWS, consulte Como usar SSL/TLS para criptografar uma conexão com uma instância de banco de dados ou cluster.

Se sua instância do RDS estiver atualmente no certificado `rds-ca-2019` CA e você quiser fazer o upgrade para`rds-ca-rsa2048-g1`, siga as instruções em Atualizando seu certificado de CA modificando sua instância de banco de dados ou cluster ou Atualizando seu certificado de CA aplicando manutenção.

Épicos

Configurar a instância do Amazon RDS para Oracle

Tarefa	Descrição	Habilidades necessárias
Crie a instância do banco de dados Oracle.	Faça login em sua conta AWS, abra o Console de Gerenciamento da AWS e navegue até o console do Amazon RDS. No console, escolha Criar banco de dados e, em seguida, Oracle.	AWS, DBA geral
Configurar grupos de segurança.	Configurar grupos de segurança de entrada e saída.	AWS geral
Crie um grupo de opções.	Crie um grupo de opções na mesma VPC e no mesmo grupo de segurança do banco de dados Amazon RDS para Oracle. Em Opção, escolha SSL. Em Porta, escolha 2484 (para conexões SSL).	AWS geral
Defina as configurações da opção.	Use as seguintes configurações: • `SQLNET.CIPHER_SUITE : SSL_RSA_WITH_AES_256_CBC_SHA` • `SQLNET.SSL_VERSION : 1.2 or 1.0`	AWS geral
Modifique a instância do banco de dados RDS para Oracle.	Defina o certificado CA como rds-ca-rsa2048-g1.	AWS, DBA geral

Tarefa	Descrição	Habilidades necessárias
	Em Grupo de opções, anexe o grupo de opções criado anteriormente.	

Tarefa	Descrição	Habilidades necessárias

Confirme se a instância do banco de dados RDS para Oracle está disponível.	Certifique-se de que a instância do banco de dados Amazon RDS para Oracle esteja em execução e que o esquema do banco de dados esteja acessível.
	
	Para se conectar ao banco de dados RDS para Oracle, use o comando `sqlplus` da linha de comando.
	
	`$ sqlplus orcl/**** @myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com:1521/ORCL`
	`SQL*Plus: Release 12.1.0.2.0 Production on Tue Oct 15 18:11:07 2019`
	`Copyright (c) 1982, 2016, Oracle. All rights reserved.`
	`Last Successful login time: Mon Dec 16 2019 23:17:31 +05:30`
	`Connected to:`
	`Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production`
	`With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options`
	`SQL>`
		DBA

Tarefa	Descrição	Habilidades necessárias
Crie objetos e dados no banco de dados RDS para Oracle.	Crie objetos e insira dados no esquema.	DBA

Configure a instância do Amazon RDS para PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Crie o banco de dados RDS para PostgreSQL.	Na página Criar banco de dados do console do Amazon RDS, escolha PostgreSQL para criar uma instância do banco de dados Amazon RDS para PostgreSQL.	AWS, DBA geral
Configurar grupos de segurança.	Configurar grupos de segurança de entrada e saída.	AWS geral
Criar um grupo de parâmetros.	Se você estiver usando a versão 11.x do PostgreSQL, crie um grupo de parâmetro s para definir os parâmetro s SSL. Na versão 12 do PostgreSQL, o grupo de parâmetros SSL é ativado por padrão.	AWS geral
Edite os parâmetros.	Altere o parâmetro `rds.force_ssl` para `1` (ativado). Por padrão, o parâmetro `ssl` é 1 (ativado). Ao definir o parâmetro `rds.force_ssl` como 1, você força todas as	AWS geral

Tarefa	Descrição	Habilidades necessárias
	conexões a se conectarem somente pelo modo SSL.	
Modifique a instância de banco de dados do RDS para PostgreSQL.	Defina o certificado CA como rds-ca-rsa2048-g1. Anexe o grupo de parâmetros padrão ou o grupo de parâmetros criado anteriormente, dependendo da sua versão do PostgreSQL.	AWS, DBA geral

Tarefa	Descrição	Habilidades necessárias

Confirme se a instância do banco de dados RDS para Oracle está disponível.	Certifique-se de que o banco de dados Amazon RDS para PostgreSQL esteja em execução.
	
	O comando `psql` estabelece uma conexão SSL com `sslmode` definido na linha de comando.
	
	Uma opção é definir `sslmode=1` no grupo de parâmetros e usar uma conexão `psql` sem incluir o parâmetro `sslmode` no comando.
	
	O resultado a seguir mostra que a conexão SSL foi estabelecida.
	
	`$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser"`
	`Password for user pguser:`
	`psql (11.3, server 11.5)`
	`SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)`
	`Type "help" for help.`
		DBA

Tarefa	Descrição	Habilidades necessárias
	pgdb=> Uma segunda opção é definir `sslmode=1` no grupo de parâmetros e incluir o parâmetro `sslmode` no comando `psql`. O resultado a seguir mostra que a conexão SSL foi estabelecida. `$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser sslmode=require" Password for user pguser: psql (11.3, server 11.5) SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off) Type "help" for help. pgdb=>`	

Configurar e executar o AWS SCT

Tarefa	Descrição	Habilidades necessárias
Instale a AWS SCT.	Instale a versão mais recente do aplicativo AWS SCT.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Configure o AWS SCT com drivers JDBC.	Baixe os drivers Java Database Connectivity (JDBC) para Oracle (ojdbc8.jar) e PostgreSQL (postgresql-42.2.5.jar). Para configurar os drivers no AWS SCT, escolha Configurações, Configurações globais e Drivers.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie um projeto AWS SCT.	Crie o projeto e o relatório do AWS SCT usando o Oracle como o mecanismo de banco de dados de origem e o Amazon RDS para PostgreSQL como o mecanismo de banco de dados de destino: 1. Teste as conexões com o banco de dados Oracle de origem e o banco de dados Amazon RDS para PostgreSQL de destino fornecendo detalhes da conexão. Para o banco de dados Oracle de origem, as permissões ou os privilégios a seguir são necessários: • `CONNECT` • `SELECT_CATALOG_ROLE` • `SELECT ANY DICTIONARY` • `SELECT on SYS.USER$ TO <sct_user>` Para obter mais informações, consulte Uso de um banco de dados Oracle como para AWS SCT.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	As conexões de origem e de destino devem ser bem-sucedidas antes que o AWS SCT possa iniciar o relatório de migração. 2. Depois do relatório, insira o esquema a ser convertido e escolha Finalizar.	

Tarefa	Descrição	Habilidades necessárias
Valide objetos do banco de dados.	1. Escolha Carregar esquema. O AWS SCT exibe os objetos da origem e do destino convertidos, incluindo objetos com erros. Atualize os objetos incorretos no banco de dados de destino. 2. Analise os erros e elimine-os por meio de intervenção manual. 3. Depois que todos os erros forem eliminados, escolha Carregar esquema novamente. 4. Escolha Aplicar ao banco de dados. 5. Conecte-se ao pgAdmin ou a qualquer ferrament a que ofereça suporte a uma conexão do banco de dados PostgreSQL e verifique o esquema e os objetos.	AWS, DBA geral

Configurar e executar o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Criação de uma instância de replicação.	1. Faça login em sua conta, abra o Console de Gerenciamento da AWS e	AWS geral

Tarefa	Descrição	Habilidades necessárias
	navegue até o console do Amazon DMS. 2. Crie uma instância de replicação com configurações válidas para VPC, grupo de segurança, zona de disponibilidade e atributos extras de conexão.	
Importar o certificado.	Baixe o pacote de certificados (PEM) para sua região da AWS. O pacote contém os certificados intermediário e raiz do `rds-ca-2019` . O pacote também contém os certificados CA raiz do `rds-ca-rsa2048-g1` , do `rds-ca-rsa4096-g1` e do `rds-ca-ecc384-g1` . Seu repositório confiável de aplicativos precisa registrar somente o certificado CA raiz.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie um endpoint de origem.	1. Crie um endpoint de origem para o Amazon RDS para Oracle escolhendo Selecionar instância do banco de dados RDS e, em seguida, seleciona ndo a instância do banco de dados RDS para Oracle que você criou. Os detalhes da configura ção do endpoint serão preenchidos automatic amente. 2. Escolha Fornecer informaçõ es de acesso manualmente. Em Porta, certifique-se de inserir 2484. 3. No modo Secure Socket Layer (SSL), escolha `everify-ca` , em seguida, escolha o certifica do CA que você criou anteriormente. 4. Em Configurações do endpoint, adicione o atributo `NumberDat aTypeScale=-2` de conexão extra para fornecer suporte ao tipo de dados `NUMBER` sem restrição de tamanho.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte Uso de um banco de dados do Oracle como origem do AWS Database Migration Service.	
Crie um endpoint de destino.	1. Crie um endpoint de destino para o Amazon RDS para PostgreSQL escolhendo Seleciona r instância do banco de dados RDS e, em seguida, selecionando a instância do banco de dados RDS para PostgreSQL. Os detalhes da configura ção do endpoint serão preenchidos automatic amente. 2. Escolha Fornecer informaçõ es de acesso manualmente. Em Porta, certifique-se de inserir 2484. Para obter mais informações, consulte Uso de um banco de dados do PostgreSQL como destino do AWS Database Migration Service.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Testar os endpoints.	1. Teste os endpoints de origem e de destino para confirmar se ambos foram bem-sucedidos e estão disponíveis. 2. Se um teste falhar, verifique se as regras de entrada do grupo de segurança são válidas.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Criar tarefas de migração.	Para criar uma tarefa de migração para carga total e captura de dados de alteração (CDC) ou para validação de dados, faça o seguinte: 1. Para criar uma tarefa de migração de banco de dados, escolha a instância de replicação, o endpoint do banco de dados de origem e o endpoint do banco de dados de destino. Especifique o tipo de migração como uma das seguintes opções: • Migrar dados existentes (carga total) • Replicação somente de alterações de dados (CDC) • Migração de dados existentes e replicação de alterações contínuas (carga total e CDC) 2. Em Mapeamentos de tabela, você pode configura r regras de seleção e de transformação nos formatos GUI ou JSON: • Em Regras de seleção, selecione o esquema, insira o nome da tabela e selecione a ação	AWS geral

Tarefa	Descrição	Habilidades necessárias
	(incluir ou excluir) a ser configurada; por exemplo, Esquema ORCL, Nome da tabela %, Inclusão da ação. • Em Regras de transform ação, siga um destes procedimentos: • Selecione o esquema e escolha a ação (minúscula/maiúscula, prefixo, sufixo); por exemplo, Esquema de destino ORCL, Ação fazer minúscula. • Selecione o esquema, insira o nome da tabela e escolha a ação (minúscula/maiúscula, prefixo, sufixo); por exemplo, Esquema de destino ORCL, Tabela %, Ação fazer minúscula. 3. Ative o monitoramento do Amazon CloudWatch Logs. 4. Para as regras de mapeamento, adicione o código JSON a seguir. `{ "rules": [ {`	

Tarefa	Descrição	Habilidades necessárias
	"rule-type": "transformation", "rule-id": "1", "rule-name": "1", "rule-target": "table", "object-locator": { "schema-name": "%", "table-name": "%" }, "rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "transformation", "rule-id": "2", "rule-name": "2", "rule-target": "schema", "object-locator": { "schema-name": "ORCL", "table-name": "%" },	

Tarefa	Descrição	Habilidades necessárias
	"rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "selection", "rule-id": "3", "rule-name": "3", "object-locator": { "schema-name": "ORCL", "table-name": "DEPT" }, "rule-action": "include", "filters": [] }] }	
Planeje a execução da produção.	Confirme o tempo de inatividade com as partes interessadas, como proprietários de aplicativos, para executar o AWS DMS em sistemas de produção.	Líder de migração

Tarefa	Descrição	Habilidades necessárias
Pare a tarefa de migração.	1. Inicie a tarefa do AWS DMS que tem o status Pronto e monitore os registros da tarefa de migração na Amazon em CloudWatch busca de erros. Se você escolheu Migrar dados existentes e replicar alterações contínuas como o tipo de migração e o status for Carga completa, replicação contínua, a carga total com a migração de dados da CDC será concluída e a validação é contínua. 2. Depois de iniciar a migração, você pode obter informações adicionais sobre a conexão SSL em. CloudWatch Para Oracle, CloudWatch mostra a seguinte cadeia de conexão. `2019-12-17T09:15:11 [SOURCE_UNLOAD ]I: Connecting to Oracle: Beginning session (oracle_endpoint_conn.c:834)`	AWS geral

Tarefa	Descrição	Habilidades necessárias
	A string de conexão PostgreSQL será semelhante ao exemplo a seguir. `2019-12-17T09:15:11 [TARGET_LOAD ]I: Going to connect to ODBC connection string: PROTOCOL=7.4-0;DRIVER={PostgreSQL};SERVER=mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com;DATABASE=pgdb;PORT=5432;sslmode=require;UID=pguser; (odbc_endpoint_imp.c:2218)`	

Tarefa	Descrição	Habilidades necessárias
Valide os dados.	Analise os resultados e os dados da tarefa de migração nos bancos de dados Oracle de origem e PostgreSQL de destino: 1. Conecte-se ao pgAdmin e verifique os dados em seu banco de dados PostgreSQL com o esquema `ORCL`. 2. Para a CDC, verifique as alterações contínuas inserindo ou atualizando dados no banco de dados Oracle de origem.	DBA
Pare a tarefa de migração.	Depois de concluir com êxito a validação dos dados, interrompa a tarefa de migração.	AWS geral

Limpe os recursos

Tarefa	Descrição	Habilidades necessárias
Exclua as tarefas do AWS DMS.	1. No console do AWS DMS, navegue até Tarefas de migração do banco de dados e interrompa qualquer tarefa do AWS DMS em andamento ou em execução.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	2. Selecione as tarefas, escolha Ações e escolha Excluir.	
Exclua os endpoints do AWS DMS.	Selecione os endpoints de origem e de destino que você criou, escolha Ações e, em seguida, Excluir.	AWS geral
Exclua a instância de replicação do AWS DMS.	Escolha a instância de replicação, Ações e, em seguida, escolha Excluir.	AWS geral
Exclua o banco de dados PostgreSQL.	1. No console do Amazon RDS, escolha Bancos de dados. 2. Selecione a instância do banco de dados PostgreSQL que você criou, escolha Ações e, em seguida, Excluir.	AWS geral
Exclua o banco de dados Oracle.	No console do Amazon RDS, selecione a instância do banco de dados Oracle, escolha Ações e, em seguida, Excluir.	AWS geral

Solução de problemas

Problema	Solução
As conexões de teste de origem e de destino do AWS SCT estão falhando.	Configure as versões do driver JDBC e as regras de entrada do grupo de segurança da VPC para aceitar o tráfego de entrada.

Problema	Solução
A execução do teste do endpoint de origem Oracle falha.	Verifique as configurações do endpoint e se a instância de replicação está disponível.
A execução de carga total da tarefa do AWS DMS falha.	Verifique se os bancos de dados de origem e de destino têm tipos e tamanhos de dados correspondentes.
A tarefa de migração de validação do AWS DMS retorna erros.	1. Verifique se a tabela tem uma chave primária. Tabelas sem chave primária não são validadas. 2. Se a tabela tiver uma chave primária, mas retornar erros, verifique o atributo de conexão extra no endpoint de origem. O atributo de conexão extra deve ter `numberDataTypeScale=-2` para fornecer suporte dinamicamente ao tipo de dados `NUMBER` sem restrição de tamanho, com base nos dados disponíveis na tabela.

Recursos relacionados

Bancos de dados

- Amazon RDS para Oracle
- Amazon RDS para PostgreSQL

Conexões de bancos de dados SSL

- Usar SSL/TLS para criptografar uma conexão com uma instância de um banco de dados
  - Usar SSL com um RDS para uma instância de banco de dados Oracle
  - Proteger conexões com o RDS para PostgreSQL com SSL/TLS
  - Baixe pacotes de certificados para regiões específicas da AWS
    - Baixe o certificado raiz CA-2019 (expirado em agosto de 2024)
- Trabalhar com grupos de opções

  - Adição de opções a instâncias de banco de dados Oracle
  - Oracle Secure Sockets Layer
- Trabalhar com grupos de parâmetros
- Parâmetro de conexão sslmode do PostgreSQL
- Usar SSL do JDBC
- Rotação do seu certificado SSL/TLS
  - Atualizando seu certificado CA modificando sua instância de banco de dados ou cluster
  - Atualizando seu certificado CA aplicando a manutenção

AWS SCT

- AWS Schema Conversion Tool
- Guia do usuário do AWS Schema Conversion Tool
- Usar a interface de usuário do AWS SCT
- Usar um banco de dados Oracle como origem do AWS SCT

AWS DMS

- AWS Database Migration Service
- Guia do usuário do AWS Database Migration Service
  - Uso de um banco de dados Oracle como origem para o AWS DMS
  - Usar um banco de dados PostgreSQL como destino do AWS DMS
- Usar o SSL com o AWS Database Migration Service
- Migração de aplicativos que executam bancos de dados relacionais para a AWS

Mais informações

Os certificados da Amazon RDS Certificate Authority `rds-ca-2019` expiraram em agosto de 2024. Se você usa ou planeja usar SSL ou TLS com verificação de certificado para se conectar às suas instâncias de banco de dados RDS ou clusters de banco de dados Multi-AZ, considere usar um dos novos certificados CA:`rds-ca-rsa2048-g1`,, ou. `rds-ca-rsa4096-g1` `rds-ca-ecc384-g1`

Migrar os pacotes de pragma Oracle SERIALLY_REUSABLE para o PostgreSQL

Criado por Vinay Paladi (AWS)

Resumo

Esse padrão fornece uma step-by-step abordagem para migrar pacotes Oracle definidos como pragma SERIALLY_REUSABLE para o PostgreSQL na Amazon Web Services (AWS). Essa abordagem mantém a funcionalidade do pragma SERIALLY_REUSABLE.

O PostgreSQL não suporta o conceito de pacotes e o pragma SERIALLY_REUSABLE. Para obter uma funcionalidade semelhante no PostgreSQL, você pode criar esquemas para pacotes e implantar todos os objetos relacionados (como funções, procedimentos e tipos) dentro dos esquemas. Para aplicar essas variáveis, o exemplo de script de função wrapper fornecido nesse padrão usa um pacote de extensão do AWS Schema Conversion Tool (AWS SCT).

Para obter mais informações, consulte o Pragma SERIALLY_REUSABLE na documentação da Oracle.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- A versão mais recente do AWS SCT e os drivers necessários
- Um banco de dados Amazon Aurora Edição Compatível com PostgreSQL ou Amazon Relational Database Service (Amazon RDS) para banco de dados PostgreSQL

Versões do produto

- Banco de dados Oracle versão 10g e posterior

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Oracle on-premises

Pilha de tecnologias de destino

- Compatível com Aurora PostgreSQL ou Amazon RDS para PostgreSQL
- AWS SCT

Arquitetura de migração

Ferramentas

Serviços da AWS

- O AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.
- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.
- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.

Outras ferramentas

- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.

Épicos

Migrar o pacote Oracle usando o AWS SCT

Tarefa	Descrição	Habilidades necessárias
Configurar o AWS SCT.	Configurar a conectividade do AWS SCT com o banco de dados de origem. Para obter mais informações, consulte Uso de banco de dados Oracle como origem para o AWS SCT.	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Converter o script.	Use o AWS SCT para converter o pacote Oracle selecionando o banco de dados de destino como compatível com o Aurora PostgreSQL.	DBA, Desenvolvedor
Salve os arquivos .sql.	Antes de salvar o arquivo .sql, modifique a opção Configurações do projeto no AWS SCT para Arquivo único por estágio. O AWS SCT deverá separar o arquivo .sql em vários arquivos .sql com base no tipo de objeto.	DBA, Desenvolvedor
Alterar o código.	Abra a função `init` gerada pelo AWS SCT e altere-a conforme mostrado no exemplo na seção Informações adicionais. Ele adicionará uma variável para obter a funcionalidade `pg_serialize = 0` .	DBA, Desenvolvedor
Teste a conversão.	Implante a função `init` no banco de dados compatível com PostgreSQL do Aurora e teste os resultados.	DBA, Desenvolvedor

Recursos relacionados

- AWS Schema Conversion Tool
- Amazon RDS
- Características do Amazon Aurora

- Pragma SERIALLY_REUSABLE

Mais informações

```
Source Oracle Code:

CREATE OR REPLACE PACKAGE test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
PROCEDURE function_1
 (test_id number);
PROCEDURE function_2
 (test_id number
 );
END;

CREATE OR REPLACE PACKAGE BODY test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
v_char VARCHAR2(20) := 'shared.airline';
v_num number := 123;

PROCEDURE function_1(test_id number)
IS
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
v_char:='test1';
function_2(0);
END;

PROCEDURE function_2(test_id number)
is
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
END;
END test_pkg_var;

Calling the above functions

set serveroutput on
```

```
EXEC test_pkg_var.function_1(1);


EXEC test_pkg_var.function_2(1);


Target Postgresql Code:


CREATE SCHEMA test_pkg_var;

CREATE OR REPLACE FUNCTION test_pkg_var.init(pg_serialize IN INTEGER DEFAULT 0)

RETURNS void
AS
$BODY$

DECLARE

BEGIN

if aws_oracle_ext.is_package_initialized( 'test_pkg_var' ) AND pg_serialize = 0

then

return;

end if;

PERFORM aws_oracle_ext.set_package_initialized( 'test_pkg_var' );

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'shared.airline.basecurrency'::CHARACTER

VARYING(100));

PERFORM aws_oracle_ext.set_package_variable('test_pkg_var', 'v_num', 123::integer);

END;

$BODY$

LANGUAGE plpgsql;
```

```
CREATE OR REPLACE FUNCTION test_pkg_var.function_1(pg_serialize int default 1)

RETURNS void
AS

$BODY$
DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'test1'::varchar);

PERFORM test_pkg_var.function_2(0);
END;

$BODY$
LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_2(IN pg_serialize integer default 1)

RETURNS void

AS

$BODY$

DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');
```

```
raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

END;
$BODY$
LANGUAGE plpgsql;


Calling the above functions

select test_pkg_var.function_1()

 select test_pkg_var.function_2()
```

Migre tabelas externas da Oracle para a compatibilidade com o Amazon Aurora PostgreSQL

Criado por Rakesh Raghav (AWS) e anuradha chintha (AWS)

Resumo

As tabelas externas dão à Oracle a capacidade de consultar dados armazenados fora do banco de dados em arquivos simples. Você pode usar o driver ORACLE_LOADER para acessar qualquer dado armazenado em qualquer formato que possa ser carregado pelo utilitário SQL*Loader. Você não pode usar a Linguagem de Manipulação de Dados (DML) em tabelas externas, mas pode usar tabelas externas para operações de consulta, junção e classificação.

Amazon Aurora Edição Compatível com PostgreSQL não fornece funcionalidades semelhantes às tabelas externas da Oracle. Em vez disso, você deve usar a modernização para desenvolver uma solução escalável que atenda aos requisitos funcionais e seja econômica.

Esse padrão fornece etapas para migrar diferentes tipos de tabelas externas da Oracle para Aurora edição compatível com PostgreSQL na nuvem da Amazon Web Services (AWS) usando a extensão `aws_s3`.

Recomendamos testar minuciosamente essa solução antes de implementá-la em um ambiente de produção.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI)
- Uma instância de banco de dados Aurora compatível com o PostgreSQL disponível.
- Um banco de dados da Oracle on-premises com uma tabela externa
- API pg.Client
- Arquivos de dados

Limitações

- Esse padrão não fornece a funcionalidade para atuar como um substituto para tabelas externas da Oracle. No entanto, as etapas e o código de amostra podem ser aprimorados ainda mais para atingir suas metas de modernização do banco de dados.
- Os arquivos não devem conter o caractere que está sendo passado como delimitador nas funções de exportação e importação `aws_s3`.

Versões do produto

- Para importar do Amazon S3 para o RDS para PostgreSQL, o banco de dados deve estar executando o PostgreSQL versão 10.7 ou superior.

Arquitetura

Pilha de tecnologia de origem

- Oracle

Arquitetura de origem

Pilha de tecnologias de destino

- Amazon Aurora compatível com PostgreSQL
- Amazon CloudWatch
- AWS Lambda
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)

Arquitetura de destino

O diagrama a seguir mostra uma representação de alto nível da solução.

1. Os arquivos são enviados para o bucket do S3.
2. A função do Lambda é iniciada.

3. A função do Lambda inicia a chamada da função de banco de dados.
4. O Secrets Manager fornece as credenciais para acesso ao banco de dados.
5. Dependendo da função de banco de dados, um alarme SNS é criado.

Automação e escala

Qualquer adição ou alteração nas tabelas externas pode ser tratada com a manutenção de metadados.

Ferramentas

- Amazon Aurora compatível com PostgreSQL: o Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e compatível com o PostgreSQL e compatível com ACID, que combina a velocidade e a confiabilidade de bancos de dados comerciais de ponta com a economia de bancos de dados de código aberto.
- AWS CLI: o AWS Command Line Interface (AWS CLI) é uma ferramenta unificada para gerenciar os serviços da AWS. Com apenas uma ferramenta para fazer o download e configurar, você poderá controlar vários serviços da AWS pela linha de comando e automatizá-los usando scripts.
- Amazon CloudWatch — A Amazon CloudWatch monitora os recursos e a utilização do Amazon S3.
- AWS Lambda: o AWS Lambda é um serviço de computação com tecnologia sem servidor que oferece suporte à execução de código sem provisionar ou gerenciar servidores, criar uma lógica de escalabilidade de cluster com reconhecimento de workload, manter integrações de eventos ou gerenciar runtimes. Nesse padrão, o Lambda executa a função de banco de dados sempre que um arquivo é carregado no Amazon S3.
- AWS Secrets Manager: o AWS Secrets Manager é um serviço para armazenamento e recuperação de credenciais. O Secrets Manager permite a substituição de credenciais codificadas no seu código, incluindo senhas, por uma chamada de API para o Secrets Manager para recuperar o segredo de forma programática.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) fornece uma camada de armazenamento para receber e armazenar arquivos para consumo e transmissão de e para o cluster do Aurora compatível com PostgreSQL.
- aws_s3: a extensão `aws_s3` integra o Amazon S3 e o Aurora compatível com PostgreSQL.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) coordena e gerencia a entrega ou envio de mensagens entre publicadores e clientes. Nesse padrão, o Amazon SNS é usado para enviar notificações.

Código

Sempre que um arquivo é colocado no bucket do S3, uma função de banco de dados deve ser criada e chamada a partir do aplicativo de processamento ou da função do Lambda. Para obter detalhes, consulte o código (em anexo).

Épicos

Criar um arquivo externo

Tarefa	Descrição	Habilidades necessárias
Adicione um arquivo externo ao banco de dados de origem.	Crie um arquivo externo e mova-o para o diretório `oracle`.	DBA

Configurar o destino (Aurora compatível com PostgreSQL)

Tarefa	Descrição	Habilidades necessárias
Crie um banco de dados Aurora PostgreSQL.	Crie uma instância de banco de dados em seu cluster Amazon Aurora compatível com PostgreSQL.	DBA
Crie um esquema, uma extensão aws_s3 e tabelas.	Use o código em `ext_tbl_scripts` na seção Informações adicionais. As tabelas incluem tabelas reais, tabelas intermediárias, tabelas de erros e logs e uma metatabela.	DBA, Desenvolvedor
Criar a função de banco de dados.	Para criar a função de banco de dados (DB), use o código na função `load_external_table_latest` da seção Informações adicionais.	DBA, Desenvolvedor

Criar e configurar a função do Lambda

Tarefa	Descrição	Habilidades necessárias
Crie uma função.	Crie uma função com permissões para acessar o Amazon S3 e Amazon Relational Database Service (Amazon RDS). Essa função será atribuída ao Lambda para executar o padrão.	DBA
Criar a função do Lambda.	Crie uma função do Lambda que leia o nome do arquivo do Amazon S3 (por exemplo `file_key = info.get( 'object', {}).get(' key') ` ,) e chame a função de banco de dados (por exemplo, `curs.call proc("load_externa l_tables", [file_key ]) )` com o nome do arquivo como parâmetro de entrada. Dependendo do resultado da chamada de função, uma notificação do SNS será iniciada (por exemplo, `client.publish(Top icArn='arn:',Messa ge='fileloadsucces s',Subject='filelo adsuccess') `). Com base nas necessida des da sua empresa, você pode criar uma função do	DBA

Tarefa	Descrição	Habilidades necessárias
	Lambda com código extra, se necessário. Para obter mais informações, consulte a documentação do Lambda.	
Configurar um gatilho do evento do bucket do S3.	Configure um mecanismo para chamar a função do Lambda para todos os eventos de criação de objetos no bucket do S3.	DBA
Criar um segredo.	Crie um nome secreto para as credenciais do banco de dados usando o Secrets Manager. Passe o segredo na função do Lambda.	DBA
Faça upload dos arquivos de suporte do Lambda.	Faça upload de um arquivo .zip que contenha os pacotes de suporte do Lambda e o script Python anexado para conexão com o Aurora compatível com PostgreSQL. O código Python chama a função que você criou no banco de dados.	DBA
Criar um tópico do SNS.	Crie um tópico do SNS para enviar e-mails sobre o sucesso ou a falha do carregamento de dados.	DBA

Adicionar integração com o Amazon S3

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	No console do Amazon S3, você criará um bucket do S3 com um nome exclusivo que não contenha barras iniciais. Um nome de bucket do S3 é globalmente exclusivo, e o namespace é compartilhado por todas as contas da AWS.	DBA
Criar políticas do IAM.	Para criar políticas do AWS Identity and Access Management (IAM), use o código em `s3bucketpolicy_for_import` na seção Informações adicionais.	DBA
Criar funções.	Crie duas funções para o Aurora compatível com PostgreSQL, uma função para Importar e outra para Exportar. Atribua as políticas correspondentes às funções.	DBA
Anexe as funções ao cluster Aurora compatível com o PostgreSQL.	Em Gerenciar funções, anexe as funções de importação e exportação ao cluster do Aurora PostgreSQL.	DBA
Crie objetos de suporte para o Aurora compatível com PostgreSQL.	Para os scripts de tabela, use o código em `ext_tbl_scripts` na seção Informações adicionais.	DBA

Tarefa	Descrição	Habilidades necessárias
	Para a função personalizada, use o código em `load_external_Table_latest` na seção Informações adicionais.	

Processar um arquivo de teste

Tarefa	Descrição	Habilidades necessárias
Faça upload de um arquivo no bucket do S3.	Para fazer upload de um arquivo de teste no bucket do S3, use o console ou o comando a seguir na AWS CLI. `aws s3 cp /Users/Desktop/ukpost/exttbl/"testing files"/aps s3://s3importtest/inputext/aps` Assim que o arquivo é carregado, um evento de bucket inicia a função do Lambda, que executa função do Aurora compatível com PostgreSQL.	DBA
Verifique os dados e os arquivos de log e erro.	A função compatível com o Aurora PostgreSQL carrega os arquivos na tabela principal e cria arquivos `.log` e `.bad` no bucket do S3.	DBA

Tarefa	Descrição	Habilidades necessárias
Monitore a solução.	No CloudWatch console da Amazon, monitore a função Lambda.	DBA

Recursos relacionados

- Integração do Amazon S3
- Amazon S3
- Trabalhar com o Amazon Aurora Edição Compatível com PostgreSQL
- AWS Lambda
- Amazon CloudWatch
- AWS Secrets Manager
- Configurar notificações do Amazon SNS

Mais informações

ext_table_scripts

```
CREATE EXTENSION aws_s3 CASCADE;
CREATE TABLE IF NOT EXISTS meta_EXTERNAL_TABLE
(
    table_name_stg character varying(100) ,
    table_name character varying(100)  ,
    col_list character varying(1000)  ,
    data_type character varying(100)  ,
    col_order numeric,
    start_pos numeric,
    end_pos numeric,
    no_position character varying(100)  ,
    date_mask character varying(100)  ,
    delimeter character(1)  ,
    directory character varying(100)  ,
    file_name character varying(100)  ,
    header_exist character varying(5)
);
CREATE TABLE IF NOT EXISTS ext_tbl_stg
```

```
(
    col1 text
);
CREATE TABLE IF NOT EXISTS error_table
(
    error_details text,
    file_name character varying(100),
    processed_time timestamp without time zone
);
CREATE TABLE IF NOT EXISTS log_table
(
    file_name character varying(50) COLLATE pg_catalog."default",
    processed_date timestamp without time zone,
    tot_rec_count numeric,
    proc_rec_count numeric,
    error_rec_count numeric
);
sample insert scripts of meta data:
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'source_filename', 'character varying', 2, 8, 27, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'record_type_identifier', 'character varying', 3, 28, 30, NULL, NULL, NULL,
 'databasedev', 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'fad_code', 'numeric', 4, 31, 36, NULL, NULL, NULL, 'databasedev', 'externalinterface/
loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'session_sequence_number', 'numeric', 5, 37, 42, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'transaction_sequence_number', 'numeric', 6, 43, 48, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
```

s3bucketpolicy_for import

```
---Import role policy
--Create an IAM policy to allow, Get,  and list actions on S3 bucket
 {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3import",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest",
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
--Export Role policy
--Create an IAM policy to allow, put,  and list actions on S3 bucket
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3export",
            "Action": [
                "S3:PutObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
```

Exemplo de função de banco de dados load_external_tables_latest

```
CREATE OR REPLACE FUNCTION public.load_external_tables(pi_filename text)
```

```
 RETURNS character varying
 LANGUAGE plpgsql
AS $function$
/* Loading data from S3 bucket into a APG table */
DECLARE
 v_final_sql TEXT;
 pi_ext_table TEXT;
 r refCURSOR;
 v_sqlerrm text;
 v_chunk numeric;
 i integer;
 v_col_list TEXT;
 v_postion_list CHARACTER VARYING(1000);
 v_len  integer;
 v_delim varchar;
 v_file_name CHARACTER VARYING(1000);
 v_directory CHARACTER VARYING(1000);
 v_table_name_stg CHARACTER VARYING(1000);
 v_sql_col TEXT;
 v_sql TEXT;
 v_sql1 TEXT;
 v_sql2 TEXT;
 v_sql3 TEXT;
 v_cnt integer;
 v_sql_dynamic TEXT;
 v_sql_ins TEXT;
 proc_rec_COUNT integer;
 error_rec_COUNT integer;
 tot_rec_COUNT integer;
 v_rec_val integer;
 rec record;
 v_col_cnt integer;
 kv record;
 v_val text;
 v_header text;
 j integer;
 ERCODE VARCHAR(5);
 v_region text;
 cr CURSOR FOR
 SELECT distinct DELIMETER,
   FILE_NAME,
   DIRECTORY
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
```

```
   AND DELIMETER IS NOT NULL;


 cr1 CURSOR FOR
   SELECT   col_list,
   data_type,
   start_pos,
   END_pos,
   concat_ws('',' ',TABLE_NAME_STG) as TABLE_NAME_STG,
   no_position,date_mask
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
 order by col_order asc;
cr2 cursor FOR
SELECT  distinct table_name,table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);


BEGIN
 -- PERFORM utl_file_utility.init();
   v_region := 'us-east-1';
   /* find tab details from file name */


   --DELETE FROM  ERROR_TABLE WHERE file_name= pi_filename;
  -- DELETE FROM  log_table WHERE file_name= pi_filename;


 BEGIN


   SELECT distinct table_name,table_name_stg INTO strict pi_ext_table,v_table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);
 EXCEPTION
   WHEN NO_DATA_FOUND THEN
    raise notice 'error 1,%',sqlerrm;
    pi_ext_table := null;
    v_table_name_stg := null;
      RAISE USING errcode = 'NTFIP' ;
    when others then
        raise notice 'error others,%',sqlerrm;
 END;
```

```
 j :=1 ;

for rec in  cr2
 LOOP




  pi_ext_table     := rec.table_name;
  v_table_name_stg := rec.table_name_stg;
  v_col_list := null;


 IF pi_ext_table IS NOT NULL
  THEN
    --EXECUTE concat_ws('','truncate table  ' ,pi_ext_table) ;
   EXECUTE concat_ws('','truncate table  ' ,v_table_name_stg) ;




       SELECT distinct DELIMETER INTO STRICT v_delim
       FROM  meta_EXTERNAL_TABLE
       WHERE table_name = pi_ext_table;


       IF v_delim IS NOT NULL THEN
     SELECT distinct DELIMETER,
       FILE_NAME,
       DIRECTORY ,
       concat_ws('',' ',table_name_stg),
       case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
     INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
     FROM  meta_EXTERNAL_TABLE
     WHERE table_name = pi_ext_table
       AND DELIMETER IS NOT NULL;


     IF    upper(v_delim) = 'CSV'
     THEN
       v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3 ( ''',
       v_table_name_stg,''','''',
       ''DELIMITER '''','''' CSV HEADER QUOTE '''''''''', aws_commons.create_s3_uri
( ''',
```

```
      v_directory,''',''',v_file_name,''', ''',v_region,'''))');
      ELSE
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
          v_table_name_stg, ''','''', ''DELIMITER AS ''''^''''','''','
         aws_commons.create_s3_uri
          ( ''',v_directory, ''','''',
          v_file_name, ''',',
           '''',v_region,''')
         )');
         raise notice 'v_sql , %',v_sql;
      begin
       EXECUTE  v_sql;
      EXCEPTION
        WHEN OTHERS THEN
          raise notice 'error 1';
        RAISE USING errcode = 'S3IMP' ;
      END;


      select count(col_list) INTO v_col_cnt
      from  meta_EXTERNAL_TABLE where table_name = pi_ext_table;







       -- raise notice 'v_sql 2, %',concat_ws('','update ',v_table_name_stg, ' set
col1 = col1||''',v_delim,''''');


      execute concat_ws('','update ',v_table_name_stg, ' set col1 =
col1||''',v_delim,''''');




      i :=1;
      FOR rec in cr1
      loop
      v_sql1 := concat_ws('',v_sql1,'split_part(col1,''',v_delim,''',', i,')',' as
',rec.col_list,',');
      v_sql2 := concat_ws('',v_sql2,rec.col_list,',');
  --    v_sql3 := concat_ws('',v_sql3,'rec.',rec.col_list,'::',rec.data_type,',');
```

```
      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                coalesce((trim(split_part(col1,''',v_delim,''',',
i,')))::NUMERIC,0)::',rec.data_type,' END as ',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''99990101''),''YYYYMMDD'')::',rec.data_type,' END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
 'MM/DD/YYYY hh24:mi:ss'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''01/01/9999 0024:00:00''),''MM/DD/YYYY hh24:mi:ss'')::',rec.data_type,' END as
',rec.col_list,',');
         ELSE
       v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                 coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),'''')::',rec.data_type,' END as ',rec.col_list,',') ;
      END case;


      i :=i+1;
      end loop;


        -- raise notice 'v_sql 3, %',v_sql3;
```

```
       SELECT trim(trailing ' ' FROM v_sql1) INTO v_sql1;
       SELECT trim(trailing ',' FROM v_sql1) INTO v_sql1;


       SELECT trim(trailing ' ' FROM v_sql2) INTO v_sql2;
       SELECT trim(trailing ',' FROM v_sql2) INTO v_sql2;


       SELECT trim(trailing ' ' FROM v_sql3) INTO v_sql3;
       SELECT trim(trailing ',' FROM v_sql3) INTO v_sql3;


       END IF;
      raise notice 'v_delim , %',v_delim;


     EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)  INTO v_cnt;


    raise notice 'stg cnt , %',v_cnt;


    /* if upper(v_delim) = 'CSV' then
       v_sql_ins := concat_ws('', ' SELECT * from ' ,v_table_name_stg );
     else
      -- v_sql_ins := concat_ws('',' SELECT ',v_sql1,'  from (select col1 from
 ' ,v_table_name_stg , ')sub ');
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ')sub ');
       END IF;*/


v_chunk := v_cnt/100;




for i in 1..101
loop
     BEGIN
    -- raise notice 'v_sql , %',v_sql;
       -- raise notice 'Chunk number , %',i;
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ' offset ',v_chunk*(i-1), ' limit ',v_chunk,') sub ');
```

```
    v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
    -- raise notice 'select statement , %',v_sql_ins;
         -- v_sql := null;
    -- EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins, 'offset
',v_chunk*(i-1), ' limit ',v_chunk );
    --v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins );


    -- raise notice 'insert statement , %',v_sql;


   raise NOTICE 'CHUNK START %',v_chunk*(i-1);
  raise NOTICE 'CHUNK END %',v_chunk;


    EXECUTE v_sql;


 EXCEPTION
      WHEN OTHERS THEN
      -- v_sql_ins := concat_ws('',' SELECT ',v_sql1, '  from (select col1 from
' ,v_table_name_stg , ' )sub ');
        -- raise notice 'Chunk number for cursor , %',i;


   raise NOTICE 'Cursor - CHUNK START %',v_chunk*(i-1);
  raise NOTICE 'Cursor -  CHUNK END %',v_chunk;
        v_sql_ins := concat_ws('',' SELECT ',v_sql3, '  from (select col1 from
' ,v_table_name_stg , ' )sub ');


        v_final_sql := REPLACE (v_sql_ins, ''''::text, ''''''::text);
       -- raise notice 'v_final_sql %',v_final_sql;
        v_sql :=concat_ws('','do $a$ declare  r refcursor;v_sql text; i
numeric;v_conname text;  v_typ  ',pi_ext_table,'[]; v_rec  ','record',';
          begin
```

```
          open r for execute ''select col1 from ',v_table_name_stg ,'  offset
 ',v_chunk*(i-1), ' limit ',v_chunk,''';
          loop
          begin
          fetch r into v_rec;
          EXIT WHEN NOT FOUND;




          v_sql := concat_ws('''','insert into  ',pi_ext_table,' SELECT ',REPLACE
 (v_sql3, ''''::text, ''''''::text) , '  from ( select ''''''',v_rec.col1,''''''' as
 col1) v'');
           execute v_sql;


          exception
           when others then
         v_sql := ''INSERT INTO  ERROR_TABLE VALUES (concat_ws(''''''''','''''Error
 Name: ''''',$$''||SQLERRM||''$$,''''Error State: ''''',''''''||
SQLSTATE||'''''',''''record : ''''',$$''||v_rec.col1||''$$),'''''||
pi_filename||''''',now())'';


             execute v_sql;
            continue;
          end ;
          end loop;
          close r;
          exception
          when others then
        raise;
          end ; $a$');
     -- raise notice ' inside excp v_sql %',v_sql;
         execute v_sql;
     --  raise notice 'v_sql %',v_sql;
      END;
  END LOOP;
     ELSE


     SELECT distinct DELIMETER,FILE_NAME,DIRECTORY ,concat_ws('',' ',table_name_stg),
       case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
       INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
```

```
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table                  ;
    v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
      v_table_name_stg, ''','''', ''DELIMITER AS ''''#'''' ',v_header,' '','','
     aws_commons.create_s3_uri
      ( ''',v_directory, ''','''',
      v_file_name, ''',',
       '''',v_region,''')
     )');
        EXECUTE  v_sql;


    FOR rec in cr1
    LOOP


     IF rec.start_pos IS NULL AND rec.END_pos IS NULL AND rec.no_position = 'recnum'
     THEN
       v_rec_val := 1;
     ELSE


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1)))::NUMERIC,0)::',rec.data_type,' END as
',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''99990101''),''YYYYMMDD''):',rec.data_type,'
END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDDHH24MISS'
        THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
```

```
               THEN null
                ELSE
                to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''9999010100240000''),''YYYYMMDDHH24MISS''):',rec.data_
END as ',rec.col_list,',');
         ELSE
       v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                 coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''''):',rec.data_type,' END as
',rec.col_list,',') ;
      END case;


     END IF;
     v_col_list := concat_ws('',v_col_list ,v_sql1);
    END LOOP;




          SELECT trim(trailing ' ' FROM v_col_list) INTO v_col_list;
          SELECT trim(trailing ',' FROM v_col_list) INTO v_col_list;


          v_sql_col   :=  concat_ws('',trim(trailing ',' FROM v_col_list) , ' FROM
 ',v_table_name_stg,' WHERE col1 IS NOT NULL AND length(col1)>0 ');




          v_sql_dynamic := v_sql_col;


          EXECUTE  concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg) INTO v_cnt;




        IF v_rec_val = 1 THEN
            v_sql_ins := concat_ws('',' select row_number() over(order by ctid) as
line_number ,' ,v_sql_dynamic) ;
```

```
        ELSE
              v_sql_ins := concat_ws('',' SELECT' ,v_sql_dynamic) ;
          END IF;


    BEGIN
      EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
          EXCEPTION
             WHEN OTHERS THEN
         IF v_rec_val = 1 THEN
                v_final_sql := ' select row_number() over(order by ctid) as
line_number ,col1 from ';
               ELSE
                v_final_sql := ' SELECT col1 from';
              END IF;
      v_sql :=concat_ws('','do $a$ declare  r refcursor;v_rec_val numeric :=
',coalesce(v_rec_val,0),';line_number numeric; col1 text; v_typ  ',pi_ext_table,'[];
v_rec  ',pi_ext_table,';
            begin
            open r for execute ''',v_final_sql, ' ',v_table_name_stg,' WHERE col1 IS
NOT NULL AND length(col1)>0 '' ;
            loop
            begin
            if   v_rec_val = 1 then
            fetch r into line_number,col1;
            else
            fetch r into col1;
            end if;


            EXIT WHEN NOT FOUND;
             if v_rec_val = 1 then
             select line_number,',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             else
               select ',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             end if;


            insert into  ',pi_ext_table,' select v_rec.*;
             exception
             when others then
```

```
              INSERT INTO  ERROR_TABLE VALUES (concat_ws(''''',''Error Name:
'',SQLERRM,''Error State: '',SQLSTATE,''record : '',v_rec),''',pi_filename,''',now());
              continue;
             end ;
              end loop;
            close r;
             exception
             when others then
             raise;
             end ; $a$');
        execute v_sql;


    END;


        END IF;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  ' ,pi_ext_table)   INTO proc_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  error_table WHERE file_name
='''',pi_filename,''' and processed_time::date = clock_timestamp()::date')  INTO
error_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)   INTO tot_rec_COUNT;


  INSERT INTO  log_table values(pi_filename,now(),tot_rec_COUNT,proc_rec_COUNT,
error_rec_COUNT);


  raise notice 'v_directory, %',v_directory;


  raise notice 'pi_filename, %',pi_filename;


  raise notice 'v_region, %',v_region;
```

```
  perform aws_s3.query_export_to_s3('SELECT
 replace(trim(substring(error_details,position(''('' in
 error_details)+1),'')''),'','','';''),file_name,processed_time FROM  error_table WHERE
 file_name = '''||pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );


raise notice 'v_directory, %',v_directory;


   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  log_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.log', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );




   END IF;
 j := j+1;
 END LOOP;


       RETURN 'OK';
EXCEPTION
    WHEN  OTHERS THEN
  raise notice 'error %',sqlerrm;
   ERCODE=SQLSTATE;
   IF ERCODE = 'NTFIP' THEN
     v_sqlerrm := concat_Ws('',sqlerrm,'No data for the filename');
   ELSIF ERCODE = 'S3IMP' THEN
    v_sqlerrm := concat_Ws('',sqlerrm,'Error While exporting the file from S3');
   ELSE
      v_sqlerrm := sqlerrm;
   END IF;
```

```
 select distinct directory into v_directory from  meta_EXTERNAL_TABLE;



 raise notice 'exc v_directory, %',v_directory;


   raise notice 'exc pi_filename, %',pi_filename;


   raise notice 'exc v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  error_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );
    RETURN null;
END;
$function$
```

Migre índices baseados em funções do Oracle para o PostgreSQL

Criado por Veeranjaneyulu Grandhi (AWS) e Navakanth Talluri (AWS)

Resumo

Os índices são uma forma comum de aprimorar o desempenho do banco de dados. Um índice permite que o servidor do banco de dados encontre e recupere linhas específicas com muito mais rapidez do que poderia sem um índice. Mas os índices também adicionam sobrecarga ao sistema de banco de dados como um todo, portanto, devem ser usados com sensatez. Índices baseados em funções, baseados em uma função ou expressão, podem envolver várias colunas e expressões matemáticas. Um índice baseado em funções melhora o desempenho das consultas que usam a expressão de índice.

Nativamente, o PostgreSQL não suporta a criação de índices baseados em funções usando funções que têm volatilidade definida como estável. No entanto, você pode criar funções semelhantes com volatilidade `IMMUTABLE` e usá-las na criação de índices.

Uma função `IMMUTABLE` não pode modificar o banco de dados e é garantido que retornará os mesmos resultados com os mesmos argumentos para sempre. Essa categoria permite que o otimizador pré-avalie a função quando uma consulta a chama com argumentos constantes.

Esse padrão ajuda na migração dos índices baseados em funções do Oracle quando usados com funções como `to_char`, `to_date` e `to_number` para o equivalente do PostgreSQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS)
- Uma instância de banco de dados do Oracle de origem com o serviço de receptor configurado e em execução
- Familiaridade com bancos de dados PostgreSQL

Limitações

- O limite de tamanho do banco de dados é 64 TB.
- As funções usadas na criação do índice devem ser IMUTÁVEIS.

Versões do produto

- Todas as edições do banco de dados do Oracle para versões 11g (versões 11.2.0.3.v1 e posteriores) e até 12.2 e 18c
- PostgreSQL, versões 9.6 e superiores

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Oracle no local ou em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou uma instância de banco de dados Amazon RDS for Oracle

Pilha de tecnologias de destino

- Qualquer mecanismo do PostgreSQL

Ferramentas

- O pgAdmin 4 é uma ferramenta de gerenciamento de código aberto para o Postgres. A ferramenta pgAdmin 4 fornece uma interface gráfica para criar, manter e usar objetos de banco de dados.
- O Oracle SQL Developer é um ambiente de desenvolvimento integrado (IDE) para desenvolver e gerenciar o Oracle Database em implantações tradicionais e na nuvem.

Épicos

Crie um índice baseado em funções usando uma função padrão

Tarefa	Descrição	Habilidades necessárias
Crie um índice baseado em função em uma coluna usando a função to_char.	Use o código a seguir para criar o índice baseado em função. `postgres=# create table funcindex( col1 timestamp without time zone);`	DBA, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	``` CREATE TABLE postgres=# insert into funcindex values (now()); INSERT 0 1 postgres=# select * from funcindex; col1 ---------------------- ------ 2022-08-09 16:00:57. 77414 (1 rows) postgres=# create index funcindex_idx on funcindex(to_char(col1,'DD-MM-YYYY HH24:MI:SS')); ERROR: functions in index expression must be marked IMMUTABLE ``` **Note** O PostgreSQL não permite criar um índice baseado em funções sem a cláusula. `IMMUTABLE`	
Verifique a volatilidade da função.	Para verificar a volatilidade da função, use o código na seção Informações adicionais.	DBA

Crie índices baseados em funções usando uma função de encapsulamento

Tarefa	Descrição	Habilidades necessárias
Crie uma função de encapsulamento.	Para criar uma função de encapsulamento, use o código na seção Informações adicionais.	Desenvolvedor do PostgreSQL
Crie um índice usando a função de encapsulamento.	Use o código na seção Informações adicionais para criar uma função definida pelo usuário com a palavra-chave `IMMUTABLE` no mesmo esquema do aplicativo e faça referência a ela no script de criação de índice. Se uma função definida pelo usuário for criada em um esquema comum (do exemplo anterior), atualize o `search_path` conforme mostrado. `ALTER ROLE <ROLENAME> set search_path=$user, COMMON;`	DBA, desenvolvedor do PostgreSQL

Validar a criação de um índice

Tarefa	Descrição	Habilidades necessárias
Valide a criação de um índice.	Valide se o índice precisa ser criado, com base nos padrões de acesso à consulta.	DBA

Tarefa	Descrição	Habilidades necessárias
Valide se o índice pode ser usado.	Para verificar se o índice baseado em função é captado pelo PostgreSQL Optimizer, execute uma instrução SQL usando explain (explicar) ou explain analyze (explicar e analizar). Use o código na seção Informações adicionais. Se possível, reúna também as estatísticas da tabela. **Note** Se você observar o plano de explicaçã o, o otimizador do PostgreSQL escolheu um índice baseado em funções devido à condição do predicado .	DBA

Recursos relacionados

- Índices baseados em funções (documentação da Oracle)
- Índices em expressões (documentação do PostgreSQL)
- Volatilidade do PostgreSQL (documentação do PostgreSQL)
- PostgreSQL search_path (documentação do PostgreSQL)
- Manual de migração do Oracle Database 19c para o PostgreSQL do Amazon Aurora

Mais informações

Crie uma função de encapsulamento

```
CREATE OR REPLACE FUNCTION myschema.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
```

Crie um índice usando a função encapsulamento

```
postgres=# create function common.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
CREATE FUNCTION
postgres=# create index funcindex_idx on funcindex(common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS'));
CREATE INDEX
```

Verifique a volatilidade da função

```
SELECT DISTINCT p.proname as "Name",p.provolatile as "volatility" FROM
 pg_catalog.pg_proc p
 LEFT JOIN pg_catalog.pg_namespace n ON n.oid = p.pronamespace
 LEFT JOIN pg_catalog.pg_language l ON l.oid = p.prolang
 WHERE n.nspname OPERATOR(pg_catalog.~) '^(pg_catalog)$' COLLATE pg_catalog.default AND
 p.proname='to_char'GROUP BY p.proname,p.provolatile
ORDER BY 1;
```

Valide se o índice pode ser usado

```
explain analyze <SQL>


postgres=# explain select col1 from funcindex where common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS') = '09-08-2022 16:00:57';
                                                    QUERY PLAN
-------------------------------------------------------------------------------------------
 Index Scan using funcindex_idx on funcindex  (cost=0.42..8.44 rows=1 width=8)
   Index Cond: ((common.to_char(col1, 'DD-MM-YYYY HH24:MI:SS'::character
 varying))::text = '09-08-2022 16:00:57'::text)
(2 rows)
```

Migre funções nativas do Oracle para o PostgreSQL usando extensões

Criado por Pinesh Singal (AWS)

Resumo

Esse padrão de migração fornece step-by-step orientação para migrar uma instância de banco de dados Amazon Relational Database Service (Amazon RDS) para Oracle para um banco de dados Amazon RDS for PostgreSQL ou Amazon Aurora PostgreSQL compatível com o Amazon Aurora PostgreSQL, modificando as extensões e o código incorporado nativo do PostgreSQL (). `aws_oracle_ext` `orafce` `psql` Isso economizará tempo de processamento.

O padrão descreve uma estratégia de migração manual offline sem qualquer tempo de inatividade para um banco de dados de origem Oracle de vários terabytes com um grande número de transações.

O processo de migração usa o AWS Schema Conversion Tool (AWS SCT) com as extensões `aws_oracle_ext` e `orafce` para converter um esquema de banco de dados do Amazon RDS para Oracle em um esquema de banco de dados do Amazon RDS para PostgreSQL ou Aurora compatível com PostgreSQL. Em seguida, o código é alterado manualmente para código nativo incorporado `psql` compatível com PostgreSQL. Isso ocorre porque as chamadas de extensão afetam o processamento do código no servidor de banco de dados PostgreSQL, e nem todo o código da extensão é totalmente compatível ou compatível com o código PostgreSQL.

Esse padrão se concentra principalmente na migração manual de códigos SQL usando a AWS SCT e as extensões `aws_oracle_ext` e `orafce`. Você converte as extensões já usadas em incorporações nativas do PostgreSQL (`psql`). Em seguida, você remove todas as referências às extensões e converte os códigos de acordo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Sistema operacional (Windows ou Mac) ou EC2 instância da Amazon (em funcionamento)
- Orafce

Limitações

Nem todas as funções que usam extensões `aws_oracle_ext` ou `orafce` do Oracle podem ser convertidas em funções nativas do PostgreSQL. Pode ser necessário retrabalho manual para compilá-lo com as bibliotecas do PostgreSQL.

Uma desvantagem de usar extensões da AWS SCT é seu baixo desempenho na execução e na obtenção dos resultados. Seu custo pode ser entendido a partir do plano PostgreSQL EXPLAIN simples (plano de execução de uma instrução) sobre a migração da função `SYSDATE` Oracle para a função `NOW()` PostgreSQL entre os três códigos (`aws_oracle_ext`, `orafce`, `psql` e padrão), conforme explicado na seção Verificação de comparação de desempenho no documento anexo.

Versões do produto

- Origem: banco de dados Amazon RDS para Oracle 10.2 e posterior (para 10.x), 11g (11.2.0.3.v1 e posterior) e até 12.2, 18c e 19c (e posterior) para Enterprise Edition, Standard Edition, Standard Edition 1 e Standard Edition 2
- Destino : Amazon RDS para PostgreSQL ou banco de dados Aurora compatível com PostgreSQL 9.4 e posterior (para 9.x), 10.x, 11.x, 12.x, 13.x e 14.x (e versões posteriores)
- AWS SCT: versão mais recente (esse padrão foi testado com 1.0.632)
- Oracle: versão mais recente (esse padrão foi testado com 3.9.0)

Arquitetura

Pilha de tecnologia de origem

- Uma instância do banco de dados Amazon RDS para Oracle com a versão 12.1.0.2.v18

Pilha de tecnologias de destino

- Uma instância de banco de dados do Amazon RDS para PostgreSQL ou Aurora compatível com PostgreSQL com a versão 11.5

Arquitetura de migração de banco de dados

O diagrama a seguir representa a arquitetura de migração de banco de dados entre os bancos de dados Oracle de origem e PostgreSQL de destino. A arquitetura envolve a Nuvem AWS, uma nuvem privada virtual (VPC), zonas de disponibilidade, uma sub-rede privada, um banco de dados Amazon RDS para Oracle, AWS SCT, um banco de dados Amazon RDS para PostgreSQL ou Aurora

compatível com PostgreSQL, extensões para Oracle (`aws_oracle_ext` e `orafce`) e arquivos de linguagem de consulta estruturada (SQL).

1. Inicie a instância de banco de dados Amazon RDS para Oracle (banco de dados de origem).
2. Use a AWS SCT com os pacotes de extensão `aws_oracle_ext` e `orafce` para converter o código-fonte do Oracle para o PostresQL.
3. A conversão produz arquivos .sql migrados compatíveis com o PostgreSQL.
4. Converta manualmente os códigos de extensão Oracle não convertidos em códigos PostgreSQL (`psql`).
5. A conversão manual produz arquivos .sql convertidos compatíveis com o PostgreSQL.
6. Execute esses arquivos .sql na instância do banco de dados Amazon RDS para PostgreSQL (banco de dados de destino).

Ferramentas

Ferramentas

Serviços da AWS

- AWS SCT: a AWS Schema Conversion Tool (AWS SCT) converte seu esquema de banco de dados existente de um mecanismo de banco de dados para outro. Você pode converter o esquema Online Transactional Processing (OLTP) relacional ou o esquema de data warehouse. Seu esquema convertido é adequado para uma instância de banco de dados Amazon RDS para MySQL, um cluster de banco de dados Amazon Aurora, uma instância de banco de dados Amazon RDS para PostgreSQL ou um cluster do Amazon Redshift. O esquema convertido também pode ser usado com um banco de dados em uma EC2 instância da Amazon ou armazenado como dados em um bucket do Amazon S3.

  A AWS SCT oferece uma interface de usuário baseada em projeto que permite converter automaticamente o esquema do banco de dados de origem em um formato que seja compatível com a instância do Amazon RDS de destino.

  Você pode usar a AWS SCT para fazer a migração de um banco de dados de origem Oracle para qualquer um dos destinos listados anteriormente. Usando a AWS SCT, você pode exportar as definições de objetos do banco de dados de origem, como esquema, visualizações, procedimentos armazenados e funções.

Você pode usar a AWS SCT para convertes dados do Oracle para Amazon RDS para PostgreSQL ou Amazon Aurora Edição Compatível com PostgreSQL.

Nesse padrão, você usa a AWS SCT para converter e migrar o código Oracle para o PostgreSQL usando as extensões `aws_oracle_ext` e `orafce` migrando manualmente os códigos de extensão para o código `psql` padrão ou nativo incorporado.

- O pacote de extensões da AWS SCT é um módulo complementar que emula funções presentes no banco de dados de origem e necessárias ao converter objetos para o banco de dados de destino. Antes de poder instalar o pacote de extensões da AWS SCT, você precisa converter seu esquema de banco de dados.

  Quando você converte seu banco de dados ou esquema de data warehouse, a AWS SCT adiciona mais um esquema ao seu banco de dados de destino. Esse esquema implementa as funções de sistema SQL do banco de dados de origem necessárias para gravar o esquema convertido no banco de dados de destino. Esse esquema adicional é chamado de esquema do pacote de extensões.

  O esquema do pacote de extensões para bancos de dados OLTP é nomeado de acordo com o banco de dados de origem. Para bancos de dados Oracle, o esquema do pacote de extensão é `AWS_ORACLE_EXT`.

Outras ferramentas

- Orafce: o Orafce é um módulo que implementa funções, tipos de dados e pacotes compatíveis com Oracle. É uma ferramenta de código aberto com uma licença Berkeley Source Distribution (BSD) para que qualquer pessoa possa usá-la. O módulo `orafce` é útil para migrar do Oracle para o PostgreSQL porque tem muitas funções Oracle implementadas no PostgreSQL.

Código

Para obter uma lista de todos os códigos comumente usados e migrados do Oracle para o PostgreSQL para evitar o uso do código de extensão da AWS SCT, consulte o documento em anexo.

Épicos

Configurar o banco de dados de origem do Amazon RDS para Oracle

Tarefa	Descrição	Habilidades necessárias
Crie a instância do banco de dados Oracle.	Crie uma instância de banco de dados do Amazon RDS para Oracle ou Aurora compatível com PostgreSQL a partir do console do Amazon RDS.	AWS geral, DBA
Configurar os grupos de segurança.	Configurar grupos de segurança de entrada e saída.	AWS geral
Criar o banco de dados.	Crie o banco de dados Oracle com os usuários e esquemas necessários.	AWS geral, DBA
Criar os objetos.	Crie objetos e insira dados no esquema.	DBA

Configurar o banco de dados de destino do Amazon RDS para PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Crie a instância do banco de dados para PostgreSQL.	Crie uma instância do banco de dados Amazon RDS para PostgreSQL ou Amazon Aurora PostgreSQL a partir do console do Amazon RDS.	AWS geral, DBA
Configurar os grupos de segurança.	Configurar grupos de segurança de entrada e saída.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Criar o banco de dados.	Crie o banco de dados PostgreSQL com os usuários e esquemas necessários.	AWS geral, DBA
Validar as extensões.	Verifique se `aws_oracle_ext` e `orafce` estão instalados e configurados corretamente no banco de dados PostgreSQL.	DBA
Verifique se o banco de dados PostgreSQL está disponível.	Certifique-se de que o banco de dados PostgreSQL esteja ativo e funcionando.	DBA

Migre o esquema Oracle para o PostgreSQL usando a AWS SCT e as extensões

Tarefa	Descrição	Habilidades necessárias
Instale a AWS SCT.	Instalar a versão mais recente da AWS SCT.	DBA
Configure a AWS SCT.	Configure o AWS SCT com drivers Java Database Connectivity (JDBC) para Oracle (`ojdbc8.jar`) e PostgreSQL (`postgresql-42.2.5.jar`).	DBA
Habilite o pacote de extensão ou modelo da AWS SCT.	Em Configurações do projeto da AWS SCT, habilite a implementação de funções incorporadas com as extensões `aws_oracle_ext` e `orafce` para o	DBA

Tarefa	Descrição	Habilidades necessárias
	esquema do banco de dados Oracle.	
Converta o esquema.	Na AWS SCT, escolha Converter esquema para converter o esquema do Oracle para o PostgreSQL e gerar os arquivos .sql.	DBA

Converta o código de extensão da AWS SCT em código psql

Tarefa	Descrição	Habilidades necessárias
Converta manualmente o código.	Converta manualmente cada linha de código compatível com a extensão em código incorporado padrão `psql`, conforme detalhado no documento anexo. Por exemplo, altere `AWS_ORACLE_EXT.SYSDATE()` ou `ORACLE.SYSDATE()` para `NOW()`.	DBA
Valide o código	(Opcional) Valide cada linha de código executando-o temporariamente no banco de dados PostgreSQL.	DBA
Crie objetos no banco de dados PostgreSQL.	Para criar objetos no banco de dados PostgreSQL, execute os arquivos .sql que foram gerados pela AWS SCT e modificados nas duas etapas anteriores.	DBA

Recursos relacionados

- Banco de dados
  - Oracle no Amazon RDS
  - PostgreSQL no Amazon RDS
  - Trabalho com Amazon Aurora PostgreSQL
  - Plano PostgreSQL EXPLAIN
- AWS SCT
  - Visão geral do AWS Schema Conversion Tool
  - Guia do usuário do AWS SCT
  - Usar a interface de usuário da AWS SCT
  - Usar um banco de dados Oracle como origem para AWS SCT
- Extensões para AWS SCT
  - Usar o pacote de extensões da AWS SCT
  - Funcionalidade Oracle (en)
  - orafce do PGXN
  - GitHub orafce

Mais informações

Para obter mais informações, siga os comandos detalhados, com sintaxe e exemplos, para converter manualmente o código no documento anexo.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre um banco de dados Db2 da Amazon para o EC2 Aurora MySQL compatível usando o AWS DMS

Criado por Pinesh Singal (AWS)

Resumo

Depois de migrar seu banco de dados IBM Db2 for LUW para o Amazon Elastic Compute Cloud (Amazon EC2), considere rearquitetar o banco de dados migrando para um banco de dados nativo em nuvem da Amazon Web Services (AWS). Esse padrão abrange a migração de um banco de dados IBM Db2 for LUW executado em uma EC2 instância da Amazon para um banco de dados Amazon Aurora MySQL compatível com o Amazon Aurora MySQL Edition na AWS.

O padrão descreve uma estratégia de migração on-line com tempo de inatividade mínimo para um banco de dados de origem Db2 de vários terabytes com um grande número de transações.

Esse padrão usa o AWS Schema Conversion Tool (AWS SCT) para converter o esquema do banco de dados Db2 em um esquema do Aurora MySQL-Compatible. Em seguida, o padrão usa o AWS Database Migration Service (AWS DMS) para migrar dados do banco de dados Db2 para o banco de dados Aurora MySQL-Compatible. Serão necessárias conversões manuais para o código que não foi convertido pelo AWS SCT.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa com uma nuvem privada virtual (VPC)
- AWS SCT
- AWS DMS

Versões do produto

- Versão mais recente do AWS SCT
- Db2 para Linux versão 11.1.4.4 e posterior

Arquitetura

Pilha de tecnologia de origem

- DB2/Linux x86-64 bits montado em uma instância EC2

Pilha de tecnologias de destino

- Uma instância de banco de dados do Amazon Aurora Edição Compatível com MySQL

Arquitetura de origem e destino

O diagrama a seguir mostra a arquitetura de migração de dados entre os bancos de dados Db2 de origem e Aurora MySQL-Compatible de destino. A arquitetura na Nuvem AWS inclui uma nuvem privada virtual (VPC), uma zona de disponibilidade, uma sub-rede pública para a instância do Db2 e a instância de replicação do AWS DMS, além de uma sub-rede privada para o banco de dados Aurora MySQL-Compatible.

Ferramentas

Serviços da AWS

- O Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado criado para a nuvem e compatível com o MySQL e o PostgreSQL.
- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino. O AWS SCT é compatível como uma origem IBM Db2 para Linux versões 9.1, 9.5, 9.7, 10.1, 10.5, 11,1 e 11.5.

Práticas recomendadas

Para obter informações, consulte Melhores práticas do AWS Database Migration Service.

Épicos

Configurar o banco de dados IBM Db2 de origem

Tarefa	Descrição	Habilidades necessárias
Crie o banco de dados IBM Db2 na Amazon EC2.	Você pode criar um banco de dados IBM Db2 em uma EC2 instância usando uma Amazon Machine Image (AMI) do AWS Marketplace ou instalando o software Db2 em uma EC2 instância. Inicie uma EC2 instância selecionando uma AMI para IBM Db2 (por exemplo, IBM Db2 v11.5.7 RHEL 7.9), que é semelhante a um banco de dados local.	AWS, DBA geral
Configurar grupos de segurança.	Configure as regras de entrada do grupo de segurança da VPC para SSH (Secure Shell) e TCP com as portas 22 e 50000, respectiv amente.	AWS geral
Criar uma instância de banco de dados.	Crie uma nova instância (usuário) e banco de dados (esquema) ou use a instância `db2inst1` padrão e o banco de dados de amostra. 1. Conecte-se à EC2 instância usando o terminal para se conectar ao banco de dados Db2. Como alternati	DBA

Tarefa	Descrição	Habilidades necessárias
	va, você pode instalar qualquer software cliente de banco de dados que se conecte ao banco de dados Db2. 2. Para definir a senha do usuário db2inst1, execute o comando `sudo passwd db2inst1`. 3. Para se conectar à instância db2inst1, execute o comando `sudo su - db2inst1`. 4. Para se conectar ao banco de dados Db2, execute o comando `db2`. 5. Para se conectar ao banco de dados modelo, execute o comando `connect to sample`. Como alternativa, conecte-se ao banco de dados que você criou. 6. Depois de se conectar à instância do banco de dados, crie objetos e insira dados nesses objetos usando instruções SQL do Db2.	
Verifique se a instância de banco de dados Db2 está disponível.	Para confirmar se a instância do banco de dados Db2 está em execução, use o comando `Db2pd -`.	DBA

Configurar o banco de dados Aurora MySQL-Compatible de destino

Tarefa	Descrição	Habilidades necessárias
Crie o banco de dados Aurora MySQL-Compatible.	Crie um banco de dados Amazon Aurora com compatibilidade com MySQL a partir do serviço AWS RDS • Crie um banco de dados no Amazon Aurora com compatibilidade com MySQL e a versão de sua escolha, por exemplo, Aurora (MySQL)–5.6.10a • Instale o aplicativo MySQL Workbench ou o software cliente de banco de dados de sua preferência, que permite que você se conecte ao banco de dados MySQL	AWS, DBA geral
Configurar grupos de segurança.	Configure as regras de entrada do grupo de segurança da VPC para conexões SSH e TCP.	AWS geral
Confirme se o banco de dados Aurora está disponível.	Para garantir que o banco de dados Aurora MySQL-Compatible esteja em execução, faça o seguinte: 1. Conecte-se à EC2 instância por meio de SSH. 2. Configure e conecte-se à instância do Aurora MySQL-Compatible a partir	DBA

Tarefa	Descrição	Habilidades necessárias
	do MySQL Workbench. Use o endpoint como nome do host, conforme mostrado no exemplo a seguir. `mysql-cluster-instance-1.cokmvis0v46q.us-east-1.rds.amazonaws.com` 3. Crie e conecte-se ao novo esquema (por exemplo,`mysql-sample-db2`). 4. Execute as instruções MySQL para verificar os esquemas e objetos no banco de dados.	

Configurar e executar o AWS SCT

Tarefa	Descrição	Habilidades necessárias
Instale a AWS SCT.	Baixe e instale a versão mais recente do AWS SCT (a versão mais recente atual 1.0.628).	AWS geral
Configure a AWS SCT.	1. Baixe os drivers Java Database Connectivity (JDBC) para IBM Db2 (versão 4.22.X) e MySQL (8.x). 2. Para configurar os drivers no AWS SCT, escolha	AWS geral

Tarefa	Descrição	Habilidades necessárias
	Configurações, Configurações globais e Drivers.	
Crie um projeto AWS SCT.	Crie um projeto e um relatório do AWS SCT que use o Db2 para LUW como o mecanismo de banco de dados de origem e o Aurora MySQL-Compatible para o mecanismo de banco de dados de destino. Para identificar os privilégios necessários para se conectar a um banco de dados Db2 para LUW, consulte Uso do Db2 para LUW como origem para o AWS SCT.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Valide os objetos.	Escolha Carregar esquema e valide os objetos. Atualize qualquer objeto incorreto no banco de dados de destino: 1. Conecte-se ao servidor do Amazon Aurora MySQL-Compatible fornecendo os detalhes da conexão e escolha Testar conexão. As conexões de origem e de destino devem ser bem-sucedidas antes que o AWS SCT possa iniciar o relatório de migração. 2. Após concluir o relatório , insira o esquema a ser convertido e escolha Finalizar. O AWS SCT lista todos os objetos de origem e destino que são convertidos e têm erros. 3. Analise os erros e elimine-os manualmente. 4. Depois de eliminar todos os erros, abra o menu de contexto (clique com o botão direito do mouse) do esquema e escolha Carregar esquema. 5. Escolha Aplicar ao banco de dados.	AWS, DBA geral

Tarefa	Descrição	Habilidades necessárias
	6. No MySQL Workbench, conecte-se ao banco de dados Aurora MySQL-Compatible e verifique o esquema e os objetos.	

Configurar e executar o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Criação de uma instância de replicação.	Faça login no Console de Gerenciamento da AWS, navegue até o serviço do AWS DMS e crie uma instância de replicação com configurações válidas para o grupo de segurança da VPC que você configurou para os bancos de dados de origem e destino.	AWS geral
Criar endpoints.	Crie o endpoint de origem para o banco de dados Db2 e crie o endpoint de destino para o banco de dados Aurora MySQL-Compatible: 1. Crie um endpoint para o IBM Db2 como origem escolhendo Seleciona r instância do banco de dados RDS e, em seguida, escolha a instância do Db2 que você criou. Os detalhes da configura	AWS geral

Tarefa	Descrição	Habilidades necessárias
	ção do endpoint serão preenchidos automatic amente. 2. Nas configurações específic as do endpoint, adicione os seguintes atributos extras de conexão. `CurrentLSN=<scan>; MaxKBytesPerRead=64; SetDataCaptureChanges=true` Se você não mencionar esses atributos, a conexão de teste do endpoint de origem não será bem-sucedida. Para obter mais informações, consulte Uso do IBM Db2 para LUW como origem para o AWS DMS. 3. Crie um endpoint para o Aurora MySQL-Compatible como destino escolhend o Selecionar instância do banco de dados RDS e, em seguida, escolhend o a instância do Aurora MySQL-Compatible que você criou. Os detalhes da configuração do endpoint serão preenchid os automaticamente. Para obter mais informações,	

Tarefa	Descrição	Habilidades necessárias
	consulte Uso de um banco de dados compatível com MySQL como destino do AWS Database Migration Service. 4. Testar os endpoints de origem e de destino. Confirme se ambos foram bem-sucedidos e estão disponíveis 5. Se um teste falhar, verifique se as regras de entrada do grupo de segurança são válidas.	

Tarefa	Descrição	Habilidades necessárias
Criar tarefas de migração.	Crie uma única tarefa de migração ou várias tarefas de migração para carga total e CDC ou validação de dados: 1. Para criar uma tarefa de migração de banco de dados, escolha a instância de replicação, o endpoint do banco de dados de origem e o endpoint do banco de dados de destino. Especifique o tipo de migração como Migrar dados existentes (carga total), Replicar somente alterações de dados (CDC) ou Migrar dados existente s e replicar alterações contínuas (carga total e CDC). 2. Em Mapeamentos de tabela, você pode configura r regras de seleção e de transformação nos formatos GUI ou JSON. 3. Em Regras de seleção, selecione o esquema, insira o nome da tabela e selecione a ação (incluir ou excluir) a ser configurada (por exemplo, Esquema: SAMPLE, Nome da tabela: %; Ação: Incluir).	AWS geral

Tarefa	Descrição	Habilidades necessárias
	4. Em Regras de transform ação, selecione o destino (esquema, tabela ou coluna). Selecione o nome do esquema e escolha a ação (minúscula/ maiúscula, prefixo, sufixo); por exemplo, Destino: Esquema; `mysql-sam ple-db` ; Ação: tornar minúscula. 5. Ative o monitoramento do Amazon CloudWatch Logs.	
Planeje a execução da produção.	Confirme o tempo de inatividade com as partes interessadas, como proprietários de aplicativos, para executar o AWS DMS em sistemas de produção.	Líder de migração
Execute as tarefas de migração.	1. Inicie a tarefa do AWS DMS que tem o status Pronto. 2. Monitore os registros de tarefas de migração no Amazon CloudWatch Logs em busca de erros.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Valide os dados.	Analise os resultados e os dados da tarefa de migração nos bancos de dados Db2 de origem e MySQL de destino: 1. Se o status for Carga completa, replicação contínua, a migração de dados de carga total com CDC será concluída e a validação estará em andamento. 2. Conecte-se ao banco de dados Aurora MySQL-Com patible e verifique os dados. 3. Verifique as alterações em andamento inserindo ou atualizando dados no banco de dados Db2.	DBA
Pare as tarefas de migração.	Depois de concluir com êxito a validação dos dados, interrompa as tarefas de validação de migração.	AWS geral

Solução de problemas

Problema	Solução
As conexões de teste de origem e de destino do AWS SCT estão falhando.	Configure as versões do driver JDBC e as regras de entrada do grupo de segurança da VPC para aceitar o tráfego de entrada.

Problema	Solução
A execução do teste do endpoint de origem Db2 falha.	Defina a configuração de conexão extra `CurrentLSN=<scan>;` .

Problema	Solução

A AWSDMS tarefa falha ao se conectar à origem do Db2 e o erro a seguir é retornado.
 	
`database is recoverable if either or both of the database configuration parameters LOGARCHMETH1 and LOGARCHMETH2 are set to ON`
	Para evitar o erro, execute os comandos a seguir:
	
	1. `$ db2 update db cfg for sample using LOGARCHMETH1 DISK:/home/db2inst1/logs`
	2. `$ db2stop`
	3. `$ db2start`
	4. `$ db2 connect to sample`
	
	```SQL1116N A connection to or activation of database "SAMPLE" cannot be made because of BACKUP PENDING. SQLSTATE=57019```
	
	5. `$ db2 backup database sample to ../logs`
	
	```SQL2036N The path for the file or device "../logs" is not valid```
	
	6. `$ cd`
	7. `$ pwd`
	
	```/home/db2inst1```
	
	8. `$ mkdir /tmp/backup`
	9. `$ db2 backup database sample to /tmp/backup`
	
	```Backup successful. The timestamp for this backup image is : 20190530084921```
	
	10. `$ db2 connect to sample`
	
	```Database Connection Information```

Problema	Solução

	`Database server = DB2/LINUX 9.7.1`
	`SQL authorization ID = DB2INST1`
	`Local database alias = SAMPLE`

Recursos relacionados

Amazon EC2

- Amazon EC2
- Guias EC2 do usuário da Amazon

Bancos de dados

- Banco de dados IBM Db2
- Amazon Aurora
- Como trabalhar com o Amazon Aurora MySQL

AWS SCT

- AWS DMS Schema Conversion
- Guia do usuário do AWS Schema Conversion Tool
- Usar a interface de usuário do AWS SCT
- Usar o IBM Db2 LUW como origem para o AWS SCT

AWS DMS

- AWS Database Migration Service
- Guia do usuário do AWS Database Migration Service
- Origens para a migração de dados
- Destinos para a migração de dados
- O AWS Database Migration Service e o AWS Schema Conversion Tool agora oferecem suporte ao IBM Db2 LUW como origem (publicação do blog)

- Migração de aplicativos que executam bancos de dados relacionais para a AWS

Migre um banco de dados Microsoft SQL Server da Amazon EC2 para o Amazon DocumentDB usando o AWS DMS

Criado por Umamaheswara Nooka (AWS)

Resumo

Esse padrão descreve como usar o AWS Database Migration Service (AWS DMS) para migrar um banco de dados Microsoft SQL Server hospedado em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para um banco de dados Amazon DocumentDB (com compatibilidade com o MongoDB).

A tarefa de replicação do AWS DMS lê a estrutura da tabela do banco de dados SQL Server, cria a coleção correspondente no Amazon DocumentDB e executa uma migração de carga completa.

Você também pode usar esse padrão para migrar uma instância de banco de dados SQL Server on-premises ou Amazon Relational Database Service (Amazon RDS) para SQL Server para o Amazon DocumentDB. Para obter mais informações, consulte o guia Migração de bancos de dados do Microsoft SQL Server para a nuvem AWS no site Recomendações da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados SQL Server existente em uma EC2 instância.
- Função fixa do banco de dados (db_owner) atribuída ao AWS DMS no banco de dados do SQL Server. Para obter mais informações, consulte Funções em nível de banco de dados na documentação do SQL Server.
- Familiaridade com o uso dos utilitários `mongodump`, `mongorestore`, `mongoexport` e `mongoimport` para mover dados para dentro e para fora de um cluster do Amazon DocumentDB.
- Microsoft SQL Server Management Studio, instalado e configurado.

Limitações

- O limite de tamanho do cluster no Amazon DocumentDB é 64 TB. Para obter mais informações, consulte Limites de cluster na documentação do Amazon DocumentDB.

- O AWS DMS não oferece suporte à mesclagem de várias tabelas de origem em uma única coleção do Amazon DocumentDB.
- Se o AWS DMS processar qualquer alteração de uma tabela de origem sem uma chave primária, ele ignorará as colunas de objetos grandes (LOB) na tabela de origem.

Arquitetura

Pilha de tecnologia de origem

- Amazon EC2

Arquitetura de destino

Pilha de tecnologias de destino

- Amazon DocumentDB

Ferramentas

- AWS DMS: o AWS Database Migration Service (AWS DMS) ajuda você a migrar bancos de dados com facilidade e segurança.
- Amazon DocumentDB: o Amazon DocumentDB (compatível com MongoDB) é um serviço de banco de dados rápido, confiável e totalmente gerenciado.
- Amazon EC2 — A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS.
- Microsoft SQL Server: o SQL Server é um sistema de gerenciamento de banco de dados relacional.
- SQL Server Management Studio (SSMS): o SSMS é uma ferramenta para gerenciar o SQL Server, incluindo acesso, configuração e administração de componentes do SQL Server.

Épicos

Criar e configurar uma VPC

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. Crie uma nuvem privada virtual (VPC) com um intervalo de blocos IPv4 CIDR.	Administrador de sistema
Crie grupos de segurança e rede ACLs.	No console da Amazon VPC, crie grupos de segurança e listas de controle de acesso à rede (rede ACLs) para sua VPC, de acordo com seus requisitos. Você também pode usar as configurações padrão para essas configurações. Para obter mais informações sobre essa e outras histórias , consulte a seção “Recursos relacionados”.	Administrador de sistema

Criar e configurar o cluster do Amazon DocumentDB

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do Amazon DocumentDB.	Abra o console do Amazon DocumentDB e escolha “Clusters”. Escolha “Create” e crie um cluster Amazon DocumentDB com uma instância. Importante: certifiqu e-se de configurar esse cluster	Administrador de sistema

Tarefa	Descrição	Habilidades necessárias
	com os grupos de segurança da sua VPC.	
Instale o shell do mongo.	O shell do Mongo é um utilitário de linha de comando que você usa para se conectar e consultar seu cluster do Amazon DocumentDB. Para instalá-lo, execute o comando “/etc/yum.repos.d/mongodb-org-3.6.repo” para criar o arquivo do repositório. Execute o comando “sudo yum install -y mongodb-org-shell” para instalar o shell mongo. Para criptografar dados em trânsito, faça download da chave pública do Amazon DocumentDB e conecte-se à sua instância do Amazon DocumentDB. Para obter mais informações sobre essas etapas, consulte a seção “Recursos relacionados”.	Administrador de sistema
Crie um banco de dados no cluster do Amazon DocumentDB.	Execute o comando “use” com o nome do seu banco de dados para criar um banco de dados em seu cluster Amazon DocumentDB.	Administrador de sistema

Criar e configurar a instância de replicação do AWS DMS

Tarefa	Descrição	Habilidades necessárias
Crie a instância de replicação do AWS DMS.	Abra o console do AWS DMS e escolha “Criar instância de replicação”. Insira um nome e uma descrição para sua tarefa de replicação. Escolha a classe da instância, a versão do mecanismo, o armazenamento, a VPC, o Multi-AZ e torne-a acessível ao público. Selecione a guia “Avançado” para definir as configurações de rede e criptografia. Especifique as configurações de manutenção e escolha “Criar instância de replicação”.	Administrador de sistema
Configurar o banco de dados do SQL Server.	Faça login no Microsoft SQL Server e adicione uma regra de entrada para comunicação entre o endpoint de origem e a instância de replicação do AWS DMS. Use o endereço IP privado da instância de replicação como origem. Importante: a instância de replicação e o endpoint de destino devem estar na mesma VPC. Use uma fonte alternativa no grupo de segurança se elas VPCs forem diferentes para as instâncias de origem e replicação.	Administrador de sistema

Crie e teste os endpoints de origem e destino no AWS DMS

Tarefa	Descrição	Habilidades necessárias
Crie endpoints para os bancos de dados de origem e destino.	Abra o console do AWS DMS e escolha “Connect Conectar endpoints de banco de dados de origem e de destino”. Especifique as informações de conexão para os bancos de dados de origem e de destino. Se necessário, escolha a guia “Avançado” para definir valores para “Atributos de conexão adicionais”. Baixe e use o pacote de certifica dos na configuração do seu endpoint.	Administrador de sistema
Teste as conexões do endpoint.	Selecione Run test (Executar o teste) para testar a conexão. Solucione qualquer mensagem de erro verifican do as configurações do grupo de segurança e as conexões com a instância de replicação do AWS DMS das instâncias de banco de dados de origem e de destino.	Administrador de sistema

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Crie a tarefa de migração do AWS DMS.	No console do AWS DMS, escolha “Tarefas”, “Criar	Administrador de sistema

Tarefa	Descrição	Habilidades necessárias
	tarefa". Especifique as opções de tarefas, incluindo os nomes dos endpoints de origem e destino e os nomes das instâncias de replicação. Em "Tipo de migração", escolha "Migrar dados existentes" e "Replicar somente alteraçõe s de dados". Escolha "Iniciar tarefa".	
Execute a tarefa de migração do AWS DMS.	Em "Configurações de tarefa", especifique as configura ções do modo de preparaçã o da tabela, como "Não fazer nada", "Soltar tabelas no destino", "Truncar" e "Incluir colunas LOB na replicação". Defina um tamanho máximo de LOB que o AWS DMS aceitará e escolha "Ativar registro". Deixe as "Configur ações avançadas" em seus valores padrão e escolha "Criar tarefa".	Administrador de sistema

Tarefa	Descrição	Habilidades necessárias
Monitorar a migração.	No console do AWS DMS, escolha “Tarefas” e escolha sua tarefa de migração. Escolha “Monitoramento de tarefas” para monitorar sua tarefa. A tarefa para por conta própria quando a migração de carga total é concluída e as alterações em cache são aplicadas.	Administrador de sistema

Testar e verificar a migração

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao cluster Amazon DocumentDB usando o shell do mongo.	Abra o console do Amazon DocumentDB e escolha o seu cluster em “Clusters”. Na guia “Conectividade e segurança ”, escolha “Conectar a este cluster com o shell do Mongo”.	Administrador de sistema
Verifique os resultados da sua migração.	Execute o comando “use” com o nome do seu banco de dados e, em seguida, execute o comando “show collectio ns”. Execute o comando “db. .count ();” com o nome do seu banco de dados. Se os resultados corresponderem ao seu banco de dados de origem, sua migração foi bem-sucedida.	Administrador de sistema

Recursos relacionados

Criar e configurar uma VPC

- Crie um grupo de segurança para a VPC
- Criar uma ACL de rede

Criar e configurar o cluster do Amazon DocumentDB

- Criar um cluster do Amazon DocumentDB
- Instale o shell do mongo para o Amazon DocumentDB
- Conectar ao cluster do Amazon DocumentDB

Criar e configurar a instância de replicação do AWS DMS

- Use instâncias de replicação públicas e privadas

Crie e teste os endpoints de origem e destino no AWS DMS

- Use o Amazon DocumentDB como destino para o AWS DMS
- Use um banco de dados SQL Server como origem para o AWS DMS
- Use endpoints do AWS DMS

Migrar dados

- Migre para o Amazon DocumentDB

Outros recursos

- Limitações de uso do SQL Server como origem para o AWS DMS
- Como usar o Amazon DocumentDB para criar e gerenciar aplicativos em grande escala

Migre um banco de dados ThoughtSpot Falcon local para o Amazon Redshift

Criado por Battulga Purevragchaa (AWS) e Antony Prasad Thevaraj (AWS)

Resumo

Os data warehouses on-premises exigem tempo e recursos administrativos significativos, especialmente para grandes conjuntos de dados. O custo financeiro de construir, manter e cultivar esses armazéns também é muito alto. Para ajudar a gerenciar custos, manter baixa a complexidade de extração, transformação e carregamento (ETL) e oferecer desempenho à medida que seus dados crescem, você deve escolher constantemente quais dados carregar e quais arquivar.

Ao migrar seus bancos de dados ThoughtSpot Falcon locais para a nuvem da Amazon Web Services (AWS), você pode acessar data lakes e data warehouses baseados na nuvem que aumentam a agilidade, a segurança e a confiabilidade dos aplicativos de sua empresa, além de reduzir os custos gerais de infraestrutura. O Amazon Redshift ajuda a reduzir significativamente o custo e a sobrecarga operacional de um data warehouse. Você também pode usar o Amazon Redshift Spectrum para analisar grandes quantidades de dados em seu formato nativo sem carregar dados.

Esse padrão descreve as etapas e o processo para migrar um banco de dados ThoughtSpot Falcon de um datacenter local para um banco de dados do Amazon Redshift na nuvem da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados ThoughtSpot Falcon hospedado em um data center local

Versões do produto

- ThoughtSpot versão 7.0.1

Arquitetura

O diagrama mostra o seguinte fluxo de trabalho:

1. Os dados são hospedados em um banco de dados relacional on-premises.

2. O AWS Schema Conversion Tool (AWS SCT) converte a linguagem de definição de dados (DDL) compatível com o Amazon Redshift.
3. Depois de criar as tabelas, você pode migrar dados usando o AWS Database Migration Service (AWS DMS).
4. Os dados são carregados no Amazon Redshift.
5. Os dados são armazenados no Amazon Simple Storage Service (Amazon S3) se você usa Redshift Spectrum ou já hospeda dados no Amazon S3.

Ferramentas

- AWS DMS: o AWS Data Migration Service (AWS DMS) ajuda você a migrar bancos de dados para a AWS de forma rápida e segura.
- O Amazon Redshift: o Amazon Redshift é um serviço de data warehouse rápido, totalmente gerenciado e em escala de petabytes que torna simples e econômica a análise eficiente de todos os seus dados usando as ferramentas de business intelligence existentes.
- AWS SCT: o AWS Schema Conversion Tool (AWS SCT) converte seu esquema de banco de dados existente de um mecanismo de banco de dados para outro.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Identifique a configuração apropriada do Amazon Redshift.	Identifique a configuração apropriada do cluster do Amazon Redshift com base em seus requisitos e volume de dados. Para obter mais informações, consulte Clusters do Amazon Redshift na documentação do Amazon Redshift.	DBA

Tarefa	Descrição	Habilidades necessárias
Pesquisar o Amazon Redshift para avaliar se ele atende aos seus requisitos.	Use o Amazon Redshift FAQs para entender e avaliar se o Amazon Redshift atende aos seus requisitos.	DBA

Preparar o cluster de destino do Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do Amazon Redshift.	Faça login no Console de gerenciamento da AWS, abra o console do Amazon Redshift e crie um cluster do Amazon Redshift em uma nuvem privada virtual (VPC). Para obter mais informações, consulte Criar um cluster em uma VPC na documentação do Amazon Redshift.	DBA
Conduzir uma PoC para o design do seu banco de dados do Amazon Redshift.	Siga as práticas recomendadas do Amazon Redshift conduzindo uma prova de conceito (PoC) para o design do seu banco de dados. Para obter mais informações, consulte Condução de uma prova de conceito do Amazon Redshift na documentação do Amazon Redshift.	DBA
Criar usuários do banco de dados.	Crie os usuários em seu banco de dados do Amazon	DBA

Tarefa	Descrição	Habilidades necessárias
	Redshift e conceda os perfis apropriados para acesso ao esquema e às tabelas. Para obter mais informaçõ es, consulte Conceção de privilégios de acesso para um usuário ou grupo de usuários na documentação do Amazon Redshift.	
Aplicar as configurações ao banco de dados de destino.	Aplique configurações ao banco de dados do Amazon Redshift de acordo com seus requisitos. Para obter mais informaçõ es sobre como habilitar parâmetros em nível de banco de dados, sessão e servidor, consulte a Referência de configuração na documenta ção do Amazon Redshift.	DBA

Criar objetos no cluster do Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Crie tabelas manualmen te com DDL no Amazon Redshift.	(Opcional) Se você usa o AWS SCT, as tabelas são criadas automaticamente. No entanto, se houver falhas na replicação DDLs, você precisará criar manualmente as tabelas	DBA

Tarefa	Descrição	Habilidades necessárias
Crie tabelas externas para Redshift Spectrum.	Crie uma tabela externa com um esquema externo para o Amazon Redshift Spectrum. Para criar tabelas externas, você deve ser o proprietário do esquema externo ou um superusuário do banco de dados. Para obter mais informaçõ es, consulte Criar tabelas externas para o Amazon Redshift Spectrum na documentação do Amazon Redshift.	DBA

Migrar dados usando o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Use o AWS DMS para migrar os dados.	Depois de criar o DDL das tabelas no banco de dados do Amazon Redshift, migre seus dados para o Amazon Redshift usando o AWS DMS. Para obter etapas e instruçõe s detalhadas, consulte Uso de um banco de dados do Amazon Redshift como destino do AWS DMS na documentação do AWS DMS.	DBA
Usar um comando COPY para carregar dados.	Use o comando `COPY` do Amazon Redshift para	DBA

Tarefa	Descrição	Habilidades necessárias
	carregar dados do Amazon S3 para o Amazon Redshift. Para obter mais informaçõ es, consulte Uso do comando COPY para carregar do Amazon S3 na documentação do Amazon Redshift.	

Validar o cluster do Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Valide os registros de origem e de destino.	Valide a contagem de tabelas para os registros de origem e destino que foram carregados do seu sistema de origem.	DBA
Implementar as práticas recomendadas do Amazon Redshift para ajuste de desempenho.	Práticas recomendadas do Amazon Redshift para projetar tabelas. Para obter mais informações, consulte a publicação As 10 melhores técnicas de ajuste de desempenho do Amazon Redshift no blog.	DBA
Otimize o desempenho da consulta.	O Amazon Redshift usa consultas baseadas em SQL para interagir com dados e objetos no sistema. A linguagem de manipulação de dados (DML) é um subconjun to da SQL que pode ser usado para ver, adicionar, alterar	DBA

Tarefa	Descrição	Habilidades necessárias
	e excluir dados. DDL é um subconjunto de SQL usado para adicionar, alterar excluir objetos do banco de dados, como tabelas e visualizações. Para obter mais informações, consulte Ajuste do desempenho da consulta na documentação do Amazon Redshift.	
Implementar o WLM.	Você pode usar o gerenciamento de workload (WLM) para definir diversas filas de consultas e rotear consultas para filas apropriadas no runtime. Para obter mais informações, consulte Implementação do gerenciamento do workload na documentação do Amazon Redshift.	DBA

Tarefa	Descrição	Habilidades necessárias
Trabalhe com escalonamento de simultaneidade.	Ao usar o atributo de escalabilidade de simultaneidade, você pode oferecer suporte a usuários simultâneos e consultas simultâneas praticamente ilimitadas, com desempenho de consulta consistentemente rápido. Para obter mais informações, consulte Trabalho com escalabilidade simultânea na documentação do Amazon Redshift.	DBA
Use as práticas recomendadas do Amazon Redshift para design de tabelas.	Ao planejar seu banco de dados, certas decisões importantes de design de tabela podem influenciar fortemente o desempenho geral da consulta. Para obter mais informações sobre como escolher a opções de design de tabelas mais adequada, consulte Práticas recomendadas do Amazon Redshift para projetar tabelas na documentação do Amazon Redshift.	DBA

Tarefa	Descrição	Habilidades necessárias
Crie visões materializadas no Amazon Redshift.	Uma visão materializada contém um conjunto de resultados pré-computados, com base em uma consulta SQL a uma ou mais tabelas base. É possível emitir instruções `SELECT` para consultar uma visão materializada, da mesma maneira como você pode consultar outras tabelas ou visualizações no banco de dados. Para obter mais informações, consulte Criar visões materializadas no Amazon Redshift na documentação do Amazon Redshift.	DBA

Tarefa	Descrição	Habilidades necessárias
Definir as junções entre as tabelas.	Para pesquisar mais de uma tabela ao mesmo tempo ThoughtSpot, você deve definir junções entre as tabelas especificando colunas que contêm dados correspon dentes em duas tabelas. Essas colunas representam a extremidade `primary key` da junção `foreign key`. Você pode defini-las usando o `ALTER TABLE` comando no Amazon Redshift ou. ThoughtSpot Para obter mais informações, consulte ALTER TABLE na documentação do Amazon Redshift.	DBA

Configurar a ThoughtSpot conexão com o Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Adicione uma conexão do Amazon Redshift.	Adicione uma conexão do Amazon Redshift ao seu banco de dados Falcon local ThoughtSpot . Para obter mais informaçõ es, consulte Adicionar uma conexão com o Amazon Redshift na ThoughtSpot documentação.	DBA

Tarefa	Descrição	Habilidades necessárias
Editar a conexão do Amazon Redshift.	Você pode editar a conexão do Amazon Redshift para adicionar tabelas e colunas. Para obter mais informaçõ es, consulte Editar uma conexão do Amazon Redshift na ThoughtSpot documenta ção.	DBA

Tarefa	Descrição	Habilidades necessárias
Remapear a conexão do Amazon Redshift.	Modifique os parâmetros de conexão editando o arquivo .yaml de mapeamento de origem que foi criado quando você adicionou a conexão do Amazon Redshift. Por exemplo, você pode remapear a tabela ou coluna existente para uma tabela ou coluna diferente em uma conexão de banco de dados existente. ThoughtSpot recomenda que você verifique as dependências antes e depois de remapear uma tabela ou coluna em uma conexão para garantir que elas sejam exibidas conforme necessário. Para obter mais informações, consulte Remapear uma conexão do Amazon Redshift na ThoughtSpot documentação.	DBA

Tarefa	Descrição	Habilidades necessárias
Excluir uma tabela da conexão do Amazon Redshift.	(Opcional) Se você tentar remover uma tabela em uma conexão do Amazon Redshift, ThoughtSpot verifica as dependências e mostra uma lista de objetos dependentes. Você pode escolher os objetos listados para excluí-los ou remover a dependência. Em seguida, você pode remover a tabela. Para obter mais informações, consulte Excluir uma tabela de uma conexão do Amazon Redshift na ThoughtSpot documentação.	DBA

Tarefa	Descrição	Habilidades necessárias
Exclua uma tabela com objetos dependentes de uma conexão do Amazon Redshift.	(Opcional) Se você tentar excluir uma tabela com objetos dependentes, a operação será bloqueada . Uma janela `Cannot delete` é exibida, com uma lista de links para objetos dependentes. Quando todas as dependências forem removidas, você poderá excluir a tabela Para obter mais informações, consulte Excluir uma tabela com objetos dependentes de uma conexão do Amazon Redshift na ThoughtSpot documentação.	DBA
Excluir uma conexão do Amazon Redshift.	(Opcional) Como uma conexão pode ser usada em várias fontes de dados ou visualizações, você deve excluir todas as fontes e tarefas que usam essa conexão antes de excluir a conexão do Amazon Redshift. Para obter mais informaçõ es, consulte Excluir uma conexão do Amazon Redshift na ThoughtSpot documenta ção.	DBA

Tarefa	Descrição	Habilidades necessárias
Verificar a referência de conexão do Amazon Redshift.	Certifique-se de fornecer as informações necessárias para sua conexão com o Amazon Redshift usando a referência de conexão na ThoughtSpot documentação.	DBA

Mais informações

- Análise orientada por IA em qualquer escala com o Amazon ThoughtSpot Redshift
- Preços do Amazon Redshift
- Conceitos básicos do AWS SCT
- Conceitos básicos do Amazon Redshift
- Uso de agentes de extração de dados
- Chick-fil-A melhora a velocidade de obtenção de insights com ThoughtSpot a AWS

Migrar um banco de dados Oracle para o Amazon DynamoDB usando AWS DMS

Criado por Rambabu Karnena (AWS)

Resumo

Esse padrão orienta você pelas etapas de migração de um banco de dados Oracle para o Amazon DynamoDB usando o AWS Database Migration Service (AWS DMS). Ele abrange três tipos de bancos de dados de origem:

- Bancos de dados Oracle on-premises.
- Bancos de dados Oracle na Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS) para instâncias do banco de dados do Oracle

Nessa prova de conceito, esse padrão se concentra na migração de uma instância de banco de dados do Amazon RDS para Oracle.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo que se conecta a um banco de dados do Amazon RDS para Oracle
- Uma tabela criada no banco de dados de origem Amazon RDS para Oracle com uma chave primária e dados de amostra

Limitações

- Objetos de banco de dados Oracle, como procedimentos, funções, pacotes e gatilhos, não são considerados para migração porque o Amazon DynamoDB não oferece suporte a esses objetos de banco de dados.

Versões do produto

- Esse padrão se aplica a todas as edições e versões dos bancos de dados Oracle que são compatíveis com o AWS DMS. Para obter mais informações, consulte Como usar um banco de dados Oracle como origem para o AWS DMS e usar um banco de dados do Amazon DynamoDB

como destino para o AWS DMS. Recomendamos que você use as versões mais recentes do AWS DMS para obter o suporte mais abrangente de versões e atributos.

Arquitetura

Pilha de tecnologia de origem

- Amazon RDS para instâncias de banco de dados Oracle, Oracle na EC2 Amazon ou bancos de dados Oracle locais

Pilha de tecnologias de destino

- Amazon DynamoDB

Arquitetura de migração de dados da AWS

Ferramentas

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS. Esse padrão usa o Amazon RDS para Oracle.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	Crie uma nuvem privada virtual (VPC) e uma sub-rede privada na conta da AWS.	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Criar grupos de segurança e listas de controle de acesso à rede.	Para obter mais informações, consulte a documentação da AWS.	Administrador de sistemas
Configurar e iniciar a instância de banco de dados Amazon RDS para Oracle	Para obter mais informações, consulte a documentação da AWS.	DBA, administrador de sistemas

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Para criar um perfil do IAM para acesso ao DynamoDB.	No console do AWS Identity and Access Management (IAM) crie a função, anexe a política `AmazonDynamoDBFullAccess to it`, e selecione o AWS DMS como o serviço.	Administrador de sistemas
Crie uma instância de replicação do AWS DMS para migração.	A instância de replicação deve estar na mesma zona de disponibilidade e VPC que o banco de dados de origem.	Administrador de sistemas
Criação de endpoints no AWS DMS de origem e de destino.	Para criar o endpoint do banco de dados de origem, você tem duas opções: • No console do Amazon RDS, escolha Bancos de dados, identificador de banco de dados, conectividade e segurança e escolha o endpoint.	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	• No console do AWS DMS, escolha Selecionar instância de banco de dados do RDS. Para criar o endpoint do banco de dados de destino, escolha a função nome do recurso da Amazon (ARN) na tarefa anterior para acessar o DynamoDB.	
Crie uma tarefa do AWS DMS para carregar as tabelas de origem do banco de dados Oracle no DynamoDB.	Escolha os nomes dos endpoints de origem e destino e a instância de replicação nas etapas anteriores. O tipo pode ser carga total. Escolha o esquema Oracle e especifiq ue% para selecionar todas as tabelas.	Administrador de sistemas
Valide as tabelas no DynamoDB.	Para ver os resultados da migração, escolha Tabelas no painel de navegação esquerdo no console do DynamoDB.	DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Modifique o código do aplicativ o	Para se conectar e recuperar dados do DynamoDB, atualize o código do aplicativo.	Proprietário do aplicativ o, DBA, administrador de sistemas

Substituir

Tarefa	Descrição	Habilidades necessárias
Troque os clientes do aplicativo para usar o DynamoDB.		DBA, proprietário do aplicativo, administrador de sistemas

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Desligar recursos da AWS	Por exemplo, o desligamento da instância Amazon RDS para Oracle, DynamoDB e da instância de replicação do AWS DMS.	DBA, administrador de sistemas
Colete métricas.	As métricas incluem o tempo de migração, as porcentagens do trabalho manual e do trabalho realizado pela ferramenta e a economia de custos.	DBA, proprietário do aplicativo, administrador de sistemas

Recursos relacionados

- AWS Database Migration Service e Amazon DynamoDB: o que você precisa saber (postagem do blog)
- Uso de um banco de dados Oracle como origem para o AWS DMS
- Uso do banco de dados Amazon DynamoDB como destino para o AWS Database Migration Service
- Melhores práticas para migrar do RDBMS para o Amazon DynamoDB (whitepaper)

Migre uma tabela particionada do Oracle para o PostgreSQL usando o AWS DMS

Criado por Saurav Mishra (AWS) e Eduardo Valentim (AWS)

Resumo

Esse padrão descreve como acelerar o carregamento de uma tabela particionada do Oracle para o PostgreSQL usando o AWS Database Migration Service (AWS DMS), que não oferece suporte ao particionamento nativo. O banco de dados PostgreSQL de destino pode ser instalado no Amazon Elastic Compute Cloud (Amazon) ou pode ser uma instância de banco de dados EC2 Amazon Relational Database Service (Amazon RDS) para PostgreSQL ou Amazon Aurora PostgreSQL Compatible Edition.

O upload de uma tabela particionada inclui as seguintes etapas:

1. Crie uma tabela principal semelhante à tabela de partições do Oracle, mas não inclua nenhuma partição.
2. Crie tabelas secundárias que herdarão da tabela principal que você criou na etapa 1.
3. Crie uma função de procedimento e um gatilho para lidar com as inserções na tabela principal.

No entanto, como o gatilho é acionado para cada inserção, a carga inicial usando o AWS DMS pode ser muito lenta.

Para acelerar os carregamentos iniciais do Oracle para o PostgreSQL 9.0, esse padrão cria uma tarefa separada do AWS DMS para cada partição e carrega as tabelas secundárias correspondentes. Em seguida, você cria um gatilho durante a substituição.

O PostgreSQL versão 10 suporta particionamento nativo. No entanto, você pode decidir usar o particionamento herdado em alguns casos. Para obter mais informações, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados do Oracle de origem com uma tabela particionada
- Um banco de dados do PostgreSQL na AWS

Versões do produto

- PostgreSQL 9.0

Arquitetura

Pilha de tecnologia de origem

- Uma tabela particionada no Oracle

Pilha de tecnologias de destino

- Uma tabela particionada no PostgreSQL (na EC2 Amazon, Amazon RDS for PostgreSQL ou Aurora PostgreSQL)

Arquitetura de destino

Ferramentas

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.

Épicos

Configurar o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Crie as tabelas no PostgreSQL.	Crie as tabelas principal e secundária correspondentes no PostgreSQL com as condições de verificação necessárias para partições.	DBA
Crie a tarefa do AWS DMS para cada partição.	Inclua a condição do filtro da partição na tarefa do AWS DMS. Mapeie as partições	DBA

Tarefa	Descrição	Habilidades necessárias
	para as tabelas secundári as correspondentes do PostgreSQL.	
Execute as tarefas do AWS DMS usando carga total e captura de dados alterados (CDC).	Verifique se o parâmetro `StopTaskCachedChan gesApplied` está definido como `true` e se o parâmetro `StopTaskCachedChan gesNotApplied` está definido como `false`.	DBA

Substituir

Tarefa	Descrição	Habilidades necessárias
Interrompe as tarefas de replicação.	Antes de interromper as tarefas, confirme se a origem e o destino estão sincroniz ados.	DBA
Crie um gatilho na tabela principal.	Como a tabela principal receberá todos os comandos de inserção e atualização, crie um gatilho que roteará esses comandos para as respectiv as tabelas secundárias com base na condição de particion amento.	DBA

Recursos relacionados

- AWS DMS
- Particionamento de tabelas (documentação do PostgreSQL)

Mais informações

Embora a versão 10 do PostgreSQL ofereça suporte ao particionamento nativo, você pode decidir usar o particionamento herdado para os seguintes casos de uso:

- O particionamento impõe uma regra de que todas as partições devem ter o mesmo conjunto de colunas que a principal, mas a herança de tabelas permite que os filhos tenham colunas extras.
- A herança de tabelas oferece suporte a várias heranças.
- O particionamento declarativo oferece suporte somente ao particionamento de listas e intervalos. Com a herança de tabelas, você pode dividir os dados como quiser. No entanto, se a exclusão da restrição não puder remover partições de forma eficaz, o desempenho da consulta será prejudicado.
- Algumas operações precisam de um bloqueio mais forte ao usar o particionamento declarativo do que ao usar a herança de tabelas. Por exemplo, adicionar ou remover uma partição de ou para uma tabela particionada exige um bloqueio `ACCESS EXCLUSIVE` na tabela principal, enquanto um bloqueio `SHARE UPDATE EXCLUSIVE` é suficiente para a herança regular.

Ao usar partições de trabalho separadas, você também pode recarregar partições se houver algum problema de validação do AWS DMS. Para melhorar o desempenho e o controle da replicação, execute tarefas em instâncias de replicação separadas.

Migre do Amazon RDS para Oracle para o Amazon RDS para MySQL

Criado por Jitender Kumar (AWS), Neha Sharma (AWS) e Srini Ramaswamy (AWS)

Resumo

Esse padrão fornece orientação para migrar uma instância de banco de dados Amazon Relational Database Service (Amazon RDS) para Oracle para uma instância de banco de dados Amazon RDS for MySQL na Amazon Web Services (AWS). O padrão usa o AWS Database Migration Service (AWS DMS) e a AWS Schema Conversion Tool (AWS SCT).

O padrão fornece as melhores práticas para lidar com a migração de procedimentos armazenados. Ele também abrange e codifica alterações para dar suporte à camada de aplicação.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Banco de dados de origem do Amazon RDS para Oracle.
- Banco de dados de destino do Amazon RDS para MySQL. Os bancos de dados de origem e destino devem estar na mesma nuvem privada virtual (VPC). Se você estiver usando vários VPCs, ou precisar ter as permissões de acesso necessárias.
- Grupos de segurança que permitem a conectividade entre os bancos de dados de origem e de destino, o AWS SCT, o servidor de aplicativos e o AWS DMS.
- Uma conta de usuário com o privilégio necessário para executar o AWS SCT no banco de dados de origem.
- Registro suplementar habilitado para execução do AWS DMS no banco de dados de origem.

Limitações

- O limite de tamanho do banco de dados Amazon RDS de origem e destino é 64 TB. Para obter informações sobre o tamanho do Amazon RDS, consulte a documentação da AWS.
- O Oracle não diferencia maiúsculas de minúsculas para objetos de banco de dados, mas o MySQL não. O AWS SCT pode lidar com esse problema ao criar um objeto. No entanto, é necessário algum trabalho manual para suportar a insensibilidade total de maiúsculas e minúsculas.

- Essa migração não usa extensões do MySQL para habilitar funções nativas da Oracle. O AWS SCT processa a maior parte da conversão, mas é necessário algum trabalho para alterar o código manualmente.
- Alterações do driver Java Database Connectivity (driver JDBC) são necessárias no aplicativo.

Versões do produto

- Amazon RDS para Oracle 12.2.0.1 e versões posteriores. Para ver as versões do RDS para Oracle atualmente suportadas, consulte a documentação da AWS.
- Amazon RDS para MySQL 8.0.15 e versões posteriores. Para ver as versões atualmente suportadas do RDS para MySQL, consulte a documentação da AWS.
- AWS DMS versão 3.3.0 e posterior. Consulte a documentação da AWS para obter mais informações sobre endpoints de origem e endpoints de destino compatíveis com o AWS DMS.
- AWS SCT versão 1.0.628 e posterior. Veja a matriz de suporte de endpoints de origem e destino do AWS SCT na documentação da AWS.

Arquitetura

Pilha de tecnologia de origem

- Amazon RDS para Oracle. Para obter mais informações, consulte Usando um banco de dados Oracle como fonte para o AWS DMS.

Pilha de tecnologias de destino

- Amazon RDS para MySQL. Para obter mais informações, consulte Uso de um banco de dados compatível com MySQL como destino para o AWS DMS.

Arquitetura de migração

No diagrama a seguir, o AWS SCT copia e converte objetos de esquema do banco de dados de origem do Amazon RDS for Oracle e envia os objetos para o banco de dados de destino do Amazon RDS for MySQL. O AWS DMS replica dados do banco de dados de origem e os envia para a instância do Amazon RDS for MySQL.

Ferramentas

- O AWS Data Migration Service ajuda você a migrar armazenamentos de dados para a nuvem da AWS ou entre combinações de configurações na nuvem e no local.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS. Esse padrão usa Amazon RDS para Oracle e Amazon RDS para MySQL.
- O AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Validar versões e mecanismos do banco de dados de origem e de destino.		DBA
Identifique os requisitos de hardware para a instância do servidor de destino.		DBA, SysAdmin
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, SysAdmin
Escolha o tipo de instância adequado (capacidade, atributos de armazenamento e atributos de rede).		DBA, SysAdmin
Identifique os requisitos de segurança do acesso à rede		DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
para os bancos de dados de origem e de destino.		
Escolha uma estratégia de migração de aplicativos.	Considere se você quer tempo de inatividade total ou parcial para atividades de substitui ção.	DBA SysAdmin, proprietário do aplicativo

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma VPC e sub-redes.		SysAdmin
Crie grupos de segurança e listas de controle de acesso à rede (ACLs).		SysAdmin
Configure e inicie a instância do Amazon RDS para Oracle.		DBA, SysAdmin
Configure e inicie a instância do Amazon RDS para MySQL.		DBA, SysAdmin
Prepare um caso de teste para validação da conversão de código.	Isso ajudará no teste de unidade do código convertido.	DBA, Desenvolvedor
Configure a instância do AWS DMS.		
Configure endpoints de origem e destino no AWS DMS.		

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Gere o script do banco de dados de destino usando o AWS SCT.	Verifique a precisão do código que foi convertido pelo AWS SCT. Será necessário algum trabalho manual.	DBA, Desenvolvedor
No AWS SCT, escolha a configuração “Sem distinção entre maiúsculas e minúsculas”.	No AWS SCT, escolha Configurações do projeto, Diferenciação entre maiúsculas e minúsculas e maiúsculas e minúsculas.	DBA, Desenvolvedor
No AWS SCT, escolha não usar a função nativa da Oracle.	Em Configurações do projeto, verifique as funções TO_CHAR/TO_NUMBER/TO_DATE.	DBA, Desenvolvedor
Faça alterações no código “sql %notfound”.	Talvez seja necessário converter o código manualmente.	
Consulte tabelas e objetos em procedimentos armazenados (use consultas em minúsculas).		DBA, Desenvolvedor
Crie o script primário depois que todas as alterações forem feitas e, em seguida, implante o script primário no banco de dados de destino.		DBA, Desenvolvedor
Teste de unidade os procedimentos armazenados		

Tarefa	Descrição	Habilidades necessárias
e as chamadas de aplicativos usando dados de amostra.		
Limpe os dados que foram criados durante o teste de unidade.		DBA, Desenvolvedor
Elimine restrições de chave no banco de dados de destino.	Essa etapa é necessária para carregar dados iniciais. Se você não quiser eliminar as restrições de chave estrangeira, deverá criar uma tarefa de migração para dados específicos das tabelas primária e secundária.	DBA, Desenvolvedor
Coloque chaves primárias e chaves exclusivas no banco de dados de destino.	Essa etapa resulta em melhor desempenho para a carga inicial.	DBA, Desenvolvedor
Habilite o log suplementar no banco de dados de origem.		DBA
Crie uma tarefa de migração para a carga inicial no AWS DMS e, em seguida, execute-a.	Selecionar a opção Migrar dados existentes.	DBA
Adicione as chaves primárias e estrangeiras ao banco de dados de destino.	Restrições precisam ser adicionadas após a carga inicial.	DBA, Desenvolvedor
Crie uma tarefa de migração para a replicação contínua.	A replicação contínua mantém o banco de dados de destino sincronizado com o banco de dados de origem.	DBA

Migrar aplicativos

Tarefa	Descrição	Habilidades necessárias
Substitua as funções nativas do Oracle pelas funções nativas do MySQL.		Proprietário do App
Certifique-se de que somente nomes em minúsculas sejam usados para objetos de banco de dados em consultas SQL.		DBA SysAdmin, proprietário do aplicativo

Vá para o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Encerre o servidor do aplicativo.		Proprietário do App
Valide se os bancos de dados de origem e de destino estão em sincronia.		DBA, proprietário do aplicativo
Encerre a instância de banco de dados do Amazon RDS para Oracle.		DBA
Pare a tarefa de migração.	Isso será interrompido automaticamente depois que você concluir a etapa anterior.	DBA
Altere a conexão JDBC do Oracle para o MySQL.		Proprietário do aplicativo, DBA
Inicie o aplicativo.		DBA SysAdmin, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Revise e valide os documentos do projeto.		DBA, SysAdmin
Reúna métricas sobre o tempo de migração, porcentagem de tarefas manuais versus tarefas de ferramentas, economia de custos, etc.		DBA, SysAdmin
Pare e exclua instâncias do AWS DMS.		DBA
Remova os endpoints de origem e de destino.		DBA
Remova as tarefas de migração.		DBA
Faça uma instância de banco de dados do Amazon RDS para Oracle.		DBA
Exclua a instância de banco de dados do Amazon RDS para Oracle.		DBA
Encerre e exclua quaisquer outros recursos temporários da AWS que você usou.		DBA, SysAdmin
Feche o projeto e forneça feedback, se houver.		DBA

Recursos relacionados

- AWS DMS
- AWS SCT
- Preços do Amazon RDS
- Conceitos básicos do AWS DMS
- Conceitos básicos do Amazon RDS

Migre do IBM Db2 na Amazon para o EC2 Aurora compatível com PostgreSQL usando o AWS DMS e o AWS SCT

Criado por Sirsendu Halder (AWS) e Abhimanyu Chhabra (AWS)

Resumo

Esse padrão fornece orientação para migrar um banco de dados IBM Db2 em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para uma instância de banco de dados Amazon Aurora PostgreSQL compatível com o PostgreSQL. Este padrão usa o AWS Database Migration Service (AWS DMS) e a AWS Schema Conversion Tool (AWS SCT) para migração de dados e conversão de esquemas.

O padrão visa uma estratégia de migração on-line com pouco ou nenhum tempo de inatividade para um banco de dados IBM Db2 de vários terabytes que tem um grande número de transações. Recomendamos que você converta as colunas em chaves primárias (PKs) e chaves estrangeiras (FKs) com o tipo de dados `NUMERIC` para `INT` ou `BIGINT` no PostgreSQL para melhorar o desempenho.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados IBM Db2 de origem em uma instância EC2

Versões do produto

- DB2/LINUXX8664 versão 11.1.4.4 e posterior

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Db2 em uma instância EC2

Pilha de tecnologias de destino

- Uma instância de banco de dados compatível com o Aurora compatível com PostgreSQL versão 10.18 ou superior

Arquitetura de migração de banco de dados

Ferramentas

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar banco de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises. O banco de dados de origem permanece totalmente operacional durante a migração, o que minimiza o tempo de inatividade de aplicativos que dependem do banco de dados. Você pode usar o AWS DMS para migrar seus dados de e para os bancos de dados comerciais e de código aberto mais usados no mercado. O AWS DMS é compatível com migrações heterogêneas entre diferentes plataformas de banco de dados, como IBM Db2 para Aurora compatível com PostgreSQL, versão 10.18 ou superior. Para obter detalhes, consulte Origens para migração de dados e Destinos para migração de dados na documentação do AWS DMS.
- A AWS Schema Conversion Tool (AWS SCT) facilita as migrações heterogêneas de banco de dados convertendo automaticamente o esquema do banco de dados de origem e a maioria dos objetos de código do banco de dados, incluindo exibições, procedimentos armazenados e funções, em um formato compatível com o banco de dados de destino. Todos os objetos que não são convertidos automaticamente são claramente marcados para que possam ser convertidos manualmente para concluir a migração. O AWS SCT também pode digitalizar o código-fonte do aplicativo em busca de instruções SQL incorporadas e convertê-las.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de banco de dados do Aurora compatível com o PostgreSQL.	Para criar a instância do banco de dados, siga as instruções na documentação da AWS. Para Tipo de mecanismo, escolha Amazon Aurora. Em Edição, escolha Amazon Aurora Edição compatível com PostgreSQL.	Amazon RDS

Tarefa	Descrição	Habilidades necessárias
	A instância de banco de dados do Aurora compatível com o PostgreSQL versão 10.18 ou superior deve estar na mesma nuvem privada virtual (VPC) que o banco de dados IBM Db2 de origem.	

Converta o esquema do banco de dados

Tarefa	Descrição	Habilidades necessárias
Instale e verifique o AWS SCT.	1. Instale o AWS SCT seguindo as etapas na documentação do AWS SCT. 2. Verifique a instalação seguindo os procedimentos na documentação do AWS SCT.	Administrador da AWS, DBA, engenheiro de migração
Inicie o AWS SCT e crie um projeto.	Para iniciar a ferramenta AWS SCT e criar um novo projeto para executar um relatório de avaliação da migração do banco de dados, siga as instruções na documentação do AWS SCT.	Engenheiro de migração
Adicione servidores de banco de dados e crie uma regra de mapeamento.	1. Adicione servidores de banco de dados de origem e destino seguindo as instruções na documentação do AWS SCT.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	2. Crie uma regra de mapeamento para definir a plataforma de banco de dados de destino para seu banco de dados de origem. Para obter instruções, consulte a documentação do AWS SCT.	
Crie um relatório de avaliação de migração do banco de dados.	Crie o relatório de avaliação da migração do banco de dados seguindo as etapas na documentação do AWS SCT.	Engenheiro de migração
Visualizar o relatório de avaliação.	Use a guia Resumo do relatório de avaliação da migração do banco de dados para visualizar o relatório e analisar os dados. Essa análise ajudará você a determinar a complexidade da migração. Para obter mais informações, consulte a documentação do AWS SCT.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Converta o esquema.	Para converter seus esquemas de banco de dados de origem: 1. No console do AWS SCT, escolha Visualizar e, então, Visualização principal. 2. Selecione o objeto ou nó principal do esquema de origem, abra o menu de contexto (clique com o botão direito do mouse) e, depois, selecione Converter esquema. Para obter mais informações, consulte a documentação do AWS SCT.	Engenheiro de migração
Para aplicar o esquema de banco de dados convertido à instância de banco de dados de destino	1. Escolha o elemento do esquema no painel direito do seu projeto que exibe o esquema planejado para sua instância de banco de dados de destino. 2. Abra o menu de contexto (clique com o botão direito do mouse) do elemento do esquema e escolha Aplicar ao banco de dados. Para obter mais informações, consulte a documentação do AWS SCT.	Engenheiro de migração

Migre seus dados

Tarefa	Descrição	Habilidades necessárias
Configure grupos de parâmetros de VPC e banco de dados.	Configure grupos de parâmetros de VPC e banco de dados e configure as regras e os parâmetros de entrada necessários para a migração. Para obter instruções, consulte a documentação do AWS DMS. Para o grupo de segurança da VPC, selecione a instância do Db2 e a EC2 instância de banco de dados compatível com o Aurora PostgreSQL. Essa instância de replicação deve estar na mesma VPC das instâncias de banco de dados de origem e de destino.	Engenheiro de migração
Prepare instâncias de banco de dados de origem e destino.	Prepare as instâncias de banco de dados de origem e destino para a migração. Em um ambiente de produção, o banco de dados de origem já existirá. Para o banco de dados de origem, o nome do servidor deve ser o Sistema de Nomes de Domínio (DNS) público da EC2 instância em que o Db2 está sendo executado. Para nome de usuário, você pode usar `db2inst1` seguido pela	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	porta, que será 5000 para IBM Db2.	
Crie um EC2 cliente e endpoints da Amazon.	1. Crie um EC2 cliente Amazon. Você usa esse cliente para preencher seu banco de dados de origem com dados para replicar. Você também usa esse cliente para verificar a replicação executand o consultas no banco de dados de destino. 2. Crie endpoints para o banco de dados de origem e a instância de banco de dados de destino a ser usada nas próximas etapas. Para obter instruções, consulte a documenta ção do AWS DMS. Crie endpoints separados para os bancos de dados de origem e destino. Para a versão 10.18 ou superior do Aurora compatível com o PostgreSQL, a porta será 5432 e você poderá obter o nome do servidor no endpoint da instância de banco de dados.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de replicação.	Crie uma instância de replicação usando o console do AWS DMS e especifique os endpoints de origem e destino. A instância de replicação realiza a migração de dados entre os endpoints. Para obter mais informações, consulte a documentação do AWS DMS.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Crie uma tarefa do AWS DMS para migrar os dados.	Crie uma tarefa para carregar as tabelas de origem do IBM Db2 na instância de banco de dados PostgreSQL de destino seguindo as etapas na documentação do AWS DMS. • Para origem e destino, use os nomes dos endpoints de origem e destino. • O tipo de migração pode ser carga total. • Para a regra do esquema, você pode usar o esquema `inst1` do banco de dados Db2. • Para o nome da tabela, especifique `%` para migrar todas as tabelas. Quando o carregamento estiver concluído, você verá as tabelas Db2 do esquema `inst1` aparecendo no banco de dados do Aurora compatível com o PostgreSQL.	Engenheiro de migração

Recursos relacionados

Referências

- Documentação do Amazon Aurora
- Documentação do FDW (wrapper de dados estrangeiros) do PostgreSQL
- Documentação IMPORTAR ESQUEMA ESTRANGEIROS do PostgreSQL

- Documentação do AWS DMS
- Documentação do AWS SCT

Tutoriais e vídeos

- Conceitos básicos do AWS DMS (passo a passo)
- Introdução à Amazon EC2 — Elastic Cloud Server e hospedagem com AWS (vídeo)

Migre do Oracle 8i ou 9i para o Amazon RDS for PostgreSQL usando o AWS DMS SharePlex

Criado por Kumar Babu P G (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados Oracle 8i ou 9i on-premises para o Amazon Relational Database Service (Amazon RDS) para PostgreSQL ou Amazon Aurora PostgreSQL. O AWS Database Migration Service (AWS DMS) não oferece suporte ao Oracle 8i ou 9i como fonte, então a Quest SharePlex replica dados de um banco de dados 8i ou 9i local para um banco de dados Oracle intermediário (Oracle 10g ou 11g), que é compatível com o AWS DMS.

Da instância intermediária da Oracle, o esquema e os dados são migrados para o banco de dados PostgreSQL na AWS usando o AWS Schema Conversion Tool (AWS SCT) e o AWS DMS. Esse método ajuda a obter streaming contínuo de dados do banco de dados Oracle de origem para a instância de banco de dados PostgreSQL de destino, com atraso mínimo de replicação. Nessa implementação, o tempo de inatividade é limitado ao tempo necessário para criar ou validar todas as chaves estrangeiras, acionadores e sequências no banco de dados PostgreSQL de destino.

A migração usa uma instância do Amazon Elastic Compute Cloud (Amazon EC2) com o Oracle 10g ou 11g instalado para hospedar as alterações do banco de dados Oracle de origem. O AWS DMS usa essa instância Oracle intermediária como origem para transmitir os dados para o Amazon RDS para PostgreSQL ou Aurora PostgreSQL. A replicação de dados pode ser pausada e retomada do banco de dados Oracle on-premises para a instância intermediária da Oracle. Também pode ser pausada e retomada da instância intermediária do Oracle para o banco de dados PostgreSQL de destino para que você possa validar os dados usando a validação de dados do AWS DMS ou uma ferramenta de validação de dados personalizada.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle 8i ou 9i de origem em um datacenter on-premises
- AWS Direct Connect configurado entre o datacenter on-premises e a AWS
- Drivers de conectividade de banco de dados Java (JDBC) para conectores AWS SCT instalados em uma máquina local ou na instância em que o AWS SCT EC2 está instalado

- Familiaridade com o uso de um banco de dados Oracle como origem para o AWS DMS
- Familiaridade com o uso de um banco de dados PostgreSQL como destino para o AWS DMS
- Familiaridade com a replicação de SharePlex dados da Quest

Limitações

- O limite de tamanho do banco de dados é 64 TB.
- O banco de dados Oracle on-premises deve ser Enterprise Edition

Versões do produto

- Oracle 8i ou 9i para o banco de dados de origem
- Oracle 10g ou 11g para o banco de dados intermediário
- PostgreSQL 9.6 ou mais recente

Arquitetura

Pilha de tecnologia de origem

- Banco de dados do Oracle 8i ou 9i
- Missão SharePlex

Pilha de tecnologias de destino

- Amazon RDS para PostgreSQL ou Amazon PostgreSQL

Arquitetura de origem e destino

Ferramentas

- AWS DMS: o AWS Database Migration Service (AWS DMS) ajuda você a migrar bancos de dados com rapidez e segurança. O banco de dados de origem permanece totalmente operacional

durante a migração, o que minimiza o tempo de inatividade de aplicativos que dependem do banco de dados. O AWS DMS pode migrar seus dados dos/para os bancos de dados comerciais e de código aberto mais usados no mercado.

- AWS SCT: o AWS Schema Conversion Tool (AWS SCT) torna as migrações heterogêneas de banco de dados previsíveis ao converter automaticamente o esquema do banco de dados de origem e a maioria do código personalizado, incluindo exibições, procedimentos armazenados e funções, para um formato compatível com o banco de dados de destino. Os objetos que não são convertidos automaticamente são claramente marcados para que possam ser convertidos manualmente para concluir a migração. O AWS SCT também pode examinar o código-fonte do seu aplicativo em busca de instruções SQL incorporadas e convertê-las como parte de um projeto de conversão de esquema de banco de dados. Durante esse processo, o AWS SCT executa a otimização de código nativo de nuvem convertendo funções legadas do Oracle e do SQL Server em seus equivalentes da AWS, para ajudar você a modernizar seus aplicativos enquanto migra seus bancos de dados. Quando a conversão do esquema estiver concluída, o AWS SCT pode ajudar a migrar dados de uma variedade de data warehouses para o Amazon Redshift usando agentes de migração de dados integrados.
- Quest SharePlex — SharePlex A Quest é uma ferramenta de replicação de Oracle-to-Oracle dados para mover dados com o mínimo de tempo de inatividade e sem perda de dados.

Épicos

Crie a EC2 instância e instale o Oracle

Tarefa	Descrição	Habilidades necessárias
Configure a rede para a Amazon EC2.	Crie a nuvem privada virtual (VPC), sub-redes, gateway da Internet, tabelas de rotas e grupos de segurança.	AWS SysAdmin
Crie a nova EC2 instância.	Selecione a Amazon Machine Image (AMI) para a EC2 instância. Escolha o tamanho da instância e configure os detalhes da instância: o número de instâncias (1), a VPC e a sub-rede da etapa	AWS SysAdmin

Tarefa	Descrição	Habilidades necessárias
	anterior, atribuição automática de IP público e outras opções. Adicione armazenamento, configure grupos de segurança e execute a instância. Quando solicitado, crie e salve um par de chaves para a próxima etapa.	
Instale o Oracle na EC2 instância.	Adquira as licenças e os binários Oracle necessários e instale o Oracle 10g ou 11g na instância. EC2	DBA

Configurar SharePlex em uma EC2 instância e configurar a replicação de dados

Tarefa	Descrição	Habilidades necessárias
Configurar SharePlex.	Crie uma EC2 instância da Amazon e instale os SharePlex binários compatíveis com o Oracle 8i ou 9i.	AWS SysAdmin, DBA
Configure a replicação de dados.	Siga as SharePlex melhores práticas para configurar a replicação de dados de um banco de dados Oracle 8i/9i local para uma instância Oracle 10g/11g.	DBA

Converta o esquema do banco de dados Oracle em PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Configure o AWS SCT.	Crie um novo relatório e, em seguida, conecte-se ao Oracle como origem e ao PostgreSQL como destino. Nas configurações do projeto, abra a guia SQL Scripting e altere o script SQL de destino para Vários arquivos.	DBA
Converta o esquema do banco de dados Oracle.	Na guia Ação, escolha Gerar relatório, Converter esquema e, depois, Salvar como SQL.	DBA
Modifique os scripts SQL gerados pelo AWS SCT.		DBA

Crie e configure a instância de banco de dados do Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Criar a instância de banco de dados do Amazon RDS	No console do Amazon RDS, crie uma nova instância de banco de dados PostgreSQL.	AWS SysAdmin, DBA
Configure a instância de banco de dados.	Especifique a versão do mecanismo de banco de dados, a classe da instância de banco de dados, a implantação Multi-AZ, o tipo de armazenamento e o armazenamento alocado. Insira o identificador da instância de banco de dados,	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
	um nome de usuário principal e uma senha mestra.	
Configure rede e segurança.	Especifique a VPC, o grupo de sub-redes, a acessibilidade pública, a preferência da zona de disponibilidade e os grupos de segurança.	AWS SysAdmin, DBA
Configure as opções do banco de dados.	Especifique o nome do banco de dados, a porta, o grupo de parâmetros, a criptografia e a chave mestra.	AWS SysAdmin, DBA
Configure os backups.	Especifique o período de retenção do backup, a janela do backup, a hora de início, a duração e se as tags devem ser copiadas para instantân eos.	AWS SysAdmin, DBA
Configure opções de monitoramento.	Habilite ou desabilite insights de monitoramento e desempenho avançados.	AWS SysAdmin, DBA
Configure opções de manutenção.	Especifique a atualizaç ão automática da versão secundária, a janela de manutenção e o dia, a hora e a duração de início.	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
Execute os scripts de pré-migração do AWS SCT.	Na instância do Amazon RDS, execute esses scripts: create_database.sql, create_sequence.sql, create_table.sql, create_view.sql, and create_function.sql.	AWS SysAdmin, DBA

Migrar dados usando o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de replicação no AWS DMS.	Preencha os campos para nome, classe da instância, VPC (igual à EC2 instância), Multi-AZ e acessibilidade pública. Na seção de configuração avançada, especifique o armazenamento alocado, o grupo de sub-rede, a zona de disponibilidade, os grupos de segurança da VPC e a chave raiz do AWS Key Management Service (AWS KMS).	AWS SysAdmin, DBA
Crie o endpoint do banco de dados de origem.	Especifique o nome do endpoint, tipo, mecanismo de origem (Oracle), nome do servidor (nome DNS EC2 privado da Amazon), porta, modo SSL, nome de usuário, senha, SID, VPC (especifique a VPC que tem a instância	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
	de replicação) e instância de replicação. Para testar a conexão, escolha Executar teste e, em seguida, crie o endpoint. Você também pode definir as seguintes configurações avançadas: maxFileSize e numberDataType Escala.	
Crie a tarefa de replicação do AWS DMS.	Especifique o nome da tarefa, a instância de replicação, os endpoints de origem e destino e a instância de replicação. Para tipo de migração escolha “Migrar dados existentes e replicar alterações contínuas ”. Desmarque a caixa de seleção “Iniciar tarefa ao criar”.	AWS SysAdmin, DBA
Defina as configurações da tarefa de replicação do AWS DMS.	Para o modo de preparação da tabela de destino, escolha “Não fazer nada”. Pare a tarefa após a conclusão da carga completa para criar chaves primárias. Especifiq ue o modo LOB limitado ou completo e ative as tabelas de controle. Opcionalmente, você pode definir a configuração CommitRate avançada.	DBA

Tarefa	Descrição	Habilidades necessárias
Configure os mapeamentos da tabela.	Na seção mapeamentos de tabela, crie uma regra de inclusão para todas as tabelas em todos os esquemas incluídos na migração e, em seguida, crie uma regra de exclusão. Adicione três regras de transformação para converter os nomes do esquema, da tabela e da coluna para letra minúscula e adicione quaisquer outras regras necessárias para essa migração específica.	DBA
Iniciar a tarefa.	Iniciar a tarefa de replicação. Verifique se a carga total está em execução. Execute ALTER SYSTEM SWITCH LOGFILE no banco de dados Oracle primário para iniciar a tarefa.	DBA
Execute os scripts de meio da migração do AWS SCT.	No Amazon RDS para PostgreSQL, execute esses scripts: create_index.sql e create_constraint.sql.	DBA
Reinicie a tarefa para continuar a captura de dados de alteração (CDC).	Na instância de banco de dados Amazon RDS para PostgreSQL, execute VACUUM e reinicie a tarefa do AWS DMS para aplicar as alterações do CDC em cache.	DBA

Substitua para o banco de dados PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Verifique os registros de log e as tabelas de metadados do AWS DMS.	Valide todos os erros e corrija, se necessário.	DBA
Interrompa todas as dependências do Oracle.	Desligue os receptores no banco de dados Oracle e execute ALTER SYSTEM SWITCH LOGFILE. Interrompa a tarefa do AWS DMS quando ele não mostrar nenhuma atividade.	DBA
Execute os scripts de pós-migração do AWS SCT.	No Amazon RDS para PostgreSQL, execute esses scripts: create_foreign_key_constraint.sql e create_triggers.sql.	DBA
Conclua qualquer etapa adicional do Amazon RDS para PostgreSQL.	Incremente as sequências para corresponder ao Oracle, se necessário; execute VACUUM e ANALYZE e tire um instantâneo para fins de conformidade.	DBA
Escolha conectar ao Amazon RDS para PostgreSQL.	Remova os grupos de segurança do AWS DMS do Amazon RDS para PostgreSQL, adicione grupos de segurança de produção e direcione seus aplicativos para o novo banco de dados.	DBA

Tarefa	Descrição	Habilidades necessárias
Limpe os recursos AWS DMS.	Remova os endpoints, as tarefas de replicação, as instâncias de replicação e a instância. EC2	SysAdmin, DBA

Recursos relacionados

- Documentação do AWS DMS
- Documentação do AWS SCT
- Definição de preço para o Amazon RDS para PostgreSQL
- Uso de um banco de dados Oracle como origem para o AWS DMS
- Uso de um banco de dados PostgreSQL como destino do AWS DMS
- SharePlex Documentação da Quest

Migre do Oracle 8i ou 9i para o Amazon RDS para PostgreSQL usando visões materializadas e o AWS DMS

Criado por Kumar Babu P G (AWS) e Pragnesh Patel (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados Oracle legado 8i ou 9i on-premises para o Amazon Relational Database Service (Amazon RDS) para PostgreSQL ou Amazon Aurora Edição Compatível com PostgreSQL.

O AWS Database Migration Service (AWS DMS) não é compatível com o Oracle 8i ou 9i como fonte, então esse padrão usa uma instância intermediária de banco de dados Oracle compatível com o AWS DMS, como Oracle 10g ou 11g. Ele também usa o atributo de visões materializadas para migrar dados da instância Oracle 8i/9i de origem para a instância intermediária do Oracle 10g/11g.

O AWS Schema Conversion Tool (AWS SCT) converte o esquema do banco de dados e o AWS DMS migra os dados para o banco de dados PostgreSQL de destino.

Esse padrão ajuda os usuários que desejam migrar de um bancos de dados Oracle legados com o mínimo de tempo de inatividade do banco de dados. Nessa implementação, o tempo de inatividade seria limitado ao tempo necessário para criar ou validar todas as chaves estrangeiras, acionadores e sequências no banco de dados de destino.

O padrão usa instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com um banco de dados Oracle 10g/11g instalado para ajudar o AWS DMS a transmitir os dados. Você pode pausar temporariamente a replicação de streaming do banco de dados Oracle on-premises para a instância intermediária da Oracle para permitir que o AWS DMS atualize a validação de dados ou use outra ferramenta de validação de dados. A instância de banco de dados PostgreSQL e o banco de dados Oracle intermediário terão os mesmos dados quando o AWS DMS terminar de migrar as alterações atuais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle 8i ou 9i de origem em um datacenter on-premises
- AWS Direct Connect configurado entre o datacenter on-premises e a AWS

- Drivers de conectividade de banco de dados Java (JDBC) para conectores AWS SCT instalados em uma máquina local ou na instância em que o AWS SCT EC2 está instalado
- Familiaridade com o uso de um banco de dados Oracle como origem para o AWS DMS
- Familiaridade com o uso de um banco de dados PostgreSQL como destino para o AWS DMS

Limitações

- O limite de tamanho do banco de dados é 64 TB.

Versões do produto

- Oracle 8i ou 9i para o banco de dados de origem
- Oracle 10g ou 11g para o banco de dados intermediário
- PostgreSQL 10.17 ou superior

Arquitetura

Pilha de tecnologia de origem

- Banco de dados do Oracle 8i ou 9i

Pilha de tecnologias de destino

- Amazon RDS para PostgreSQL ou Aurora compatível com PostgreSQL

Arquitetura de destino

Ferramentas

- O AWS DMS ajuda a migrar bancos de dados com rapidez e de forma segura. O banco de dados de origem permanece totalmente operacional durante a migração, o que minimiza o tempo de inatividade de aplicativos que dependem do banco de dados. O AWS DMS pode migrar seus dados dos/para os bancos de dados comerciais e de código aberto mais usados no mercado.
- O AWS SCT converte automaticamente o esquema e uma maioria dos objetos do código do banco de dados, incluindo visualizações, procedimentos armazenados e funções para um

formato compatível com o banco de dados de destino. Os objetos que não são convertidos automaticamente são claramente marcados para que possam ser convertidos manualmente para concluir a migração. O AWS SCT também pode examinar o código-fonte do seu aplicativo em busca de instruções SQL incorporadas e convertê-las como parte de um projeto de conversão de esquema de banco de dados. Durante esse processo, o AWS SCT executa a otimização de código nativo de nuvem convertendo funções legadas do Oracle e do SQL Server em seus equivalentes da AWS, para ajudar você a modernizar seus aplicativos enquanto migra seus bancos de dados. Quando a conversão do esquema estiver concluída, o AWS SCT pode ajudar a migrar dados de uma variedade de data warehouses para o Amazon Redshift usando agentes de migração de dados integrados.

Práticas recomendadas

Para obter as práticas recomendadas para atualizar visões materializadas, consulte a seguinte documentação da Oracle:

- Atualizar visões materializadas
- Atualização rápida para visões materializadas

Épicos

Instale o Oracle em uma EC2 instância e crie visualizações materializadas

Tarefa	Descrição	Habilidades necessárias
Configure a rede para a EC2 instância.	Crie a nuvem privada virtual (VPC), sub-redes, gateway da Internet, tabelas de rotas e grupos de segurança.	AWS SysAdmin
Crie a EC2 instância.	Selecione a Amazon Machine Image (AMI) para a EC2 instância. Escolha o tamanho da instância e configure os detalhes da instância: o número de instâncias (1), a VPC e a sub-rede da etapa	AWS SysAdmin

Tarefa	Descrição	Habilidades necessárias
	anterior, atribuição automática de IP público e outras opções. Adicione armazenamento, configure grupos de segurança e execute a instância. Quando solicitado, crie e salve um par de chaves para a próxima etapa.	
Instale o Oracle na EC2 instância.	Adquira as licenças e os binários Oracle necessários e instale o Oracle 10g ou 11g na instância. EC2	DBA
Configure a rede Oracle.	Modifique ou adicione entradas em `listener.ora` para se conectar ao banco de dados Oracle 8i/9i de origem on-premises e, em seguida, crie os links do banco de dados.	DBA
Criar visão materializada	Identifique os objetos do banco de dados a serem replicados no banco de dados Oracle 8i/9i de origem e, em seguida, crie visões materializadas para todos os objetos usando o link do banco de dados.	DBA

Tarefa	Descrição	Habilidades necessárias
Implante scripts para atualizar as visões materializadas nos intervalos necessários.	Desenvolva e implante scripts para atualizar visualizações materializadas nos intervalo s necessários na instância Amazon EC2 Oracle 10g/11g. Use a opção de atualização incremental para atualizar visões materializadas.	DBA

Converta o esquema do banco de dados Oracle em PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Configure o AWS SCT.	Crie um novo relatório e, em seguida, conecte-se ao Oracle como origem e ao PostgreSQ L como destino. Nas configura ções do projeto, abrir a guia SQL Scripting. Altere o script SQL de destino para Vários arquivos. (O AWS SCT não é compatível com bancos de dados Oracle 8i/9i, então você precisa restaurar o despejo somente do esquema na instância intermediária do Oracle 10g/11g e usá-lo como fonte para o AWS SCT.)	DBA
Converta o esquema do banco de dados Oracle.	Na guia Ação, escolha Gerar relatório, Converter esquema e depois, Salvar como SQL.	DBA
Modifique os scripts SQL.	Faça modificações com base nas práticas recomendadas.	DBA, DevDBA

Tarefa	Descrição	Habilidades necessárias
	Por exemplo, mude para tipos de dados adequados e desenvolva equivalentes do PostgreSQL para funções específicas do Oracle.	

Crie e configure a instância de banco de dados do Amazon RDS para hospedar o banco de dados convertido

Tarefa	Descrição	Habilidades necessárias
Criar a instância de banco de dados do Amazon RDS	No console do Amazon RDS, crie uma nova instância de banco de dados PostgreSQL.	AWS SysAdmin, DBA
Configure a instância de banco de dados.	Especifique a versão do mecanismo de banco de dados, a classe da instância de banco de dados, a implantação Multi-AZ, o tipo de armazenamento e o armazenamento alocado. Insira o identificador da instância de banco de dados, um nome de usuário principal e uma senha mestra.	AWS SysAdmin, DBA
Configure rede e segurança.	Especifique a VPC, o grupo de sub-redes, a acessibilidade pública, a preferência da zona de disponibilidade e os grupos de segurança.	DBA, SysAdmin
Configure as opções do banco de dados.	Especifique o nome do banco de dados, a porta, o grupo de	DBA, AWS SysAdmin

Tarefa	Descrição	Habilidades necessárias
	parâmetros, a criptografia e a chave mestra.	
Configure os backups.	Especifique o período de retenção do backup, a janela do backup, a hora de início, a duração e se as tags devem ser copiadas para instantân eos.	AWS SysAdmin, DBA
Configure opções de monitoramento.	Habilite ou desabilite insights de monitoramento e desempenho avançados.	AWS SysAdmin, DBA
Configure opções de manutenção.	Especifique a atualizaç ão automática da versão secundária, a janela de manutenção e o dia, a hora e a duração de início.	AWS SysAdmin, DBA
Execute os scripts de pré-migração do AWS SCT.	Na instância de destino do Amazon RDS para PostgreSQ L, crie o esquema do banco de dados usando os scripts SQL do AWS SCT com outras modificações. Isso pode incluir a execução de vários scripts e a criação de usuários, criação de banco de dados, criação de esquemas, tabelas, visualiza ções, perfis e outros objetos de código.	AWS SysAdmin, DBA

Migrar dados usando o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de replicação no AWS DMS.	Preencha os campos para nome, classe da instância, VPC (igual à EC2 instância), Multi-AZ e acessibil idade pública. Na seção de configuração avançada, especificar o armazenamento alocado, o grupo de sub-rede, a Zona de disponibilidade, os Grupos de segurança da VPC e a chave do AWS Key Management Service (AWS KMS).	AWS SysAdmin, DBA
Crie o endpoint do banco de dados de origem.	Especifique o nome do endpoint, o tipo, o mecanismo de origem (Oracle), o nome do servidor (o nome DNS privado da EC2 instância), a porta, o modo SSL, o nome de usuário, a senha, o SID, a VPC (especifique a VPC que tem a instância de replicaçã o) e a instância de replicaçã o. Para testar a conexão, escolha Executar teste e, em seguida, crie o endpoint. Você também pode definir as seguintes configurações avançadas: maxFileSizee numberDataTypeEscala.	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
Conecte o AWS DMS ao Amazon RDS para PostgreSQL.	Crie um grupo de segurança de migração para conexões entre VPCs, se seu banco de dados PostgreSQL estiver em outra VPC.	AWS SysAdmin, DBA
Crie o endpoint do banco de dados de destino.	Especifique o nome do endpoint, o tipo, o mecanismo de origem (PostgreSQL), o nome do servidor (endpoint do Amazon RDS), a porta, o modo SSL, o nome do usuário, a senha, o nome do banco de dados, a VPC (especificar a VPC que tem a instância de replicação) e a instância de replicação. Para testar a conexão, escolha Executar teste e, em seguida, crie o endpoint. Você também pode definir as seguintes configurações avançadas : maxFileSizee numberDataTypeEscala.	AWS SysAdmin, DBA
Crie a tarefa de replicação do AWS DMS.	Especifique o nome da tarefa, a instância de replicação, os endpoints de origem e destino e a instância de replicação. Para tipo de migração, escolha Migrar dados existentes e replicar alterações contínuas. Desmarque a caixa de seleção Iniciar tarefa ao criar.	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
Defina as configurações da tarefa de replicação do AWS DMS.	Para o modo de preparação da tabela de destino, escolha Não fazer nada. Interrompa a tarefa após a conclusão do carregamento total (para criar chaves primárias). Especifiq ue o modo LOB limitado ou completo e ative as tabelas de controle. Opcionalmente, você pode definir a configura ção CommitRateavançada.	DBA
Configure os mapeamentos da tabela.	Na seção Mapeamentos de tabela, crie uma regra de inclusão para todas as tabelas em todos os esquemas incluídos na migração e, em seguida, crie uma regra de exclusão. Adicione três regras de transformação para converter os nomes do esquema, da tabela e da coluna para letra minúscula e adicione quaisquer outras regras que você precise para essa migração específica.	DBA
Iniciar a tarefa.	Iniciar a tarefa de replicação. Verifique se a carga total está em execução. Execute `ALTER SYSTEM SWITCH LOGFILE` no banco de dados Oracle primário para iniciar a tarefa.	DBA

Tarefa	Descrição	Habilidades necessárias
Execute os scripts de meio da migração do AWS SCT.	No Amazon RDS para PostgreSQL, execute os seguintes scripts: `create_index.sql` e `create_constraint.sql` (se o esquema completo não tiver sido criado inicialmente).	DBA
Reinicie a tarefa para continuar a captura de dados de alteração (CDC).	Execute `VACUUM` na instância de banco de dados Amazon RDS para PostgreSQL e reinicie a tarefa do AWS DMS para aplicar as alterações do CDC em cache.	DBA

Substitua para o banco de dados PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Verifique os logs e as tabelas de validação do AWS DMS.	Verifique e corrija quaisquer erros de replicação ou validação.	DBA
Pare de usar o banco de dados Oracle no on-premises e suas dependências.	Interrompa todas as dependências do Oracle, desligue os receptores no banco de dados Oracle e execute `ALTER SYSTEM SWITCH LOGFILE`. Interrompa a tarefa do AWS DMS quando ele não mostrar nenhuma atividade.	DBA
Execute os scripts de pós-migração do AWS SCT.	No Amazon RDS para PostgreSQL, execute	DBA

Tarefa	Descrição	Habilidades necessárias
	esses scripts: `create_foreign_key_constraint.sql and create_triggers.sql` . Certifique-se de que as sequências estejam atualizadas.	
Conclua etapas adicionais do Amazon RDS para PostgreSQL.	Incremente as sequências para corresponder ao Oracle, se necessário; execute `VACUUM` e `ANALYZE` e tire um snapshot para fins de conformidade.	DBA
Escolha conectar ao Amazon RDS para PostgreSQL.	Remova os grupos de segurança do AWS DMS do Amazon RDS para PostgreSQL, adicione grupos de segurança de produção e direcione seus aplicativos para o novo banco de dados.	DBA
Limpe os objetos do AWS DMS.	Remova os endpoints, as tarefas de replicação, as instâncias de replicação e a instância. EC2	SysAdmin, DBA

Recursos relacionados

- Documentação do AWS DMS
- Documentação do AWS SCT
- Definição de preço para o Amazon RDS para PostgreSQL
- Uso de um banco de dados Oracle como origem para o AWS DMS
- Uso de um banco de dados PostgreSQL como destino do AWS DMS

Migre do Oracle na Amazon EC2 para o Amazon RDS for MySQL usando o AWS DMS e o AWS SCT

Criado por Anil Kunapareddy (AWS) e Harshad Gohil

Resumo

Gerenciar bancos de dados Oracle em instâncias do Amazon Elastic Compute Cloud (Amazon EC2) requer recursos e pode ser caro. Mover esses bancos de dados para uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS) para MySQL facilitará seu trabalho ao otimizar o orçamento geral de TI. O Amazon RDS para MySQL também fornece atributos como Multi-AZ, escalabilidade e backups automáticos.

Esse padrão orienta você na migração de um banco de dados Oracle de origem na Amazon EC2 para uma instância de banco de dados Amazon RDS for MySQL de destino. Ele usa o AWS Database Migration Service (AWS DMS) para migrar os dados e o AWS Schema Conversion Tool (AWS SCT) para converter o esquema e os objetos do banco de dados de origem em um formato compatível com o Amazon RDS para MySQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem com serviços de instância e receptor em execução, no modo ARCHIVELOG
- Um banco de dados do Amazon RDS para MySQL de destino, com armazenamento suficiente para migração de dados

Limitações

- O AWS DMS não cria um esquema no banco de dados de destino; você precisa fazer isso. O nome do esquema já deve existir para o destino. As tabelas do esquema de origem são importadas para o usuário/esquema, que o AWS DMS usa para se conectar à instância de destino. Você deverá criar várias tarefas de replicação se tiver que migrar vários schemas.

Versões do produto

- Todas as edições do banco de dados do Oracle para versões 10.2 e posteriores, 11g e até 12.2 e 18c. Para obter a lista mais recente de versões compatíveis, consulte Uso de um banco de dados do Oracle como origem para o AWS DMS e Uso de um banco de dados compatível com MySQL como destino para o AWS DMS. Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos. Para obter informações sobre as versões do banco de dados do Oracle suportadas pelo AWS SCT, consulte a documentação do AWS SCT.
- O AWS DMS oferece suporte às versões 5.5, 5.6 e 5.7 do MySQL.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Oracle em uma EC2 instância

Pilha de tecnologias de destino

- Instância do banco de dados do Amazon RDS para MySQL

Arquitetura de migração de dados

Arquitetura de origem e destino

Ferramentas

- AWS DMS — O AWS Database Migration Service (AWS DMS) é um serviço web que você pode usar para migrar dados do seu banco de dados local, em uma instância de banco de dados Amazon RDS ou em um banco de dados em uma instância, para um banco de dados em um serviço da AWS, como Amazon RDS for MySQL ou uma EC2 instância. EC2 Você também pode migrar um banco de dados de um serviço da AWS para um banco de dados on-premises. Você pode migrar dados entre mecanismos de banco de dados heterogêneos ou homogêneos.
- AWS SCT: o AWS Schema Conversion Tool (AWS SCT) torna as migrações heterogêneas de banco de dados previsíveis ao converter automaticamente o esquema do banco de dados de origem e a maioria do código personalizado, incluindo exibições, procedimentos armazenados e funções, para um formato compatível com o banco de dados de destino. Depois de converter seu

esquema de banco de dados e objetos de código usando o AWS SCT, você pode usar o AWS DMS para migrar dados do banco de dados de origem para o banco de dados de destino para concluir seus projetos de migração.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Identificar as versões e mecanismos dos bancos de dados de origem e de destino.		DBA/Desenvolvedor
Identificar a instância de replicação do DMS.		DBA/Desenvolvedor
Identifique os requisitos de armazenamento, como tipo e capacidade de armazenamento.		DBA/Desenvolvedor
Identifique os requisitos de rede, como latência e largura de banda.		DBA/Desenvolvedor
Identifique os requisitos de hardware para as instâncias do servidor de origem e de destino (com base na lista de compatibilidade e nos requisitos de capacidade da Oracle).		DBA/Desenvolvedor
Identifique os requisitos de segurança de acesso à rede para bancos de dados de origem e de destino.		DBA/Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Instale os drivers AWS SCT e Oracle.		DBA/Desenvolvedor
Determine uma estratégia de backup.		DBA/Desenvolvedor
Determine os requisitos de disponibilidade.		DBA/Desenvolvedor
Identifique a migração de aplicativos e a estratégia de transição.		DBA/Desenvolvedor
Selecione o tipo de instância de banco de dados adequado com base nos atributos de capacidade, armazenamento e rede.		DBA/Desenvolvedor

Configure o ambiente.

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC). A origem, o destino e a instância de replicação devem estar na mesma VPC. Também é bom tê-los em uma mesma zona de disponibilidade.		Desenvolvedor
Crie os grupos de segurança necessários para acesso ao banco de dados.		Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Gere e configure um par de chaves.		Desenvolvedor
Configure sub-redes, zonas de disponibilidade e blocos CIDR.		Desenvolvedor

Configurar a fonte: banco de dados Oracle na EC2 instância

Tarefa	Descrição	Habilidades necessárias
Instale o Oracle Database na Amazon EC2 com os usuários e funções necessários.		DBA
Execute as três etapas na próxima coluna para acessar o Oracle de fora da EC2 instância.	1. Mude o host local `tnsnames` para o DNS EC2 público da Amazon. 2. Mude o host local `listener` para o DNS EC2 público da Amazon. 3. Interromper e reiniciar o receptor.	DBA
Quando a Amazon EC2 é reiniciada, o DNS público muda. Certifique-se de atualizar o DNS EC2 público da Amazon em 'tnsnames' e 'listener' ou use um endereço IP elástico.		DBA/Desenvolvedor
Configure o grupo de segurança da EC2 instância para que a instância de replicação e os clientes		DBA/Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
necessários possam acessar o banco de dados de origem.		

Configurar o destino: Amazon RDS para MySQL

Tarefa	Descrição	Habilidades necessárias
Configure e inicie a instância de banco de dados do Amazon RDS para MySQL.		Desenvolvedor
Crie o espaço de tabela necessário na instância de banco de dados do Amazon RDS para MySQL.		DBA
Configure o grupo de segurança para que a instância de replicação e os clientes necessários possam acessar o banco de dados de destino.		Desenvolvedor

Configure o AWS SCT e crie um esquema no banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Instale os drivers AWS SCT e Oracle.		Desenvolvedor
Insira os parâmetros apropriados e conecte-se à origem e ao destino.		Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Gere um relatório de conversão de esquema.		Desenvolvedor
Corrija o código e o esquema conforme necessário, especialmente espaços de tabela e aspas, e execute no banco de dados de destino.		Desenvolvedor
Valide o esquema na origem x no destino antes de migrar os dados.		Desenvolvedor

Migrar dados usando o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Para carga total e captura de dados alterados (CDC) ou apenas CDC, deve-se configurar um atributo de conexão extra.		Desenvolvedor
O usuário especificado nas definições do banco de dados do Oracle do AWS DMS de origem deve receber todos os privilégios necessários. Para obter uma lista completa, consulte https://docs.aws.amazon.com/dms/ latest/userguide/CHAP _source.oracle.html #CHAP_Source .Oracle.Self-Managed.		DBA/Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Habilite o log suplementar no banco de dados de origem.		DBA/Desenvolvedor
Para carga total e captura de dados de alteração (CDC) ou apenas CDC, ative o modo ARCHIVELOG no banco de dados de origem.		DBA
Crie endpoints de origem e destino e teste as conexões.		Desenvolvedor
Quando os endpoints forem conectados com êxito, crie uma tarefa de replicação.		Desenvolvedor
Selecione somente CDC (ou) carga total mais CDC na tarefa para capturar alteraçõe s somente para replicação contínua (ou) carga total mais alterações em andamento, respectivamente.		Desenvolvedor
Execute a tarefa de replicaçã o e monitore CloudWatch os logs da Amazon.		Desenvolvedor
Valide os dados nos bancos de dados de origem e de destino.		Desenvolvedor

Migre seu aplicativo e substitua

Tarefa	Descrição	Habilidades necessárias
Siga as etapas da sua estratégia de migração de aplicativos.		DBA, desenvolvedor, proprietário do aplicativo
Siga as etapas da sua estratégia de substituição/troca de aplicativos.		DBA, desenvolvedor, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Valide o esquema e os dados nos bancos de dados de origem x de destino.		DBA/Desenvolvedor
Reúna métricas sobre o tempo de migração, porcentagem de manual x ferramenta, economia de custos etc.		DBA/Developer/AppOwner
Revise os documentos e artefatos do projeto.		DBA/Developer/AppOwner
Encerre os recursos temporários da AWS.		DBA/Desenvolvedor
Feche o projeto e forneça feedback.		DBA/Developer/AppOwner

Recursos relacionados

- Documentação do AWS DMS

- Site do AWS DMS
- Publicações no blog do AWS DMS
- Estratégias para migrar o Oracle Database para a AWS
- Amazon RDS para Oracle FAQs
- Perguntas frequentes sobre a Oracle
- Amazon EC2
- Amazon EC2 FAQs
- Licenciamento do software Oracle no ambiente de computação em nuvem

Migrar do Oracle para o Amazon DocumentDB usando o AWS DMS

Criado por Sashikanta Pattanayak (AWS) e Munesh Siddappa (AWS)

Resumo

Esse padrão fornece orientação para migrar um banco de dados do Orable para um Amazon DocumentDB (compativel com MongoDB) usando o AWS Database Migration Service (AWS DMS). Essa abordagem pode ser aplicada a um banco de dados Oracle de origem on-premises, bem como a uma instância de banco de dados Oracle do Amazon Relational Database Service (Amazon RDS). Esse padrão usa uma instância de origem de banco de dados Oracle do Amazon RDS como exemplo.

Amazon DocumentDB (compativel com MongoDB) é um serviço de banco de dados de documentos totalmente gerenciado e compatível com o MongoDB que facilita o armazenamento, a consulta e a indexação de dados JSON.

O caso de uso desse padrão é a one-to-one replicação de uma tabela de banco de dados Oracle em uma coleção do Amazon DocumentDB. O padrão usa tarefas de replicação do AWS DMS para ler a estrutura da tabela do banco de dados Oracle, criar a coleção correspondente no Amazon DocumentDB e realizar uma migração de carga completa. Você pode visualizar e consultar seus dados no Amazon DocumentDB, da mesma forma que faria no MongoDB.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Familiaridade com o uso de bancos de dados Oracle
- Familiaridade com o uso do Amazon DocumentDB
- Para o usuário Oracle, `SELECT ANY TABLE` privilégio
- Para o uso do Amazon DocumentDB, o privilégio necessário para despejo de dados

Limitações

As seguintes limitações se aplicam ao usar o Amazon DocumentDB como destino para o AWS DMS:

- No Amazon DocumentDB, os nomes de coleção não podem conter o símbolo de dólar ($). Além disso, os nomes do banco de dados não podem conter caracteres Unicode.

- O AWS DMS não oferece suporte à mesclagem de várias tabelas de origem em uma única coleção do Amazon DocumentDB.
- Quando o AWS DMS processa as alterações de uma tabela de origem que não tem uma chave primária, qualquer coluna de objetos binários grandes (LOB) na tabela é ignorada.
- Se a opção Alterar tabela estiver ativada e o AWS DMS encontrar uma coluna de origem chamada "_id", essa coluna aparecerá como "__id" (dois traços de sublinhado) na tabela de alteração.
- Se você escolher o Oracle como o endpoint de origem, a origem do Oracle deverá ter ativado o registro de log suplementar total. Caso contrário, se houver colunas na origem que não foram alteradas, os dados serão carregados no Amazon DocumentDB como valores nulos.

Versões do produto

- Versão 11.2.0.3 ou superior do Amazon RDS para Oracle
- Versão 3.1.3 ou superior do AWS DMS (para obter as informações sobre a versão mais recente, consulte Usar o Amazon DocumentDB como destino para o AWS DMS na documentação do AWS DMS)

Arquitetura

Pilha de tecnologia de origem

- Instância de banco de dados do Amazon RDS para Oracle

Pilha de tecnologias de destino

- Amazon DocumentDB

Arquitetura de origem e destino

Ferramentas

- AWS DMS: o AWS Database Migration Service (AWS DMS) é um serviço web que pode ser usado para migrar dados de um datastore de origem para outro de destino. O Guia do usuário do AWS DMS especifica as versões e edições do banco de dados de origem Oracle que são compatíveis para uso com o AWS DMS. Para obter informações adicionais relevantes a esse padrão, consulte Usar o Amazon DocumentDB como destino para o AWS DMS.

- Amazon EC2 — A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na nuvem da AWS. O cluster do Amazon DocumentDB deve estar em execução na nuvem privada virtual (VPC) padrão. Para interagir com seu cluster Amazon DocumentDB, você deve iniciar uma EC2 instância em sua VPC padrão, na mesma região da AWS em que você criou seu cluster Amazon DocumentDB. Para obter detalhes, consulte Iniciar uma EC2 instância da Amazon na documentação do Amazon DocumentDB.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Validar versões e mecanismos do banco de dados de origem e de destino.		AWS Admin
Escolha o tipo de instância adequado (capacidade, atributos de armazenamento e atributos de rede).		AWS Admin
Identifique os requisitos de segurança do acesso à rede/host para os bancos de dados de origem e de destino.		AWS Admin
Criar um grupo de segurança de saída para os bancos de dados de origem e de destino.		AWS Admin
Crie e configure uma EC2 instância para o Amazon DocumentDB.		AWS Admin

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma VPC e sub-redes.		AWS Admin
Crie grupos de segurança e listas de controle de acesso à rede (ACLs).		AWS Admin
Configurar e iniciar a instância de banco de dados do Amazon RDS para Oracle.		AWS Admin
Configurar e iniciar a instância de banco de dados do Amazon DocumentDB.		AWS Admin

Preparar o banco de dados de origem

Tarefa	Descrição	Habilidades necessárias
Verifique se o banco de dados Oracle pode ser conectado usando os detalhes da conexão.		AWS Admin
Verifique se o usuário Oracle tem o privilégio SELECT ANY TABLE.		AWS Admin

Preparar o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Crie o cluster Amazon DocumentDB escolhend		AWS Admin

Tarefa	Descrição	Habilidades necessárias
o a classe de instância e o número de instâncias adequados.		

Configurar a Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Configure a EC2 instância.	Para interagir com seu cluster Amazon DocumentDB, você deve iniciar uma EC2 instância em sua VPC padrão, na mesma região da AWS em que você criou seu cluster Amazon DocumentDB. Configure a região VPCs, as zonas de disponibilidade e as sub-redes da AWS para a EC2 instância.	AWS Admin
Configure o par de chaves.	Um par de chaves pública/privada permite que você se conecte com segurança à EC2 instância após sua execução.	AWS Admin
Defina os intervalos de CIDR do Bastion Host (opcional).	O intervalo de IPs de CIDR para acesso à Secure Shell (SSH) externa às instâncias do bastion host.	AWS Admin

Migrar dados – carga total

Tarefa	Descrição	Habilidades necessárias
Criar uma instância de replicação do AWS DMS.		AWS Admin
Criar endpoints de origem e de destino.		AWS Admin
Criar tarefas de replicação do AWS DMS para uma carga completa.		AWS Admin

Testar a migração

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao cluster Amazon DocumentDB por meio da EC2 instância.		AWS Admin
Conectar-se a um cluster usando o shell do Mongo.	Para obter instruções, consulte os links do Amazon DocumentDB na seção Referências e Ajuda.	AWS Admin
Verifique os resultados da migração.		AWS Admin

Recursos relacionados

- Como funciona o AWS DMS
- Migração para o Amazon DocumentDB
- Usar Amazon DocumentDB como destino para o AWS DMS
- Visão geral do Amazon DocumentDB

- Acesse e use o cluster do Amazon DocumentDB usando o shell do Mongo
- Migrar do MongoDB para o Amazon DocumentDB usando o método offline (publicação no blog)
- Como usar o Amazon DocumentDB (compatível com MongoDB) para criar e gerenciar aplicativos em grande escala (publicação no blog)

Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for MariaDB usando o AWS DMS e o AWS SCT

Criado por Veeranjaneyulu Grandhi (AWS) e vinod kumar (AWS)

Resumo

Esse padrão orienta você pelas etapas de migração de um banco de dados Oracle em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para uma instância de banco de dados Amazon Relational Database Service (Amazon RDS) para MariaDB. O padrão usa o AWS Database Migration Service (AWS DMS) e a AWS Schema Conversion Tool (AWS SCT) para conversão de esquemas.

Gerenciar bancos de dados Oracle em EC2 instâncias requer mais recursos e é mais caro do que usar um banco de dados no Amazon RDS. O Amazon RDS facilita a configuração, a operação e a escalabilidade de um banco de dados relacional na nuvem. O Amazon RDS fornece capacidade econômica e redimensionável enquanto automatiza tarefas administrativas, como provisionamento de hardware, configuração de banco de dados, aplicação de patches e backups.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle de origem com serviços de instância e de receptor em execução. Esse banco de dados deve estar no modo ARCHIVELOG.
- Familiaridade com Uso de um banco de dados Oracle como origem para o AWS DMS
- Familiaridade com Uso de Oracle como origem para o AWS SCT.

Limitações

- Limite de tamanho do banco de dados: 64 TB

Versões do produto

- Todas as edições do banco de dados do Oracle para versões 10.2 e posteriores, 11g e até 12.2 e 18c. Para obter a lista mais recente de versões compatíveis, consulte Uso de um banco de dados Oracle como origem para o AWS DMS e a tabela de versão AWS SCT na documentação da AWS.

- O Amazon RDS é compatível com o MariaDB Server Community Server versões 10.3, 10.4, 10.5 e 10.6. Para obter a lista mais recente de versões compatíveis, consulte a documentação do Amazon RDS.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Oracle em uma EC2 instância

Pilha de tecnologias de destino

- Amazon RDS para MariaDB

Arquitetura de migração de dados

Arquitetura de destino

Ferramentas

- O AWS Schema Conversion Tool (AWS SCT) torna as migrações heterogêneas de banco de dados previsíveis ao converter automaticamente o esquema do banco de dados de origem e a maioria do código personalizado, incluindo exibições, procedimentos armazenados e perfis, para um formato compatível com o banco de dados de destino. Depois de converter seu esquema de banco de dados e objetos de código usando o AWS SCT, você pode usar o AWS DMS para migrar dados do banco de dados de origem para o banco de dados de destino para concluir seus projetos de migração. Para obter mais informações, consulte Uso do Redis como destino para o AWS SCT na documentação do AWS SCT.
- O AWS Database Migration Service (AWS DMS) ajuda a migrar bancos de dados para a AWS de forma rápida e segura. O banco de dados de origem permanece totalmente operacional durante a migração, o que minimiza o tempo de inatividade de aplicativos que dependem do banco de dados. O AWS DMS pode migrar seus dados dos/para os bancos de dados comerciais e de código aberto mais usados no mercado. O AWS DMS oferece suporte a migrações homogêneas, como de Oracle para Oracle, além de migrações heterogêneas entre diferentes plataformas de banco de dados, como de Oracle ou Microsoft SQL Server para Amazon Aurora. Para obter mais

informações sobre como migrar bancos de dados Oracle, consulte Uso de um banco de dados Oracle como origem para o AWS DMS na documentação da AWS DMS.

Épicos

Planeje para a migração

Tarefa	Descrição	Habilidades necessárias
Identificar versões e mecanismos de banco de dados.	Identificar as versões e mecanismos dos bancos de dados de origem e de destino.	DBA, Desenvolvedor
Identificar a instância de replicação.	Identificar a instância de replicação AWS DMS.	DBA, Desenvolvedor
Identificar os requisitos de armazenamento.	Identificar o tipo e a capacidade de armazenamento.	DBA, Desenvolvedor
Identificar os requisitos de rede.	Identificar a latência e a largura de banda da rede.	DBA, Desenvolvedor
Identificar os requisitos de hardware.	Identificar os requisitos de hardware para as instâncias do servidor de origem e de destino (com base na lista de compatibilidade e nos requisitos de capacidade da Oracle).	DBA, Desenvolvedor
Identificar os requisitos de segurança.	Identificar os requisitos de segurança do acesso à rede para os bancos de dados de origem e de destino.	DBA, Desenvolvedor
Instalar drivers.	Instale os drivers AWS SCT e Oracle mais recentes.	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Determine uma estratégia de backup.		DBA, Desenvolvedor
Determine os requisitos de disponibilidade.		DBA, Desenvolvedor
Escolha uma estratégia de migração/transição de aplicativos.		DBA, Desenvolvedor
Selecione o tipo de instância do .	Selecione o tipo de instância adequado com base nos atributos de capacidade, armazenamento e rede.	DBA, Desenvolvedor

Configure o ambiente.

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).	As instâncias de origem, destino e replicação devem estar na mesma VPC e na mesma Zona de disponibi lidade (recomendado).	Desenvolvedor
Criar grupos de segurança.	Crie os grupos de segurança necessários para acesso ao banco de dados.	Desenvolvedor
Gere um par de chaves.	Gere e configure um par de chaves.	Desenvolvedor
Configure outros recursos.	Configure sub-redes, zonas de disponibilidade e blocos CIDR.	Desenvolvedor

Configure a origem

Tarefa	Descrição	Habilidades necessárias
Inicie a EC2 instância.	Para obter instruções, consulte a EC2 documentação da Amazon.	Desenvolvedor
Instale o banco de dados Oracle.	Instale o banco de dados Oracle na EC2 instância, com os usuários e funções necessários.	DBA
Siga as etapas na descrição da tarefa para acessar o Oracle de fora da EC2 instância.	1. Mude o host local `tnsnames` para o DNS EC2 público da Amazon. 2. Mude o host local `listener` para o DNS EC2 público da Amazon. 3. Interromper e reiniciar o receptor.	DBA
Atualize o DNS EC2 público da Amazon.	Depois que a EC2 instância é reiniciada, o DNS público muda. Certifique-se de atualizar o DNS EC2 público da Amazon em `tnsnames` e `listener` ou usar um endereço IP elástico.	DBA, Desenvolvedor
Configure o grupo de segurança da EC2 instância.	Configure o grupo de segurança da EC2 instância para que a instância de replicação e os clientes necessários possam acessar o banco de dados de origem.	DBA, Desenvolvedor

Configure o ambiente do Amazon RDS para MariaDB

Tarefa	Descrição	Habilidades necessárias
Inicie a instância de banco de dados RDS.	Configure e inicie a instância de banco de dados do Amazon RDS para MariaDB.	Desenvolvedor
Criar tablespaces.	Crie todos os tablespaces necessários no banco de dados MariaDB do Amazon RDS.	DBA
Configurar um grupo de segurança	Configure um grupo de segurança para que a instância de replicação e os clientes necessários possam acessar o banco de dados de destino.	Desenvolvedor

Configure o AWS SCT

Tarefa	Descrição	Habilidades necessárias
Instalar drivers.	Instale os drivers AWS SCT e Oracle mais recentes.	Desenvolvedor
Conecte-se.	Insira os parâmetros apropriados e conecte-se à origem e ao destino.	Desenvolvedor
Gere um relatório de conversão de esquema.	Gere um relatório de conversão de esquema AWS SCT.	Desenvolvedor
Corrija o código e o esquema conforme necessário.	Faça as correções necessárias no código e no esquema	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	(especialmente nos espaços de tabela e aspas).	
Valide o esquema.	Valide o esquema na origem versus no destino antes de carregar os dados.	Desenvolvedor

Migrar dados usando o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Defina um atributo de conexão.	Para carga total e captura de dados alterados (CDC) ou apenas CDC, configure um atributo de conexão extra. Para obter mais informações, consulte a documentação do Amazon RDS.	Desenvolvedor
Habilite o registro em log complementar.	Habilite o log suplementar no banco de dados de origem.	DBA, Desenvolvedor
Ativar o modo log de arquivo.	Para carga total e CDC (ou apenas CDC), habilite o modo log de arquivo no banco de dados de origem.	DBA
Crie e teste endpoints.	Crie endpoints de origem e destino e teste as conexões. Para obter mais informações, consulte a documentação do Amazon DMS.	Desenvolvedor
Criar uma tarefa de replicaçã o.	Quando os endpoints forem conectados com êxito, crie uma tarefa de replicação.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte a documentação do Amazon DMS.	
Escolha o tipo de replicação.	Escolha somente CDC ou Carga total mais CDC na tarefa para capturar alterações somente para replicação contínua ou para carga total mais alterações em andamento, respectivamente.	Desenvolvedor
Inicie e monitore a tarefa.	Inicie a tarefa de replicação e monitore CloudWatch os registros da Amazon. Para obter mais informações, consulte a documentação do Amazon DMS.	Desenvolvedor
Valide os dados.	Valide os dados nos bancos de dados de origem e de destino.	Desenvolvedor

Migre aplicativos e substitua para o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos escolhida.		DBA, proprietário do aplicativo, desenvolvedor
Siga a estratégia de substituição/transição de aplicativos escolhida.		DBA, proprietário do aplicativo, desenvolvedor

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Valide o esquema e os dados.	Certifique-se de que o esquema e os dados sejam validados com sucesso na origem em comparação ao destino antes do encerramento do projeto.	DBA, Desenvolvedor
Colete métricas.	Reúna métricas de tempo de migração, porcentagem de uso manual em comparação com as tarefas da ferramenta, economia de custos e dados similares.	DBA, proprietário do aplicativo, desenvolvedor
Revise a documentação.	Revise os documentos e artefatos do projeto.	DBA, proprietário do aplicativo, desenvolvedor
Desligar recursos.	Encerre os recursos temporários da AWS.	DBA, Desenvolvedor
Fechar o projeto.	Feche o projeto de migração e forneça qualquer feedback.	DBA, proprietário do aplicativo, desenvolvedor

Recursos relacionados

- Visão geral do MariaDB do Amazon RDS
- Detalhes de produto do Amazon RDS para MariaDB
- Uso de um banco de dados Oracle como origem para o AWS DMS
- Estratégias para migrar bancos de dados Oracle para a AWS
- Licenciamento do software Oracle no ambiente de computação em nuvem
- Amazon RDS para Oracle FAQs
- Visão geral do AWS DMS

- Publicações no blog do AWS DMS
- EC2 Visão geral da Amazon
- Amazon EC2 FAQs
- Documentação do AWS SCT

Migre um banco de dados Oracle on-premises para o Amazon RDS para MySQL, usando o AWS DMS e o AWS SCT.

Criado por Sergey Dmitriev (AWS) e Naresh Damera (AWS)

Resumo

Esse padrão orienta você na migração de um banco de dados Oracle on-premises para uma instância de banco de dadosAmazon Relational Database Service (Amazon RDS) para MySQL. Ele usa o AWS Database Migration Service (AWS DMS) para migrar os dados e o AWS Schema Conversion Tool (AWS SCT) para converter o esquema e os objetos do banco de dados de origem em um formato compatível com o Amazon RDS para MySQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle de origem em um datacenter on-premises

Limitações

- Limite de tamanho do banco de dados: 64 TB

Versões do produto

- Todas as edições do banco de dados Oracle para as versões 11g (versões 11.2.0.3.v1 e mais recente) e até 12.2 e 18c. Para obter a lista mais recente de versões compatíveis, consulte Usar um banco de dados Oracle como origem para o AWS DMS. Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos. Para obter informações sobre as versões do banco de dados Oracle suportadas pelo AWS SCT, consulte a documentação do AWS SCT.
- O AWS DMS é compatível com as versões 5.5, 5.6 e 5.7 do MySQL. Para obter a lista mais recente de versões compatíveis, consulte Usar um banco de dados compatível com MySQL como destino para o AWS DMS na documentação da AWS.

Arquitetura

Pilha de tecnologia de origem

- Banco de dados on-premises da Oracle

Pilha de tecnologias de destino

- Instância do banco de dados do Amazon RDS para MySQL

Arquitetura de migração de dados

Ferramentas

- AWS DMS: o AWS Database Migration Services (AWS DMS) ajuda a migrar bancos de dados relacionais, data warehouses, bancos de dados NoSQL e outros tipos de armazenamentos de dados. É possível usar o AWS DMS para migrar seus dados para a Nuvem AWS, entre instâncias on-premises (por meio de uma configuração da Nuvem AWS) ou entre combinações de nuvem e configurações locais.
- AWS SCT: a AWS Schema Conversion Tool (AWS SCT) é usada para converter seu esquema de banco de dados de um mecanismo de banco de dados para outro. O código personalizado que a ferramenta converte inclui visualizações, procedimentos armazenados e funções. Qualquer código que não possa ser convertido automaticamente pela ferramenta será marcado em destaque para que você mesmo possa convertê-lo.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide a versão e o mecanismo dos bancos de dados de origem e de destino.		DBA
Identifique os requisitos de hardware para a instância do servidor de destino.		DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, SysAdmin
Escolher o tipo de instância adequado com base na capacidade, nos atributos de armazenamento e nos atributos de rede.		DBA, SysAdmin
Identifique os requisitos de segurança de acesso à rede para os bancos de dados de origem e de destino.		DBA, SysAdmin
Identifique a estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC) e sub-redes.		SysAdmin
Crie os grupos de segurança e as listas de controle de acesso à rede (ACLs).		SysAdmin
Configure e inicie uma instância de banco de dados do Amazon RDS.		DBA, SysAdmin

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Migre o esquema do banco de dados usando o AWS SCT.		DBA
Migrar dados usando o AWS DMS.		DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Use o AWS SCT para analisar e converter o código SQL dentro do código do aplicativo.	Para obter mais informações, consulte https://docs.aws.amazon.com/SchemaConversionTool/ latest/userguide/ CHAP _Converting.app.html.	Proprietário do App
Siga a estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Substituir

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.		DBA SysAdmin, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, SysAdmin
Revise e valide os documentos do projeto.		DBA, SysAdmin
Reúna métricas sobre o tempo de migração, % de manual x ferramenta, economia de custos etc.		DBA, SysAdmin
Feche o projeto e forneça feedback.		

Recursos relacionados

Referências

- Documentação do AWS DMS
- Documentação do AWS SCT
- Preços do Amazon RDS

Tutoriais e vídeos

- Conceitos básicos da AWS DMS
- Conceitos básicos do Amazon RDS
- AWS DMS (vídeo)
- Amazon RDS (vídeo)

Migrar um banco de dados Oracle on-premises para o Amazon RDS para PostgreSQL usando um Oracle bystander e o AWS DMS

Criado por Cady Motyka (AWS)

Resumo

Este padrão descreve como você pode migrar um banco de dados Oracle on-premises para qualquer um dos seguintes serviços de banco de dados da AWS compatíveis com PostgreSQL com o mínimo de tempo de inatividade:

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL
- Amazon Aurora Edição Compatível com PostgreSQL

A solução usa o AWS Database Migration Service (AWS DMS) para migrar os dados, o AWS Schema Conversion Tool (AWS SCT) para converter o esquema do banco de dados e um banco de dados da Oracle bystander para ajudar a gerenciar a migração. Nessa implementação, o tempo de inatividade é restrito ao tempo necessário para criar ou validar todas as chaves estrangeiras no banco de dados.

A solução também usa instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com um banco de dados de espectadores Oracle para ajudar a controlar o fluxo de dados por meio do AWS DMS. Você pode pausar temporariamente a replicação de transmissão do banco de dados on-premises da Oracle para a Oracle bystander para ativar o AWS DMS para acompanhar a validação de dados ou usar outra ferramenta de validação de dados. A instância de banco de dados Amazon RDS para PostgreSQL ou a instância de banco de dados compatível com o Aurora PostgreSQL e o banco de dados de bystander terão os mesmos dados quando o AWS DMS terminar de migrar as alterações atuais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem Oracle em um datacenter on-premises com um banco de dados Active Data Guard configurado em espera
- AWS Direct Connect configurado entre o datacenter on-premises e o AWS Secrets Manager para armazenar os segredos do banco de dados

- Drivers de conectividade de banco de dados Java (JDBC) para conectores AWS SCT, instalados em uma máquina local ou na instância em que o AWS SCT EC2 está instalado
- Familiaridade com o uso de um banco de dados Oracle como origem para o AWS DMS
- Familiaridade com o uso de um banco de dados PostgreSQL como destino para o AWS DMS

Limitações

- Limite de tamanho do banco de dados: 64 TB

Versões do produto

- O AWS DMS oferece suporte a todas as edições do banco de dados Oracle para as versões 10.2 e versões posteriores (para versões 10.x), 11g e até 12.2, 18c e 19c. Para obter a lista mais recente de versões compatíveis, consulte Usar um banco de dados Oracle como origem para o AWS DMS. Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos. Para obter informações sobre as versões do banco de dados Oracle suportadas pelo AWS SCT, consulte a documentação do AWS SCT.
- O AWS DMS é compatível com o PostgreSQL versão 9.4 e posterior (para versões 9.x), 10.x, 11.x, 12.x e 13x. Para obter as informações mais recentes, consulte Uso de um banco de dados PostgreSQL como destino para o AWS DMS na documentação da AWS.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Oracle on-premises
- Uma EC2 instância que contém um espectador para o banco de dados Oracle

Pilha de tecnologias de destino

- Instância do Amazon RDS para PostgreSQL ou Aurora PostgreSQL, PostgreSQL 9.3 e versões posteriores

Arquitetura de destino

O diagrama a seguir mostra um exemplo de fluxo de trabalho para migrar um banco de dados Oracle para um banco de dados AWS compatível com PostgreSQL usando o AWS DMS e um bystander Oracle:

Ferramentas

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- A AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.

Épicos

Converta o esquema do banco de dados Oracle em PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Configure o AWS SCT.	Crie um novo relatório e conecte-se ao Oracle como origem e ao PostgreSQL como destino. Em Configurações do projeto, vá até a guia SQL Scripting. Altere o script SQL de destino para vários arquivos. Esses arquivos serão usados posteriormente e nomeados da seguinte forma: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql	DBA

Tarefa	Descrição	Habilidades necessárias
	• create_function.sql	
Converta o esquema do banco de dados Oracle.	Na guia Ação, escolha Gerar relatório. Em seguida, escolha Converter esquema e escolha Salvar como SQL.	DBA
Modifique os scripts.	Por exemplo, talvez você queira modificar o script se um número no esquema de origem tiver sido convertid o para o formato numérico no PostgreSQL, mas você precise usar o BIGINT em vez disso para melhorar o desempenho.	DBA

Crie e configure a instância de banco de dados do Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Criar a instância de banco de dados do Amazon RDS	Na região da AWS correta, crie uma nova instância de banco de dados PostgreSQL. Para obter mais informações, consulte Criar uma instância de banco de dados PostgreSQ L e conectar a um banco de dados em uma instância de banco de dados PostgreSQL na documentação do Amazon RDS.	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
Configure as especificações da instância de banco de dados.	Especifique a versão do mecanismo de banco de dados, a classe da instância de banco de dados, a implantação Multi-AZ, o tipo de armazenamento e o armazenamento alocado. Insira o identificador da instância de banco de dados, um nome de usuário primária e uma senha primária.	AWS SysAdmin, DBA
Configure rede e segurança.	Especifique a nuvem privada virtual (VPC), o grupo de sub-rede, a acessibilidade pública, a preferência da zona de disponibilidade e os grupos de segurança.	DBA, SysAdmin
Configure as opções do banco de dados.	Especifique o nome do banco de dados, a porta, o grupo de parâmetros, a criptografia e a chave KMS.	AWS SysAdmin, DBA
Configure os backups.	Especifique o período de retenção do backup, a janela do backup, a hora de início, a duração e se as tags devem ser copiadas para instantân eos.	AWS SysAdmin, DBA
Configure opções de monitoramento.	Ative ou desative insights aprimorados de monitoram ento e desempenho.	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
Configure opções de manutenção.	Especifique a atualizaç ão automática da versão secundária, a janela de manutenção e o dia, a hora e a duração de início.	AWS SysAdmin, DBA
Execute os scripts de pré-migração do AWS SCT.	Na instância do Amazon RDS, execute os seguintes scripts gerados pelo AWS SCT: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	AWS SysAdmin, DBA

Configurar o Oracle bystander na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Configure a rede para a Amazon EC2.	Crie a nova VPC, sub-redes, gateway da Internet, tabelas de rotas e grupos de segurança.	AWS SysAdmin
Crie a EC2 instância.	Na região apropriada da AWS, crie uma nova EC2 instância. Selecione a imagem de máquina da Amazon (AMI), escolha o tamanho da instância e configure os detalhes da instância: número de instâncias (1), a VPC e a sub-rede que você criou	AWS SysAdmin

Tarefa	Descrição	Habilidades necessárias
	na tarefa anterior, atribuiçã o automática de IP público e outras opções. Adicione armazenamento, configure grupos de segurança e inicie. Quando solicitado, crie e salve um par de chaves para a próxima etapa.	
Conecte o banco de dados de origem Oracle à EC2 instância .	Copie o endereço IP IPv4 público e o DNS em um arquivo de texto e conecte-se usando SSH da seguinte forma: ssh -i “your_file.pem” EC2-user@<your-IP - -DNS>. address-or-public	AWS SysAdmin
Configure o host inicial para um espectador na Amazon. EC2	Configure chaves SSH, perfil bash, ORATAB e links simbólicos. Crie diretórios Oracle.	AWS SysAdmin, administrador de Linux
Configure a cópia do banco de dados para um espectador na Amazon EC2	Use o RMAN para criar uma cópia do banco de dados, ativar o registro suplementar e criar o arquivo de controle em espera. Depois que a cópia estiver concluída, coloque o banco de dados no modo de recuperação.	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
Configure o Oracle Data Guard.	Modifique seu arquivo listener.ora e inicie o receptor. Configure um novo destino de arquivamento. Coloque o espectador no modo de recuperação, substitua os arquivos temporários para evitar corrupção futura, instale um crontab, se necessário, para evitar que o diretório de arquivamento fique sem espaço e edite o manage-trclog-files-oraclearquivo.cfg para a origem e o modo de espera.	AWS SysAdmin, DBA
Prepare o banco de dados Oracle para sincronizar o envio.	Adicione os arquivos de log em espera e altere o modo de recuperação. Altere o envio do log para SYNC AFFIRM na fonte primária e na fonte em espera. Ative os registros primários, confirme por meio do registro de alerta do EC2 espectador da Amazon que você está usando os arquivos de log em espera e confirme se o fluxo de redo está fluindo no SYNC.	AWS SysAdmin, DBA

Migre dados com o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de replicação no AWS DMS.	Preencha os campos para nome, classe da instância, VPC (igual à EC2 instância da Amazon), Multi-AZ e acessibil idade pública. Em Avançado, especifique o armazenamento alocado, o grupo de sub-rede, a zona de disponibilidade, os grupos de segurança da VPC e a chave do AWS Key Management Service (AWS KMS).	AWS SysAdmin, DBA
Crie o endpoint do banco de dados de origem.	Especifique o nome do endpoint, tipo, mecanismo de origem (Oracle), nome do servidor (nome DNS EC2 privado da Amazon), porta, modo SSL, nome de usuário, senha, SID, VPC (especifique a VPC que tem a instância de replicação) e instância de replicação. Para testar a conexão, escolha Executar teste e, em seguida, crie o endpoint. Você também pode definir as seguintes configura ções avançadas: maxFileSi zee numberDataTypeEscala.	AWS SysAdmin, DBA
Conecte o AWS DMS ao Amazon RDS para PostgreSQ L.	Crie um grupo de segurança de migração para conexões entre VPCs.	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
Crie o endpoint do banco de dados de destino.	Especifique o nome do endpoint, o tipo, o mecanismo de origem (PostgreSQL), o nome do servidor (endpoint do Amazon RDS), a porta, o modo SSL, o nome do usuário, a senha, o nome do banco de dados, a VPC (especificar a VPC que tem a instância de replicação) e a instância de replicação. Para testar a conexão, escolha Executar teste e, em seguida, crie o endpoint. Você também pode definir as seguintes configurações avançadas : maxFileSize e numberDat aTypeEscala.	AWS SysAdmin, DBA
Crie a tarefa de replicação do AWS DMS.	Especifique o nome da tarefa, a instância de replicação, os endpoints de origem e destino e a instância de replicaçã o. Para tipo de migração, escolha Migrar dados existentes e replicar alteraçõe s contínuas. Desmarque a caixa de seleção Iniciar tarefa ao criar.	AWS SysAdmin, DBA

Tarefa	Descrição	Habilidades necessárias
Defina as configurações da tarefa de replicação do AWS DMS.	Para o modo de preparação da tabela de destino, escolha Não fazer nada. Interrompa a tarefa após a conclusão do carregamento total (para criar chaves primárias). Especifiq ue o modo LOB limitado ou completo e ative as tabelas de controle. Opcionalmente, você pode definir a configura ção CommitRateavançada.	DBA
Configure mapeamentos de tabelas.	Na seção Mapeamentos de tabela, crie uma regra de inclusão para todas as tabelas em todos os esquemas incluídos na migração e, em seguida, crie uma regra de exclusão. Adicione três regras de transformação para converter os nomes do esquema, da tabela e da coluna para letra minúscula e adicione quaisquer outras regras necessárias para essa migração específica.	DBA
Iniciar a tarefa.	Iniciar a tarefa de replicação. Verifique se a carga total está em execução. Execute ALTER SYSTEM SWITCH LOGFILE no banco de dados Oracle primário para iniciar a tarefa.	DBA

Tarefa	Descrição	Habilidades necessárias
Execute os scripts de meio da migração do AWS SCT.	No Amazon RDS para PostgreSQL, execute os seguintes scripts gerados pelo AWS SCT: • create_index.sql • create_constraint.sql	DBA
Reinicie a tarefa para continuar a captura de dados de alteração (CDC).	Execute VACUUM na instância de banco de dados Amazon RDS para PostgreSQL e reinicie a tarefa do AWS DMS para aplicar as alterações do CDC em cache.	DBA

Substitua para o banco de dados PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Verifique se há erros nos registros e nas tabelas de validação do AWS DMS.	Verifique e corrija quaisquer erros de replicação ou validação.	DBA
Interrompa todas as dependências do Oracle.	Interrompa todas as dependências do Oracle, desligue os receptores no banco de dados Oracle e execute ALTER SYSTEM SWITCH LOGFILE. Interrompa a tarefa do AWS DMS quando ele não mostrar nenhuma atividade.	DBA
Execute os scripts de pós-migração do AWS SCT.	No Amazon RDS para PostgreSQL, execute os	DBA

Tarefa	Descrição	Habilidades necessárias
	seguintes scripts gerados pelo AWS SCT: • create_foreign_key_constraint.sql • create_triggers.sql	
Conclua etapas adicionais do Amazon RDS para PostgreSQL.	Incremente as sequências para corresponder ao Oracle, se necessário; execute VACUUM e ANALYZE e tire um instantâneo para fins de conformidade.	DBA
Escolha conectar ao Amazon RDS para PostgreSQL.	Remova os grupos de segurança do AWS DMS do Amazon RDS para PostgreSQL, adicione grupos de segurança de produção e direcione seus aplicativos para o novo banco de dados.	DBA
Limpe objetos do AWS DMS.	Remova os endpoints, as tarefas de replicação, as instâncias de replicação e a instância. EC2	SysAdmin, DBA

Recursos relacionados

- Documentação do AWS DMS
- Documentação do AWS SCT
- Preço do Amazon RDS para PostgreSQL

Migre do banco de dados Oracle para o Amazon RDS for PostgreSQL usando o Oracle GoldenGate

Criado por Dhairya Jindani (AWS), Rajeshkumar Sabankar (AWS) e Sindhusha Paturu (AWS)

Resumo

Esse padrão mostra como migrar um banco de dados Oracle para o Amazon Relational Database Service (Amazon RDS) para PostgreSQL usando o Oracle Cloud Infrastructure (OCI). GoldenGate

Usando o Oracle GoldenGate, você pode replicar dados entre seu banco de dados de origem e um ou mais bancos de dados de destino com o mínimo de tempo de inatividade.

> **Note**
>
> O banco de dados Oracle de origem pode estar no local ou em uma instância do Amazon Elastic Compute Cloud EC2 (Amazon). Você pode usar um procedimento semelhante ao usar ferramentas de replicação on-premises.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma GoldenGate licença Oracle
- Java Database Connectivity driver JDBC para conectar ao banco de dados PostgreSQL
- Esquema e tabelas criados com a AWS Schema Conversion Tool (AWS SCT) no banco de dados Amazon RDS para PostgreSQL de destino

Limitações

- O Oracle GoldenGate só pode replicar dados de tabelas existentes (carregamento inicial) e alterações em andamento (captura de dados de alteração)

Versões do produto

- Oracle Database Enterprise Edition 10g, ou versões mais recentes
- Oracle GoldenGate 12.2.0.1.1 para Oracle ou versões mais recentes

- Oracle GoldenGate 12.2.0.1.1 para PostgreSQL ou versões mais recentes

Arquitetura

O diagrama a seguir mostra um exemplo de fluxo de trabalho para migrar um banco de dados Oracle para o Amazon RDS for PostgreSQL usando o Oracle: GoldenGate

O diagrama mostra o seguinte fluxo de trabalho:

1. O processo Oracle GoldenGate Extract é executado no banco de dados de origem para extrair dados.
2. O processo Oracle GoldenGate Replicat entrega os dados extraídos ao banco de dados Amazon RDS for PostgreSQL de destino.

Ferramentas

- GoldenGateA Oracle ajuda você a projetar, executar, orquestrar e monitorar suas soluções de replicação de dados e streaming de processamento de dados na Oracle Cloud Infrastructure.
- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.

Épicos

Baixe e instale o Oracle GoldenGate

Tarefa	Descrição	Habilidades necessárias
Baixe o Oracle GoldenGate.	Baixe as seguintes versões do Oracle GoldenGate: • Oracle GoldenGate 12.2.0.1.1 para Oracle ou uma versão mais recente • Oracle GoldenGate 12.2.0.1.1 para PostgreSQL ou uma versão mais recente	DBA

Tarefa	Descrição	Habilidades necessárias
	Para baixar o software, consulte Oracle GoldenGate Downloads no site da Oracle.	
Instale o Oracle GoldenGate for Oracle no servidor de banco de dados Oracle de origem.	Para obter instruções, consulte a GoldenGate documentação da Oracle.	DBA
Instale o banco de dados Oracle GoldenGate para PostgreSQL na instância da Amazon. EC2	Para obter instruções, consulte a GoldenGate documentação da Oracle.	DBA

Configurar o Oracle GoldenGate nos bancos de dados de origem e destino

Tarefa	Descrição	Habilidades necessárias
Configure o Oracle GoldenGate for Oracle Database no banco de dados de origem.	Para obter instruções, consulte a GoldenGate documentação da Oracle. Certifique-se de configurar o seguinte: • Registro em log complementar • GoldenGate Usuários Oracle • Quaisquer concessões e permissões necessárias • Arquivos de parâmetros • Processo de gerenciamento • Diretório	DBA

Tarefa	Descrição	Habilidades necessárias
	• Arquivos GLOBALS • Carteira do Oracle	
Configure o Oracle GoldenGat e para PostgreSQL no banco de dados de destino.	Para obter instruções, consulte a Parte VI Usando o Oracle GoldenGate para PostgreSQL no site da Oracle. Certifique-se de configurar o seguinte: • Processo de gerenciamento • Arquivos GLOBALS • Carteira do Oracle	DBA

Configure a captura de dados

Tarefa	Descrição	Habilidades necessárias
Configure o processo de Extração no banco de dados de origem.	No banco de dados Oracle de origem, crie um arquivo de extração para extrair dados. Para obter instruções, consulte ADICIONAR EXTRACT na documentação da Oracle. **Note** O arquivo de extração inclui a criação do arquivo de parâmetro s de extração e do	DBA

Tarefa	Descrição	Habilidades necessárias
	diretório do arquivo de trilha.	
Configure uma bomba de dados para transferir o arquivo de trilha do banco de dados de origem para o de destino.	Crie um arquivo de parâmetros EXTRACT e um diretório de arquivos de trilha seguindo as instruções em PARFILE em Utilitários de banco de dados no site da Oracle. Para obter mais informações, consulte O que é uma trilha? no Fusion Middleware e Understanding Oracle GoldenGate no site da Oracle.	DBA

Tarefa	Descrição	Habilidades necessárias
Configure a replicação na EC2 instância da Amazon.	Crie um arquivo de parâmetros de replicação e um diretório de arquivos de trilha. Para obter mais informações sobre como criar arquivos de parâmetros de replicação, consulte a seção 3.5 Validando um arquivo de parâmetros na documentação do Oracle Database. Para obter mais informações sobre a criação de um diretório de arquivos de trilha, consulte Criar uma trilha na documentação do Oracle Cloud. **Important** Certifique-se de adicionar uma entrada de tabela de ponto de verificação no arquivo GLOBALS no destino. Para obter mais informações, consulte O que é uma réplica? no Fusion Middleware e Understanding Oracle GoldenGate no site da Oracle.	DBA

Configure a replicação de dados

Tarefa	Descrição	Habilidades necessárias
No banco de dados de origem, crie um arquivo de parâmetros para extrair dados para o carregamento inicial.	Siga as instruções em Como criar um arquivo de parâmetros no GGSCI na documentação do Oracle Cloud. **Important** Certifique-se de que o Manager esteja sendo executado no destino.	DBA
No banco de dados de destino, crie um arquivo de parâmetros para replicar dados para o carregamento inicial.	Siga as instruções em Como criar um arquivo de parâmetros no GGSCI na documentação do Oracle Cloud. **Important** Certifique-se de adicionar e iniciar o processo de replicação.	DBA

Vá para o banco de dados do Amazon RDS para PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Pare o processo de Replicação e certifique-se que os bancos de dados de origem e de destino estejam sincronizados.	Compare as contagens de linhas entre os bancos de dados de origem e de destino para garantir que a replicaçã	DBA

Tarefa	Descrição	Habilidades necessárias
	o dos dados tenha sido bem-sucedida.	
Configure o suporte DDL (Linguagem de definição de dados).	Execute o script DDL para criar acionadores, sequência, sinônimos e chaves referenci ais no PostgreSQL. **Note** Você pode usar qualquer aplicativo cliente SQL padrão para se conectar a um banco de dados no seu cluster de banco de dados. Por exemplo, você pode usar o pgAgmin para se conectar à sua instância de banco de dados.	DBA

Recursos relacionados

- Amazon RDS para PostgreSQL (Guia do usuário do Amazon RDS)
- EC2 Documentação da Amazon
- Métodos de processamento e bancos de dados GoldenGate suportados pela Oracle (documentação da Oracle)

Migre um banco de dados Oracle para o Amazon Redshift usando o AWS DMS e o AWS SCT

Criado por Piyush Goyal (AWS) e Brian motzer (AWS)

Resumo

Esse padrão fornece orientação para migrar bancos de dados Oracle para um data warehouse em nuvem do Amazon Redshift na nuvem da Amazon Web Services (AWS) usando o AWS Database Migration Service (AWS DMS) e a AWS Schema Conversion Tool (AWS SCT). O padrão abrange bancos de dados Oracle de origem que estão no local ou instalados em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Também abrange o Amazon Relational Database Service (Amazon RDS) para bancos de dados Oracle.

Pré-requisitos e limitações

Pré-requisitos

- Um banco de dados Oracle que está sendo executado em um datacenter on-premises ou na Nuvem AWS
- Uma conta AWS ativa
- Familiaridade com o uso de um banco de dados Oracle como origem para o AWS DMS
- Familiaridade com o uso de um banco de dados do Amazon Redshift como destino do AWS DMS
- Conhecimento do Amazon RDS, do Amazon Redshift, das tecnologias de banco de dados aplicáveis e do SQL
- Drivers de conectividade de banco de dados Java (JDBC) para conectores AWS SCT, onde o AWS SCT está instalado

Versões do produto

- No caso de bancos de dados Oracle autogerenciados, o DMS da AWS é compatível com todas as edições de banco de dados Oracle para as versões 10.2 e superiores (para versões 10.x), 11g e até 12.2, 18c e 19c. No caso de bancos de dados do Amazon RDS para Oracle, o DMS da AWS é compatível com todas as edições de banco de dados Oracle para as versões 11g (versões 11.2.0.4 e superiores) e até 12.2, 18c e 19c. Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos.

Arquitetura

Pilha de tecnologia de origem

Um dos seguintes:

- Um banco de dados Oracle on-premises
- Um banco de dados Oracle em uma EC2 instância
- Instância de banco de dados do Amazon RDS para Oracle

Pilha de tecnologias de destino

- Amazon Redshift

Arquitetura de destino

De um banco de dados Oracle em execução na Nuvem AWS para o Amazon Redshift:

De um banco de dados Oracle em execução em um datacenter on-premises para o Amazon Redshift:

Ferramentas

- AWS DMS: o AWS Data Migration Service (AWS DMS) ajuda você a migrar bancos de dados para a AWS de forma rápida e segura. O banco de dados de origem permanece totalmente operacional durante a migração, o que minimiza o tempo de inatividade de aplicativos que dependem do banco de dados. O AWS DMS pode migrar seus dados dos/para os bancos de dados comerciais e de código aberto mais usados no mercado.
- AWS SCT: a AWS Schema Conversion Tool (AWS SCT) pode ser usada para converter seu esquema de banco de dados existente de um mecanismo de banco de dados para outro. Ele oferece suporte a vários mecanismos de banco de dados, incluindo Oracle, SQL Server e PostgresSQL, como fontes.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões do banco de dados.	Valide as versões de origem e destino do banco de dados e certifique-se de que elas sejam suportadas pelo AWS DMS. Para obter informações sobre as versões compatíveis do Oracle Database, consulte Usando um banco de dados Oracle como origem para o AWS DMS. Para obter informações sobre o uso do Amazon Redshift como destino, consulte Usar um banco de dados do Amazon Redshift como destino do AWS DMS.	DBA
Criar um grupo de segurança e de VPC.	Crie uma nuvem privada virtual (VPC) na conta da AWS, caso ela ainda não exista. Crie um grupo de segurança para tráfego de saída para bancos de dados de origem e destino. Para obter mais informações, consulte a documentação do Amazon Virtual Private Cloud (Amazon VPC).	Administrador de sistemas
Instale a AWS SCT.	Faça download e instale a versão mais recente do AWS SCT e seus drivers	DBA

Tarefa	Descrição	Habilidades necessárias
	correspondentes. Para obter mais informações, consulte Instalação, verificação e atualização do AWS SCT.	
Criar um usuário para a tarefa do AWS DMS.	Crie um usuário do AWS DMS no banco de dados de origem e conceda a ele privilégios READ. Esse usuário será usado tanto pelo AWS SCT quanto pelo AWS DMS.	DBA
Testar a conectividade do banco de dados.	Teste a conectividade à instância de banco de dados do Oracle.	DBA
Crie de um novo projeto no AWS SCT.	Abra a ferramenta AWS SCT e crie um novo projeto.	DBA
Analise o esquema Oracle a ser migrado.	Use o AWS SCT para analisar o esquema a ser migrado e gerar um relatório de avaliação da migração do banco de dados. Para obter mais informações, consulte Criação de um relatório de avaliação de migração de banco de dados na documentação do AWS SCT.	DBA

Tarefa	Descrição	Habilidades necessárias
Analisar o relatório de avaliação.	Analise o relatório para verificar a viabilidade da migração. Alguns objetos de banco de dados podem exigir conversão manual. Para obter mais informações sobre o relatório, consulte Visualização do relatório de avaliação na documentação do AWS SCT.	DBA

Preparar o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Crie um cluster do Amazon Redshift.	Crie um cluster do Amazon Redshift dentro da VPC que você criou anteriormente. Para obter mais informações, consulte Clusters do Amazon Redshift na documentação do Amazon Redshift.	DBA
Criar usuários do banco de dados.	Extraia a lista de usuários, funções e concessões do banco de dados de origem da Oracle. Crie usuários no banco de dados de destino do Amazon Redshift e aplique as funções da etapa anterior.	DBA
Avaliar parâmetros do banco de dados.	Analise as opções, os parâmetros, os arquivos de rede e os links do banco de dados de origem Oracle e	DBA

Tarefa	Descrição	Habilidades necessárias
	avalie sua aplicabilidade ao destino.	
Aplique todas as configurações relevantes ao destino.	Para obter mais informações sobre essa etapa, consulte Referência de configuração na documentação do Amazon Redshift.	DBA

Criar objetos no banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Crie um usuário do AWS DMS no banco de dados de destino.	Crie um usuário do AWS DMS no banco de dados de destino e conceda a ele privilégios de leitura e gravação. Valide a conectividade do AWS SCT.	DBA
Converta o esquema, revise o relatório SQL e salve quaisquer erros ou avisos.	Para obter mais informações, consulte Conversão de esquemas de banco de dados usando o AWS SCT na documentação do AWS SCT.	DBA
Aplique as alterações do esquema ao banco de dados de destino ou salve-as como um arquivo .sql.	Para obter instruções, consulte Salvar e aplicar seu esquema convertido no AWS SCT na documentação do AWS SCT.	DBA
Valide os objetos no banco de dados de destino.	Valide os objetos que foram criados na etapa anterior no banco de dados de destino. Reescreva ou redesenhe	DBA

Tarefa	Descrição	Habilidades necessárias
	qualquer objeto que não tenha sido convertido com sucesso.	
Desative chaves e gatilhos externos.	Desative qualquer chave e gatilhos externos. Isso pode causar problemas de carregamento de dados durante o processo de carregamento completo ao executar o AWS DMS.	DBA

Migrar dados usando o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Criar uma instância de replicação do AWS DMS.	Faça login no console de gerenciamento da AWS e abra o console do AWS DMS. No painel de navegação, escolha Instâncias de replicação, Criar instância de replicação. Para obter instruções detalhadas, consulte a etapa 1 em Introdução ao AWS DMS na documentação do AWS DMS.	DBA
Criar endpoints de origem e de destino.	Crie endpoints de origem e destino, teste a conexão da instância de replicação com os endpoints de origem e de destino. Para obter instruções detalhadas, consulte a etapa 2 em Introdução ao AWS DMS na documentação do AWS DMS.	DBA

Tarefa	Descrição	Habilidades necessárias
Criar uma tarefa de replicação.	Crie uma tarefa de replicação e selecione o método de migração apropriado. Para obter instruções detalhadas, consulte a etapa 3 em Introdução ao AWS DMS na documentação do AWS DMS.	DBA
Iniciar a replicação dos dados.	Inicie a tarefa de replicação e monitore os logs em busca de erros.	DBA

Migrar seu aplicativo

Tarefa	Descrição	Habilidades necessárias
Crie servidores de aplicações.	Crie os novos servidores de aplicativos na AWS.	Proprietário do aplicativo
Migre o código do aplicativo.	Migre o código do aplicativo para os novos servidores.	Proprietário do aplicativo
Configure o servidor de aplicações.	Configure o servidor do aplicativo para o banco de dados e os drivers de destino.	Proprietário do aplicativo
Otimize o código do aplicativo.	Otimize o código do aplicativo para o mecanismo de destino.	Proprietário do aplicativo

Vá para o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Valide os usuários.	No banco de dados de destino do Amazon Redshift, valide	DBA

Tarefa	Descrição	Habilidades necessárias
	os usuários e conceda a eles funções e privilégios.	
Valide se o aplicativo está bloqueado.	Verifique se o aplicativo está bloqueado para evitar mais alterações.	Proprietário do aplicativo
Valide os dados.	Valide os dados no banco de dados de destino do Amazon Redshift.	DBA
Ative chaves e gatilhos externos.	Ative chaves e gatilhos externos no banco de dados de destino do Amazon Redshift.	DBA
Conecte-se ao novo banco de dados.	Configure o aplicativo para se conectar ao novo banco de dados do Amazon Redshift.	Proprietário do aplicativo
Execute as verificações finais.	Faça uma verificação final e abrangente do sistema antes de entrar em operação.	DBA, proprietário do aplicativo
Acesse.	Acesse o banco de dados de destino do Amazon Redshift.	DBA

Feche o projeto de migração

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.	Encerre recursos temporários da AWS, como a instância de replicação do AWS DMS e a EC2 instância usada para o AWS SCT.	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Analise documentos.	Revise e valide os documentos do projeto de migração.	DBA, administrador de sistemas
Colete métricas.	Colete informações sobre o projeto de migração, como o tempo de migração, a porcentagem de tarefas manuais versus tarefas de ferramentas e a economia total de custos.	DBA, administrador de sistemas
Encerre o projeto.	Feche o projeto e forneça feedback.	DBA, administrador de sistemas

Recursos relacionados

Referências

- Guia do usuário do AWS DMS
- Guia do usuário do AWS SCT
- Bem-vindo ao Guia de conceitos básicos do Amazon Redshift

Tutoriais e vídeos

- Mergulhe profundamente no AWS SCT e no AWS DMS (apresentação do AWS re:Invent 2019)
- Introdução ao AWS Database Migration Service

Migrar um banco de dados Oracle para o Aurora PostgreSQL usando AWS DMS e AWS SCT

Criado por Senthil Ramasamy (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados Oracle para o Amazon Aurora Edição Compatível com PostgreSQL usando o AWS Data Migration Service (AWS DMS) e o AWS Schema Conversion Tool (AWS SCT).

O padrão abrange bancos de dados Oracle de origem que estão no local, bancos de dados Oracle instalados em instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e Amazon Relational Database Service (Amazon RDS) para bancos de dados Oracle. O padrão converte esses bancos de dados em compatíveis com o Aurora PostgreSQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle em um datacenter on-premises ou na Nuvem AWS.
- Clientes SQL instalados em uma máquina local ou em uma EC2 instância.
- Drivers de conectividade de banco de dados Java (JDBC) para conectores AWS SCT, instalados em uma máquina local ou em uma instância em que o AWS SCT EC2 está instalado.

Limitações

- Limite de tamanho do banco de dados: 128 TB
- Se o banco de dados de origem suportar um aplicativo comercial off-the-shelf (COTS) ou for específico do fornecedor, talvez você não consiga convertê-lo em outro mecanismo de banco de dados. Antes de usar esse padrão, confirme se o aplicativo é compatível com o Aurora PostgreSQL.

Versões do produto

- No caso de bancos de dados Oracle autogerenciados, o DMS da AWS é compatível com todas as edições de banco de dados Oracle para as versões 10.2 e posteriores (para versões 10.x), 11g e

até 12.2, 18c e 19c. Para obter a lista mais recente das versões compatíveis do banco de dados Oracle (tanto autogerenciadas quanto do Amazon RDS para Oracle), consulte Usando um banco de dados Oracle como origem para o AWS DMS e Usando um banco de dados PostgreSQL como destino para o AWS DMS.

- Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos. Para obter informações sobre as versões do banco de dados Oracle suportadas pelo AWS SCT, consulte a documentação do AWS SCT.
- O Aurora oferece suporte às versões do PostgreSQL listadas nas versões de mecanismo e versões do Amazon Aurora PostgreSQL.

Arquitetura

Pilha de tecnologia de origem

Um dos seguintes:

- Um banco de dados Oracle on-premises
- Um banco de dados Oracle em uma EC2 instância
- Instância de banco de dados do Amazon RDS para Oracle

Pilha de tecnologias de destino

- Aurora compatível com PostgreSQL

Arquitetura de destino

Arquitetura de migração de dados

- De um banco de dados Oracle que executa na Nuvem AWS

- De um banco de dados Oracle que executa em um datacenter on-premises

Ferramentas

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O AWS Schema Conversion Tool (AWS SCT) é compatível com as migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maioria do código personalizado em um formato compatível com o banco de dados de destino.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Preparar o banco de dados de origem.	Para preparar o banco de dados de origem, consulte Como usar o banco de dados Oracle como origem para o AWS SCT na documentação do AWS SCT.	DBA
Crie uma EC2 instância para o AWS SCT.	Crie e configure uma EC2 instância para o AWS SCT, se necessário.	DBA
Baixe o AWS SCT.	Faça download da versão mais recente do AWS SCT e dos drivers associados. Para obter mais informações, consulte Instalação, verificação e atualização do AWS SCT na documentação do AWS SCT.	DBA
Adicione usuários e permissões do IAM.	Adicione e valide os pré-requisitos de usuários e permissões	DBA

Tarefa	Descrição	Habilidades necessárias
	s no banco de dados de origem.	
Crie um projeto AWS SCT.	Crie um projeto AWS SCT para o workload e conecte-se ao banco de dados de origem. Para obter instruções, consulte Como criar um projeto do AWS SCT e Adicionar servidores de banco de dados na documentação do AWS SCT.	DBA
Avaliar a viabilidade.	Gere um relatório de avaliação, que resume os itens de ação para esquemas que não podem ser convertidos automaticamente e fornece estimativas para esforços de conversão manual. Para obter mais informações, consulte Criação e revisão do relatório de avaliação da migração do banco de dados na documentação do AWS SCT.	DBA

Preparar o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de banco de dados do Amazon RDS.	Crie uma instância de banco de dados Amazon RDS de destino, usando o Amazon Aurora como mecanismo de	DBA

Tarefa	Descrição	Habilidades necessárias
	banco de dados. Para obter instruções, consulte Criação de uma instância de banco de dados Amazon RDS na documentação do Amazon RDS.	
Extraia usuários, funções e permissões.	Extraia a lista de usuários, funções e permissões do banco de dados de origem.	DBA
Usuários do mapa.	Mapeie os usuários do banco de dados existentes para os novos usuários do banco de dados.	Proprietário do App
Crie usuários.	Criar usuários no banco de dados de destino.	DBA, proprietário do aplicativo
Aplique funções.	Aplique funções da etapa anterior ao banco de dados de destino.	DBA
Verifique as opções, os parâmetros, os arquivos de rede e os links do banco de dados.	Examine o banco de dados de origem em busca de opções, parâmetros, arquivos de rede e links de banco de dados e, em seguida, avalie sua aplicabilidade ao banco de dados de destino.	DBA
Configurações de aplicação.	Aplique todas as configura ções relevantes ao banco de dados de destino.	DBA

Transferir objetos

Tarefa	Descrição	Habilidades necessárias
Configure a conectividade do AWS SCT.	Configure a conectividade do AWS SCT com o banco de dados de destino.	DBA
Converta o esquema usando o AWS SCT.	O AWS SCT converte automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino. Qualquer código que não possa ser convertido automaticamente pela ferramenta será marcado em destaque para que seja convertido manualmente.	DBA
Analise o relatório.	Revise o relatório SQL gerado e salve quaisquer erros e avisos.	DBA
Aplique alterações automatizadas no esquema.	Aplique alterações automatizadas de esquema ao banco de dados de destino ou salve-as como um arquivo .sql.	DBA
Valide objetos.	Valide se o AWS SCT criou os objetos no destino.	DBA
Gerencie itens que não foram convertidos.	Reescreva, rejeite ou redesenhe manualmente todos os itens que falharam na conversão automática.	DBA, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Aplicar permissões de funções e permissões de usuário.	Aplique a função gerada e as permissões do usuário e analise todas as exceções.	DBA

Migre os dados

Tarefa	Descrição	Habilidades necessárias
Determine o método.	Determine o método de migração de dados.	DBA
Criação de uma instância de replicação.	Crie uma instância de replicação do console do AWS DMS. Para obter mais informações, consulte Trabalho com uma instância de replicação do AWS DMS na documentação do AWS DMS.	DBA
Criação de endpoints de origem e de destino.	Para criar endpoints, siga as instruções em Criação de endpoints de origem e destino na documentação do AWS DMS.	DBA
Criar uma tarefa de replicaçã o.	Para criar uma tarefa, consulte Trabalho com tarefas do AWS DMS na documentação do AWS DMS.	DBA
Inicie a tarefa de replicação e monitore os logs.	Para obter mais informações sobre essa etapa, consulte Monitoramento de tarefas do	DBA

Tarefa	Descrição	Habilidades necessárias
	AWS DMS na documentação do AWS DMS.	

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Analise e converta itens SQL no código do aplicativo.	Use o AWS SCT para analisar e converter os itens SQL no código do aplicativo. Ao converter o esquema do seu banco de dados de um mecanismo para outro, é preciso também atualizar o código SQL nos seus aplicativos, a fim de interagir com o novo mecanismo de banco de dados, em vez do antigo. Você pode visualizar, analisar, editar e salvar o código SQL convertido.	Proprietário do App
Crie servidores de aplicações.	Crie os novos servidores de aplicativos na AWS.	Proprietário do App
Migre o código do aplicativo.	Migre o código do aplicativo para os novos servidores.	Proprietário do App
Configure os servidores dos aplicativos.	Configure os servidores de aplicativos para o banco de dados e os drivers de destino.	Proprietário do App
Corrija o código.	Corrija qualquer código específico do mecanismo de	Proprietário do App

Tarefa	Descrição	Habilidades necessárias
	banco de dados de origem em seu aplicativo.	
Otimize o código.	Otimize o código do seu aplicativo para o mecanismo de banco de dados de destino.	Proprietário do App

Substituir

Tarefa	Descrição	Habilidades necessárias
Vá para o banco de dados de destino.	Execute a substituição para o novo banco de dados.	DBA
Bloqueie o aplicativo.	Bloqueie o aplicativo de quaisquer outras alterações.	Proprietário do App
Validar alterações.	Validar se todas as alteraçõe s foram propagadas para o banco de dados de destino.	DBA
Redirecione para banco de dados de destino.	Aponte os novos servidores de aplicativos para o banco de dados de destino.	Proprietário do App
Confira tudo.	Execute uma verificação final e abrangente do sistema.	Proprietário do App
Acesse.	Conclua as tarefas finais de substituição.	Proprietário do App

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários.	Encerre os recursos temporários da AWS, como a instância de replicação do AWS DMS e a EC2 instância usada para o AWS SCT.	DBA, proprietário do aplicativo
Feedback de atualização.	Atualize o feedback sobre o processo do AWS DMS para as equipes internas.	DBA, proprietário do aplicativo
Revise o processo e os modelos.	Revise o processo do AWS DMS e melhore o modelo, se necessário.	DBA, proprietário do aplicativo
Valide os documentos.	Revise e valide os documentos do projeto.	DBA, proprietário do aplicativo
Colete métricas.	Reúna métricas para avaliar o tempo de migração, a porcentagem de economia de custos manuais versus ferramentas e assim por diante.	DBA, proprietário do aplicativo
Fechar o projeto.	Encerre o projeto de migração e forneça feedback às partes interessadas.	DBA, proprietário do aplicativo

Recursos relacionados

Referências

- Uso de um banco de dados Oracle como origem para o AWS DMS
- Uso do banco de dados PostgreSQL como destino para o AWS Database Migration Service

- Manual de migração do Oracle Database 11g/12c para Amazon Aurora com compatibilidade com PostgreSQL (9.6.x)
- Manual de migração do Oracle Database 19c para o Amazon Aurora com compatibilidade com PostgreSQL (12.4)
- Migrar um banco de dados do Amazon RDS para Oracle para o Amazon Aurora Edição Compatível com PostgreSQL
- AWS Data Migration Service
- AWS Schema Conversion Tool
- Migre da Oracle para o Amazon Aurora
- Preços do Amazon RDS

Tutoriais e vídeos

- Passo a Step-by-Step passo da migração de banco de dados
- Conceitos básicos do AWS DMS
- Conceitos básicos do Amazon RDS
- AWS Database Migration Service (vídeo)
- Migração de um banco de dados do Oracle para PostgreSQL (vídeo)

Mais informações

.

Migrar dados de um banco de dados Oracle on-premises para o Aurora PostgreSQL

Criado por Michelle Deng (AWS) e Shunan Xiang (AWS)

Resumo

Esse padrão fornece orientação para a migração de dados de um banco de dados Oracle on-premises para a edição compatível com Amazon Aurora PostgreSQL. Aborda uma estratégia de migração de dados on-line com um mínimo de tempo de inatividade para bancos de dados Oracle de vários terabytes que contêm grandes tabelas com atividades de alta linguagem de manipulação de dados (DML). Um banco de dados standby Oracle Active Data Guard é usado como fonte para descarregar a migração de dados do banco de dados principal. A replicação do banco de dados principal Oracle para o modo de espera pode ser suspensa durante a carga total para evitar erros do ORA-01555.

Colunas de tabela em chaves primárias (PKs) ou chaves estrangeiras (FKs), com o tipo de dados NUMBER, são comumente usadas para armazenar números inteiros no Oracle. Recomendamos que você os converta em INT ou BIGINT no PostgreSQL para melhorar o desempenho. Você pode usar a AWS Schema Conversion Tool (AWS SCT) para alterar o mapeamento de tipos de dados padrão para as colunas PK e FK. (Para obter mais informações, consulte a postagem no blog da AWS Converter o tipo de dados NUMBER do Oracle para o PostgreSQL.) A migração de dados nesse padrão usa o AWS Database Migration Service (AWS DMS) para carga total e captura de dados alterados (CDC).

Você também pode usar esse padrão para migrar um banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) para PostgreSQL ou um banco de dados Oracle hospedado no Amazon Elastic Compute Cloud (Amazon) para o Amazon EC2 RDS for PostgreSQL ou compatível com o Aurora PostgreSQL.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem Oracle em um datacenter on-premises com o Active Data Guard configurado em espera
- AWS Direct Connect configurado entre o datacenter on-premises e a Nuvem AWS
- Familiaridade com o uso de um banco de dados Oracle como origem para o AWS DMS
- Familiaridade com o uso de um banco de dados PostgreSQL como destino para o AWS DMS

Limitações

- Os clusters de banco de dados Amazon Aurora podem ser criados com até 128 TiB de armazenamento. As instâncias de banco de dados do Amazon RDS para PostgreSQL podem ser criadas com até 64 TiB de armazenamento. Para obter as informações de armazenamento mais recentes, consulte Armazenamento e confiabilidade do Amazon Aurora e armazenamento de instâncias de banco de dados do Amazon RDS na documentação da AWS.

Versões do produto

- O AWS DMS oferece suporte a todas as edições do banco de dados Oracle para as versões 10.2 e versões posteriores (para versões 10.x), 11g e até 12.2, 18c e 19c. Para obter a lista mais recente de versões compatíveis, consulte Uso de um banco de dados Oracle como origem para o AWS DMS na documentação da AWS.

Arquitetura

Pilha de tecnologia de origem

- Bancos de dados Oracle on-premises com o Oracle Active Data Guard configurado em espera

Pilha de tecnologias de destino

- Aurora compatível com PostgreSQL

Arquitetura de migração de dados

Ferramentas

- AWS DMS: o AWS Database Migration Service (AWS DMS) oferece suporte a vários bancos de dados de origem e destino. Consulte Uso de um banco de dados Oracle como origem para o AWS DMS na documentação do AWS DMS para obter uma lista das versões e edições dos bancos de dados Oracle de origem e destino compatíveis. Se o banco de dados de origem não for suportado pelo AWS DMS, você deverá selecionar outro método para migrar os dados na Fase 6 (na seção Epics). Observação importante: como essa é uma migração heterogênea, você deve primeiro verificar se o banco de dados oferece suporte a um aplicativo comercial off-the-shelf (COTS). Se o aplicativo for COTS, consulte o fornecedor para confirmar se o é compatível com o Aurora

PostgreSQL antes de continuar. Para obter mais informações, consulte as instruções de Step-by-Step migração do AWS DMS na documentação da AWS.

- AWS SCT: a AWS Schema Conversion Tool (AWS SCT) facilita migrações heterogêneas de bancos de dados ao converter automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino. O código personalizado que a ferramenta converte inclui visualizações, procedimentos armazenados e funções. Qualquer código que não possa ser convertido automaticamente pela ferramenta será marcado em destaque para que você mesmo possa convertê-lo.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões dos bancos de dados de origem e de destino.		DBA
Instale o AWS SCT e os drivers.		DBA
Adicione e valide os usuários pré-requisitos do AWS SCT e o banco de dados de fontes concessões.		DBA
Crie um projeto AWS SCT para o workload e conecte-se ao banco de dados de origem.		DBA
Gere um relatório de avaliação e avalie a viabilidade.		DBA, proprietário do aplicativo

Preparar o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Crie um banco de dados de destino compatível com o Aurora PostgreSQL.		DBA
Extraia a lista de usuários, funções e concessões do banco de dados de origem.		DBA
Mapeie os usuários do banco de dados existentes para os novos usuários do banco de dados.		Proprietário do App
Criar usuários no banco de dados de destino.		DBA
Aplique as funções da etapa anterior ao banco de dados de destino compatível com o Aurora PostgreSQL.		DBA
Analise as opções, os parâmetros, os arquivos de rede e os links do banco de dados de origem e avalie sua aplicabilidade ao banco de dados de destino.		DBA, proprietário do aplicativo
Aplique todas as configura ções relevantes ao banco de dados de destino.		DBA

Prepare-se para a conversão de objetos de códigos do banco de dados

Tarefa	Descrição	Habilidades necessárias
Configure a conectividade do AWS SCT com o banco de dados de destino.		DBA
Converta o esquema no AWS SCT e salve o código convertido como um arquivo .sql.		DBA, proprietário do aplicativo
Converta manualmente qualquer objeto de banco de dados que falhou na conversão automática.		DBA, proprietário do aplicativo
Otimize a conversão do código do banco de dados.		DBA, proprietário do aplicativo
Separe o arquivo .sql em vários arquivos .sql com base no tipo de objeto.		DBA, proprietário do aplicativo
Valide os scripts SQL no banco de dados de destino.		DBA, proprietário do aplicativo

Prepare a migração de dados

Tarefa	Descrição	Habilidades necessárias
Criar uma instância de replicação do AWS DMS.		DBA
Criação de endpoints de origem e de destino.	Se o tipo de dados do PKs e FKs for convertido de NUMBER no Oracle para	DBA

Tarefa	Descrição	Habilidades necessárias
	BIGINT no PostgreSQL, considere especificar o `numberDataTypeScale=-2` atributo de conexão ao criar o endpoint de origem.	

Migrar dados – carga total

Tarefa	Descrição	Habilidades necessárias
Crie o esquema e as tabelas no banco de dados de destino.		DBA
Crie tarefas de carga completa do AWS DMS agrupando tabelas ou dividindo uma tabela grande com base no tamanho da tabela.		DBA
Interrompa os aplicativos nos bancos de dados Oracle de origem por um curto período.		Proprietário do App
Verifique se o banco de dados stand-by Oracle está sincronizado com o banco de dados principal e interromp a a replicação do banco de dados principal para o banco de dados stand-by.		DBA, proprietário do aplicativo
Inicie os aplicativos no banco de dados Oracle de origem.		Proprietário do App
Inicie as tarefas de carga total do AWS DMS em paralelo, do		DBA

Tarefa	Descrição	Habilidades necessárias
banco de dados em espera da Oracle ao banco de dados compatível com o Aurora PostgreSQL.		
Crie PKs índices secundári os após a conclusão da carga completa.		DBA
Valide os dados.		DBA

Migrar dados – CDC

Tarefa	Descrição	Habilidades necessárias
Crie tarefas de replicaçã o contínuas do AWS DMS especificando um horário de início personalizado do CDC ou um número de alteração do sistema (SCN) quando o Oracle standby foi sincronizado com o banco de dados principal e antes de os aplicativos serem reiniciados na tarefa anterior.		DBA
Inicie as tarefas do AWS DMS em paralelo para replicar as mudanças contínuas do banco de dados em espera da Oracle para o banco de dados compatível com o Aurora PostgreSQL.		DBA

Tarefa	Descrição	Habilidades necessárias
Restabeleça a replicação do banco de dados principal Oracle para o banco de dados standby.		DBA
Monitore os registros e interrompa os aplicativos no banco de dados Oracle quando o banco de dados de destino compatível com o Aurora PostgreSQL estiver quase sincronizado com o banco de dados Oracle de origem.		DBA, proprietário do aplicativo
Interrompa as tarefas do AWS DMS quando o destino estiver totalmente sincronizado com o banco de dados Oracle de origem.		DBA
Crie FKs e valide os dados no banco de dados de destino.		DBA
Crie funções, visualizações, acionadores, sequências e outros tipos de objetos no banco de dados de destino.		DBA
Aplique concessões de funções no banco de dados de destino.		DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Use o AWS SCT para analisar e converter as instruções SQL dentro do código do aplicativo.		Proprietário do App
Crie novos servidores de aplicativos na AWS.		Proprietário do App
Migre o código do aplicativo para os novos servidores.		Proprietário do App
Configure o servidor do aplicativo para o banco de dados e os drivers de destino.		Proprietário do App
Corrija qualquer código específico do mecanismo de banco de dados de origem no aplicativo.		Proprietário do App
Otimize o código do aplicativo para o banco de dados de destino.		Proprietário do App

Substituir

Tarefa	Descrição	Habilidades necessárias
Direcione o novo aplicativo para o novo banco de dados de destino.		DBA, proprietário do aplicativo
Realize testes de sanidade.		DBA, proprietário do aplicativo
Acesse.		DBA, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, administrador de sistemas
Revise e valide os documentos do projeto.		DBA, proprietário do aplicativo
Reúna métricas de tempo de migração, porcentagem de uso manual em comparação com o uso de ferramentas, economia de custos e dados similares.		DBA, proprietário do aplicativo
Feche o projeto e forneça feedback.		DBA, proprietário do aplicativo

Recursos relacionados

Referências

- Banco de dados Oracle para banco de dados compatível com Aurora PostgreSQL: Manual de migração
- Migração de um banco de dados Amazon RDS para Oracle pra um banco de dados Amazon Aurora MySQL
- Site do AWS DMS
- Documentação do AWS DMS
- Site do AWS SCT
- Documentação do AWS SCT
- Migre do Oracle para o Amazon Aurora

Tutoriais

- Conceitos básicos do AWS DMS
- Conceitos básicos do Amazon RDS
- Instruções passo a Step-by-Step passo do AWS Database Migration Service

Migre do SAP ASE para o Amazon RDS para SQL Server usando o AWS DMS

Criado por Amit Kumar (AWS)

Resumo

Esse padrão fornece orientações para migrar um banco de dados do SAP Adaptive Server Enterprise (ASE) para uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS) que executa o Microsoft SQL Server. O banco de dados de origem pode estar localizado em um data center local ou em uma instância do Amazon Elastic Compute Cloud EC2 (Amazon). O padrão usa o AWS Database Migration Service (AWS DMS) para migrar dados e (opcionalmente) ferramentas de engenharia de software assistida por computador (CASE) para converter o esquema do banco de dados.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados SAP ASE em um data center local ou em uma instância EC2
- Um banco de dados de destino do Amazon RDS para SQL Server que está ativo e funcionando

Limitações

- Limite de tamanho do banco de dados: 64 TB

Versões do produto

- Somente SAP ASE versão 15.7 ou 16.x. Para obter as informações mais recentes, consulte Como usar um banco de dados do SAP como origem para o AWS DMS.
- Para bancos de dados de destino do Amazon RDS, o AWS DMS oferece suporte às versões do Microsoft SQL Server no Amazon RDS para as edições Enterprise, Standard, Web e Express. Para obter as informações mais recentes sobre as versões compatíveis, consulte a documentação do AWS DMS. Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados SAP ASE que está no local ou em uma EC2 instância da Amazon

Pilha de tecnologias de destino

- Uma instância de banco de dados do Amazon RDS para SQL Server

Arquitetura de origem e destino

De um banco de dados SAP ASE na Amazon EC2 para uma instância de banco de dados Amazon RDS for SQL Server:

De um banco de dados SAP ASE on-premises a uma instância de banco de dados do Amazon RDS para SQL Server:

Ferramentas

- O AWS Database Migration Service (AWS DMS) é um serviço web que você pode usar para migrar dados do seu banco de dados local, em uma instância de banco de dados Amazon RDS ou em um banco de dados em uma EC2 instância, para um banco de dados em um serviço da AWS, como Amazon RDS for SQL Server ou uma instância. EC2 Você também pode migrar um banco de dados de um serviço da AWS para um banco de dados on-premises. Você pode migrar dados entre mecanismos de banco de dados heterogêneos ou homogêneos.
- Para conversões de esquema, você pode, opcionalmente, usar o erwin Data Modeler ou o SAP. PowerDesigner

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões dos bancos de dados de origem e de destino.		DBA

Tarefa	Descrição	Habilidades necessárias
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, SysAdmin
Escolher o tipo de instância adequado com base na capacidade, nos atributos de armazenamento e nos atributos de rede.		DBA, SysAdmin
Identifique os requisitos de segurança de acesso à rede para os bancos de dados de origem e de destino.		DBA, SysAdmin
Identifique a estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC) e sub-redes.		SysAdmin
Crie grupos de segurança e listas de controle de acesso à rede (ACLs).		SysAdmin
Configure e inicie uma instância de banco de dados do Amazon RDS.		SysAdmin

Migrar dados - opção 1

Tarefa	Descrição	Habilidades necessárias
Migre o esquema do banco de dados manualmente ou use uma ferramenta CASE, como o erwin Data Modeler ou o SAP. PowerDesigner		DBA

Migrar dados - opção 2

Tarefa	Descrição	Habilidades necessárias
Migre dados usando o AWS DMS.		DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Substituir

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.		DBA SysAdmin, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, SysAdmin
Revise e valide os documentos do projeto.		DBA SysAdmin, proprietário do aplicativo
Reúna métricas como tempo para migrar, porcentagem de tarefas manuais versus automatizadas e economia de custos.		DBA SysAdmin, proprietário do aplicativo
Feche o projeto e forneça feedback.		DBA SysAdmin, proprietário do aplicativo

Recursos relacionados

Referências

- Site do AWS DMS
- Preços do Amazon RDS
- Uso de um banco de dados SAP ASE como fonte para AWS DMS
- Limitações do RDS Custom for SQL Server

Tutoriais e vídeos

- Conceitos básicos do AWS DMS
- Conceitos básicos do Amazon RDS
- AWS DMS (vídeo)
- Amazon RDS (vídeo)

Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift utilizando o AWS DMS

Criado por Marcelo Fernandes (AWS)

Resumo

Esse padrão fornece orientações para migrar um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift utilizando o AWS Data Migration Service (AWS DMS).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Microsoft SQL Server de origem em um datacenter on-premises
- Pré-requisitos preenchidos para usar um banco de dados do Amazon Redshift como destino para o AWS DMS, conforme discutido na AWS DMS documentation.

Versões do produto

- SQL Server 2005-2019, edições Enterprise, Standard, Workgroup, Developer e Web. Para obter a lista mais recente de versões compatíveis, consulte Usar um banco de dados Microsoft SQL Server como origem para o AWS DMS na documentação da AWS.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Microsoft SQL Server on-premises

Pilha de tecnologias de destino

- Amazon Redshift

Arquitetura de migração de dados

Ferramentas

- O AWS DMS é um serviço de migração de dados que oferece suporte a vários tipos de bancos de dados de origem e destino. Para obter informações sobre as versões e edições do banco de dados do SQL Server compatíveis com o AWS DMS, consulte Usar um banco de dados do Microsoft SQL Server como origem para o AWS DMS na documentação do AWS DMS. Se o AWS DMS não for compatível com o banco de dados de origem, você deve selecionar um método alterativo para migrar os dados.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide a versão e o mecanismo dos bancos de dados de origem e de destino.		DBA
Identifique os requisitos de hardware para a instância do servidor de destino.		DBA, administrador de sistemas
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, administrador de sistemas
Escolha o tipo de instância adequado com base na capacidade, nos atributos de armazenamento e nos atributos de rede.		DBA, administrador de sistemas
Identifique os requisitos de segurança de acesso à rede para os bancos de dados de origem e de destino.		DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Identifique a estratégia de migração de aplicativos.		DBA, proprietário do aplicativo, administrador de sistemas

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).	Para obter mais informações, consulte Trabalhar com uma instância de banco de dados em uma VPC na documentação da AWS.	Administrador de sistemas
Criar grupos de segurança.		Administrador de sistemas
Configurar e iniciar um cluster do Amazon Redshift.	Para obter mais informações sobre isso, consulte Criar um exemplo de cluster do Amazon Redshift na documentação do Amazon Redshift.	DBA, administrador de sistemas

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Migrar os dados do banco de dados Microsoft SQL Server usando o AWS DMS.		DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos.		DBA, proprietário do aplicativo, administrador de sistemas

Substituir

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.		DBA, proprietário do aplicativo, administrador de sistemas

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários.		DBA, administrador de sistemas
Revise e valide os documentos do projeto.		DBA, proprietário do aplicativo, administrador de sistemas
Reúna métricas como tempo para migrar, porcentagem de tarefas manuais versus automatizadas e economia de custos.		DBA, proprietário do aplicativo, administrador de sistemas
Feche o projeto e forneça feedback.		DBA, proprietário do aplicativo, administrador de sistemas

Recursos relacionados

Referências

- Documentação do AWS DMS
- Documentação do Amazon Redshift
- Preços do Amazon Redshift

Tutoriais e vídeos

- Conceitos básicos do AWS DMS
- Conceitos básicos do Amazon Redshift
- Uso do banco de dados Amazon Redshift como destino para o AWS Database Migration Service
- AWS DMS (vídeo)

Migre um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift usando agentes de extração de dados da AWS SCT

Criado por Neha Thakur (AWS)

Resumo

Esse padrão descreve as etapas para migrar um banco de dados de origem on-premises do Microsoft SQL Server para um banco de dados de destino do Amazon Redshift usando agentes de extração de dados da AWS Schema Conversion Tool (AWS SCT). Um agente é um programa externo integrado à AWS SCT, mas executa a transformação de dados em outro local e interage com outros serviços da AWS em seu nome.

Pré-requisitos e limitações

Pré-requisitos

- Um banco de dados de origem Microsoft SQL Server usado para o workload do data warehouse em um datacenter on-premises
- Uma conta AWS ativa

Versões do produto

- Microsoft SQL Server versão 2008 ou mais recente. Para obter a lista mais recente de versões compatíveis, consulte a documentação do AWS SCT.

Arquitetura

pilha de tecnologiaOrigem

- Um banco de dados Microsoft SQL Server on-premises

pilha de tecnologiaDestino

- Amazon Redshift

Arquitetura de migração de dados

Ferramentas

- A AWS Schema Conversion Tool (AWS SCT) facilita as migrações heterogêneas de banco de dados convertendo automaticamente o schema do banco de dados de origem e a maioria do código personalizado para um formato compatível com o banco de dados de destino. Quando os bancos de dados de origem e de destino são muito diferentes, você pode usar um agente do AWS SCT para realizar transformações adicionais de dados. Para obter mais informações, consulte Migrar dados de um data warehouse on-premises para o Amazon Redshift na documentação da AWS

Práticas recomendadas

- Melhores práticas para AWS SCT
- Práticas recomendadas do Amazon Redshift

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Validar versões e mecanismos do banco de dados de origem e de destino.		DBA
Identifique os requisitos de hardware para a instância do servidor de destino.		DBA, SysAdmin
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, SysAdmin
Escolha o tipo de instância adequado (capacidade,		DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
atributos de armazenamento e atributos de rede).		
Identifique os requisitos de segurança do acesso à rede para os bancos de dados de origem e de destino.		DBA, SysAdmin
Escolha uma estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC) e sub-redes.		SysAdmin
Criar grupos de segurança.		SysAdmin
Configure e inicie o cluster do Amazon Redshift.		SysAdmin

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Migre os dados usando os agentes de extração de dados da AWS SCT.		DBA

Migrar aplicativos

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos escolhida.		DBA SysAdmin, proprietário do aplicativo

Vá para o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.		DBA SysAdmin, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, SysAdmin
Revise e valide os documentos do projeto.		DBA SysAdmin, proprietário do aplicativo
Reúna métricas como tempo para migrar, porcentagem de tarefas manuais versus automatizadas e economia de custos.		DBA SysAdmin, proprietário do aplicativo
Feche o projeto e forneça feedback, se houver.		DBA SysAdmin, proprietário do aplicativo

Recursos relacionados

Referências

- Guia do usuário do AWS SCT
- Uso de agentes de extração de dados
- Preços do Amazon Redshift

Tutoriais e vídeos

- Conceitos básicos da AWS Schema Conversion Tool
- Conceitos básicos do Amazon Redshift

Migre um banco de dados Teradata para o Amazon Redshift usando agentes de extração de dados do AWS SCT

Criado por Sergey Dmitriev (AWS)

Resumo

Este padrão fornece orientações detalhadas sobre as etapas para migrar um banco de dados Teradata, usado como um data warehouse em um datacenter on-premises, para um banco de dados Amazon Redshift. O padrão usa agentes de extração de dados do AWS Schema Conversion Tool (AWS SCT). Um agente é um programa externo integrado à AWS SCT, mas executa a transformação de dados em outro local e interage com outros serviços da AWS em seu nome.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Teradata de origem em um datacenter on-premises

Versões do produto

- Teradata versão 13 e posterior. Para obter a lista mais recente de versões compatíveis, consulte a documentação do AWS SCT.

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Teradata on-premises

Pilha de tecnologias de destino

- Cluster do Amazon Redshift

Arquitetura de migração de dados

Ferramentas

- AWS SCT: a AWS Schema Conversion Tool (AWS SCT) facilita as migrações heterogêneas de banco de dados convertendo automaticamente o schema do banco de dados de origem e a maioria do código personalizado para um formato compatível com o banco de dados do destino. Quando os bancos de dados de origem e de destino são muito diferentes um do outro, você pode usar um agente do AWS SCT para realizar transformações adicionais de dados. Para obter mais informações, consulte Migração de dados de um Data Warehouse On-Premises para o Amazon Redshift na documentação da AWS.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Validar versões e mecanismos do banco de dados de origem e de destino.		DBA
Identifique os requisitos de hardware para a instância do servidor de destino.		DBA, SysAdmin
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, SysAdmin
Escolha o tipo de instância adequado (capacidade, atributos de armazenamento e atributos de rede).		DBA, SysAdmin
Identifique os requisitos de segurança do acesso à rede para os bancos de dados de origem e de destino.		DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
Escolha uma estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC) e sub-redes.		SysAdmin
Criar grupos de segurança.		SysAdmin
Configure e inicie o cluster do Amazon Redshift.		SysAdmin

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Migre os dados usando os agentes de extração de dados do AWS SCT.	Para obter informações detalhadas sobre o uso dos agentes de extração de dados do AWS SCT, consulte os links na seção Referências e Ajuda.	DBA

Migrar aplicativos

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos escolhida.		DBA SysAdmin, proprietário do aplicativo

Substitua o banco de dados Amazon Redshift de destino

Tarefa	Descrição	Habilidades necessárias
Mude os clientes de aplicativos para a nova infraestrutura.		DBA SysAdmin, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, SysAdmin
Revise e valide os documentos do projeto.		DBA SysAdmin, proprietário do aplicativo
Reúna métricas sobre o tempo de migração, porcentagem de tarefas manuais versus tarefas de ferramentas, economia de custos, etc.		DBA SysAdmin, proprietário do aplicativo
Feche o projeto e forneça feedback, se houver.		

Recursos relacionados

Referências

- Guia do usuário do AWS SCT
- Uso de agentes de extração de dados
- Preços do Amazon Redshift
- Converta o atributo Teradata RESET WHEN para o Amazon Redshift SQL (Recomendações da AWS)

- Converta o atributo temporal Teradata NORMALIZE no Amazon Redshift SQL (Recomendações da AWS)

Tutoriais

- Conceitos básicos do AWS Schema Conversion Tool
- Conceitos básicos do Amazon Redshift

Migre um banco de dados Vertica on-premises para o Amazon Redshift usando agentes de extração de dados do AWS SCT

Criado por Sergey Dmitriev (AWS)

Resumo

Esse padrão fornece orientação para migrar um banco de dados Vertica on-premises para um cluster do Amazon Redshift usando agentes de extração de dados da AWS Schema Conversion Tool (AWS SCT). Um agente é um programa externo integrado à AWS SCT, mas executa a transformação de dados em outro local e interage com outros serviços da AWS em seu nome.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem Vertica usado para o workload do data warehouse em um datacenter on-premises
- Um cluster de destino do Amazon Redshift

Versões do produto

- Vertica versão 7.2.2 e superior. Para obter a lista mais recente de versões compatíveis, consulte a documentação do AWS SCT.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Vertica on-premises

Pilha de tecnologias de destino

- Um cluster do Amazon Redshift

Arquitetura de migração de dados

Ferramentas

- A AWS Schema Conversion Tool (AWS SCT) facilita as migrações heterogêneas de banco de dados convertendo automaticamente o schema do banco de dados de origem e a maioria do código personalizado para um formato compatível com o banco de dados de destino. Quando os bancos de dados de origem e de destino são muito diferentes um do outro, você pode usar um agente do AWS SCT para realizar transformações adicionais de dados. Para obter mais informações, consulte Migração de dados de um Data Warehouse On-Premises para o Amazon Redshift na documentação da AWS.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões dos bancos de dados de origem e de destino.		DBA
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, SysAdmin
Escolha o tipo de instância adequado (capacidade, atributos de armazenamento e atributos de rede).		DBA, SysAdmin
Identifique os requisitos de segurança do acesso à rede para os bancos de dados de origem e de destino.		DBA, SysAdmin
Escolha uma estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC) e sub-redes.		SysAdmin
Criar grupos de segurança.		SysAdmin
Configurar e iniciar um cluster do Amazon Redshift.		SysAdmin

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Migre os dados usando os agentes de extração de dados da AWS SCT.	Para obter informações detalhadas sobre o uso dos agentes de extração de dados do AWS SCT, consulte os links na seção Referências e Ajuda.	DBA

Migrar aplicativos

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos escolhida.		DBA SysAdmin, proprietário do aplicativo

Vá para o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Mude os clientes de aplicativos para a nova infraestrutura.		DBA SysAdmin, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, SysAdmin
Revise e valide os documentos do projeto.		DBA SysAdmin, proprietário do aplicativo
Reúna métricas sobre o tempo de migração, porcentagem de tarefas manuais versus tarefas de ferramentas, economia de custos, etc.		DBA SysAdmin, proprietário do aplicativo
Feche o projeto e forneça feedback, se houver.		

Recursos relacionados

Referências

- Guia do usuário do AWS SCT
- Uso de agentes de extração de dados
- Preços do Amazon Redshift

Tutoriais e vídeos

- Conceitos básicos da AWS Schema Conversion Tool

- Conceitos básicos do Amazon Redshift

Migre aplicativos legados do Oracle Pro*C para o ECPG

Criado por Sai Parthasaradhi (AWS) e Mahesh Balumuri (AWS)

Resumo

A maioria dos aplicativos legados que têm código SQL incorporado usa o pré-compilador do Oracle Pro*C para acessar o banco de dados. Ao migrar esses bancos de dados do Oracle para o Amazon Relational Database Service (Amazon RDS) para PostgreSQL ou Amazon Aurora Edição Compatível com PostgreSQL, você precisa converter o código do aplicativo em um formato compatível com o pré-compilador no PostgreSQL, chamado ECPG. Esse padrão descreve como converter o código do Oracle Pro*C em seu equivalente no PostgreSQL ECPG.

Para obter mais informações sobre o Pro*C, consulte a documentação do Oracle. Para obter uma breve introdução ao ECPG, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados compatível com Amazon RDS para PostgreSQL ou Aurora compatível com PostgreSQL
- Um banco de dados do Oracle em execução on-premises

Ferramentas

- Os pacotes do PostgreSQL listados na seção seguinte.
- AWS CLI: o AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto para interagir com serviços da AWS por meio de comandos em seu shell de linha de comando. Com configuração mínima, você pode executar comandos da AWS CLI que implementam funcionalidade equivalente àquela fornecida pelo Console de Gerenciamento da AWS baseado em navegador a partir de um prompt de comando.

Épicos

Defina o ambiente de construção no CentOS ou RHEL

Tarefa	Descrição	Habilidades necessárias

Instale pacotes do PostgreSQL.	Instale os pacotes PostgreSQL necessários usando os comandos a seguir.
	`yum update -y`
	`yum install -y yum-utils`
	`rpm -ivh https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm`
	`dnf -qy module disable postgresql`
		Desenvolvedor de aplicativos, DevOps engenheiro

Instale os arquivos de cabeçalho e as bibliotecas.	Instale o pacote `postgresql12-devel`, que contém arquivos de cabeçalho e bibliotecas, usando os comandos a seguir. Instale o pacote nos ambientes de desenvolvimento e de runtime para evitar erros no ambiente de execução.
	`dnf -y install postgresql12-devel`
	`yum install ncompress zip ghostscript jq unzip wget git -y`
		Desenvolvedor de aplicativos, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	Somente para o ambiente de desenvolvimento, execute também os comandos a seguir.
	`yum install zlib-devel make -y`
	`ln -s /usr/pgsql-12/bin/ecpg /usr/bin/`	

Configure a variável do caminho do ambiente.	Defina o caminho do ambiente para as bibliotecas de cliente do PostgreSQL. `export PATH=$PATH:/usr/pgsql-12/bin`	Desenvolvedor de aplicativos, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Instale software adicional conforme necessário.	Se necessário, instale o pgLoader como substituto do SQL*Loader no Oracle.
	`wget -O /etc/yum.repos.d/pgloader-ccl.repo https://dl.packager.io/srv/opf/pgloader-ccl/master/installer/el/7.repo`
	`yum install pgloader-ccl -y`
	`ln -s /opt/pgloader-ccl/bin/pgloader /usr/bin/`
	Se você estiver chamando qualquer aplicativo Java dos módulos Pro*C, instale o Java.
	`yum install java -y`
	Instale o ant para compilar o código Java.
	`yum install ant -y`
		Desenvolvedor de aplicativos, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Instale a AWS CLI.	Instale a AWS CLI para executar comandos para interagir com os Serviços da AWS, como o AWS Secrets Manager e o Amazon Simple Storage Service (Amazon S3) a partir de seus aplicativos.
	`cd /tmp/`
	`curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`./aws/install -i /usr/local/aws-cli -b /usr/local/bin --update`
		Desenvolvedor de aplicativos, DevOps engenheiro

Identifique os programas a serem convertidos.	Identifique os aplicativos que você deseja converter do Pro*C para ECPG.	Desenvolvedor do aplicativo, proprietário do aplicativo

Converta o código Pro*C para ECPG

Tarefa	Descrição	Habilidades necessárias
Remova os cabeçalhos indesejados.	Remova os cabeçalhos `include` que não são necessários no PostgreSQL, como `oci.h`, `oratypes` e `sqlda`.	Proprietário do aplicativo, desenvolvedor do aplicativo
Atualize as declarações de variáveis.	Adicione instruções `EXEC SQL` para todas as declaraçõ	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	es de variáveis usadas como variáveis do host. Remova as declarações `EXEC SQL VAR`, como as seguintes, do seu aplicativo. `EXEC SQL VAR query IS STRING(2048);`	

Tarefa	Descrição	Habilidades necessárias

Atualize a funcionalidade ROWNUM.	A função ROWNUM não está disponível no PostgreSQL. Substitua isso pela função de janela ROW_NUMBER nas consultas SQL.
	
	Código Pro*C:
	
	`SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME FROM DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2 WHERE ROWNUM <=1 ORDER BY ROWNUM;`
	
	Código ECPG:
	
	`SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME , ROW_NUMBE R() OVER (ORDER BY FILE_NAME DESC) AS ROWNUM FROM demo_sche ma.DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2`
		Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	`WHERE ROWNUM <=1 ORDER BY ROWNUM;`	

Atualize os parâmetros da função para usar variáveis de alias.	No PostgreSQL, os parâmetros da função não podem ser usados como variáveis do host. Substitua-os usando uma variável de alias.
	
	Código Pro*C:
	
	`int processData(int referenceId){ EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
	
	Código ECPG:
	
	`int processData(int referenceIdParam){ EXEC SQL int referenceId = referenceIdParam; EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
		Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Atualize os tipos de estrutura.	Defina os tipos `struct` em `EXEC SQL BEGIN` e blocos `END` com `typedef` se as variáveis de tipo `struct` forem usadas como variáveis de host. Se os tipos `struct` forem definidos em arquivos header (`.h`), inclua os arquivos com instruções include (incluir) `EXEC SQL`. Código Pro*C: Arquivo de cabeçalho (`demo.h`) `struct s_partiti on_ranges { char sc_table_ group[31]; char sc_table_ name[31]; char sc_range_ value[10]; }; struct s_partiti on_ranges_ind { short ss_table_ group; short ss_table_ name; short ss_range_ value; };` Código ECPG:	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias

	Arquivo de cabeçalho (`demo.h`)
	
	`EXEC SQL BEGIN DECLARE SECTION;`
	`typedef struct`
	`{`
	`  char  sc_table_group[31];`
	`  char  sc_table_name[31];`
	`  char  sc_range_value[10];`
	`} s_partition_ranges;`
	`typedef struct`
	`{`
	`  short  ss_table_group;`
	`  short  ss_table_name;`
	`  short  ss_range_value;`
	`} s_partition_ranges_ind;`
	`EXEC SQL END DECLARE SECTION;`
	
	Arquivo Pro*C (`demo.pc`)
	
	`#include "demo.h"`
	`struct s_partition_ranges gc_partition_data[MAX_PART_TABLE] ;`
	`struct s_partition_ranges_ind gc_partition_data_ind[MAX_PART_TABLE] ;`
	
	Arquivo ECPG (`demo.pc`)	

Tarefa	Descrição	Habilidades necessárias
	`exec sql include "demo.h" EXEC SQL BEGIN DECLARE SECTION; s_partition_ranges gc_partition_data[ MAX_PART_TABLE] ; s_partition_ranges_ind gc_partition_data_ ind[MAX_PART_TABLE] ; EXEC SQL END DECLARE SECTION;`	

Modifique a lógica para fazer buscas nos cursores.	Para buscar várias linhas nos cursores usando variáveis de matriz, altere o código a ser usado `FETCH FORWARD`.
	
	Código Pro*C:
	
	`EXEC SQL char aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL FETCH filename_ cursor into :aPoeFile s;`
	
	Código ECPG:
	
	`EXEC SQL char aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL int fetchSize = MAX_FILES; EXEC SQL FETCH FORWARD :fetchSiz e filename_cursor into :aPoeFiles;`
		Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias

Modifique as chamadas de pacotes que não têm valores de retorno.	As funções do pacote Oracle que não têm valores de retorno devem ser chamadas com uma variável indicador a. Se seu aplicativo incluir várias funções com o mesmo nome ou se as funções de tipo desconhecido gerarem erros de runtime, converta os valores para os tipos de dados.
	
	Código Pro*C:
	
	`void ProcessData (char *data , int id) { EXEC SQL EXECUTE BEGIN pkg_demo. process_data (:data, :id); END; END-EXEC; }`
	
	Código ECPG:
	
	`void ProcessData (char *dataParam, int idParam ) { EXEC SQL char *data = dataParam;`
		Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias

	`EXEC SQL int id = idParam;`
	`EXEC SQL short rowInd;`
	`EXEC SQL short rowInd = 0;`
	`EXEC SQL SELECT pkg_demo.process_data (`
	`inp_data => :data::text,`
	`inp_id => :id )`
	`INTO :rowInd;`
	`}`	

Tarefa	Descrição	Habilidades necessárias

Reescreva as variáveis SQL_CURSOR.	Reescreva a variável `SQL_CURSOR` e sua implementação.
	
	Código Pro*C:
	
	`/* SQL Cursor */`
	`SQL_CU`
	`RSOR demo_cursor;`
	`EXEC SQL`
	` ALLOCATE :demo_cursor;`
	`EXEC SQL EXECUTE`
	`  BEGIN`
	`  pkg_demo.`
	`get_cursor(`
	`  demo_cur=`
	`>:demo_cursor`
	`  );`
	`  END;`
	`END-EXEC;`
	
	Código ECPG:
	
	`EXEC SQL DECLARE`
	` demo_cursor CURSOR FOR`
	` SELECT`
	`  * from`
	`  pkg_demo.open_file`
	`name_rc(`
	`  demo_cur=`
	`>refcursor`
	`  ) ;`
	`EXEC SQL char open_file`
	`name_rcInd[100];`
	`# As the below function`
	` returns cursor_name`
	` as`
	`# return we need to`
	` use char[] type as`
	` indicator.`
		Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	`EXEC SQL SELECT pkg_demo.get_cursor ( demo_cur= >'demo_cursor' ) INTO :open_filename_rcInd;`	
Aplique padrões comuns de migração.	• Altere as consultas SQL para que sejam compatíveis com o PostgreSQL. • Mova blocos anônimos para o banco de dados quando não houver suporte no ECPG. • Remova a lógica `dbms_application_info` , que não é compatível com o PostgreSQL. • Mova as instruções `EXEC SQL COMMIT` após o fechamento do cursor. Se você confirmar consultas enquanto estiver no loop para buscar os registros do cursor, o cursor será fechado e um erro de cursor não existe será exibido. • Para obter informações sobre como lidar com exceções no ECPG e códigos de erro, consulte Tratamento de erros na documentação do PostgreSQL.	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Ative a depuração, se necessário.	Para executar o programa ECPG no modo de depuração , adicione o seguinte comando dentro do bloco de funções principal. `ECPGdebug(1, stderr);`	Desenvolvedor do aplicativo, proprietário do aplicativo

Compile programas ECPG

Tarefa	Descrição	Habilidades necessárias

Crie um arquivo executável para o ECPG.	Se você tiver um arquivo de origem SQL C incorporado chamado `prog1.pgc` , poderá criar um programa executável usando a seguinte sequência de comandos.
	`ecpg prog1.pgc`
	`cc -I/usr/local/pgsql/include -c prog1.c`
	`cc -o prog1 prog1.o -L/usr/local/pgsql/lib -lecpg`
		Desenvolvedor do aplicativo, proprietário do aplicativo

Crie um arquivo make para compilação.	Criar um arquivo make para compilar o programa ECPG, conforme mostrado no arquivo de exemplo a seguir. `CFLAGS ::= $(CFLAGS) -I/usr/pgsql-12/include -g -Wall`	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias

	`LDFLAGS ::= $(LDFLAGS) -L/usr/pgsql-12/lib -Wl,-rpath,/usr/pgsql-12/lib`
	`LDLIBS ::= $(LDLIBS) -lecpg`
	`PROGRAMS = test`
	`.PHONY: all clean`
	`%.c: %.pgc`
	`ecpg $<`
	`all: $(PROGRAMS)`
	`clean:`
	`rm -f $(PROGRAMS) $(PROGRAMS:%=%.c) $(PROGRAMS:%=%.o)`	

Teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Teste o código.	Teste o código do aplicativo convertido para verificar se ele funciona corretamente.	Desenvolvedor de aplicativos, proprietário do aplicativo, engenheiro de teste

Recursos relacionados

- ECPG: SQL incorporado em C (documentação do PostgreSQL)
- Tratamento de erros (documentação do PostgreSQL)
- Por que usar o pré-compilador do Oracle Pro*C/C++ (documentação do Oracle)

Mais informações

O PostgreSQL tem um pré-compilador SQL incorporado, o ECPG, que é equivalente ao pré-compilador do Oracle Pro*C. O ECPG converte programas C que têm instruções SQL incorporadas em código C padrão, substituindo as chamadas SQL por chamadas de funções especiais. Os

arquivos de saída podem então ser processados com qualquer cadeia de ferramentas do compilador C.

Arquivos de entrada e saída

O ECPG converte cada arquivo de entrada especificado na linha de comando no arquivo de saída C correspondente. Se um nome de arquivo de entrada não tiver uma extensão de arquivo, será assumido o formato .pgc. A extensão do arquivo é substituída por `.c` para estruturar o nome do arquivo de saída. No entanto, você pode substituir o nome padrão do arquivo de saída usando a opção `-o`.

Se você usar um traço (`-`) como nome do arquivo de entrada, o ECPG lerá o programa da entrada padrão e gravará na saída padrão, a menos que você substitua isso usando a opção `-o`.

Arquivos de cabeçalho

Quando o compilador do PostgreSQL compila os arquivos de código C pré-processados, ele procura os arquivos de cabeçalho ECPG no diretório `include` do PostgreSQL. Portanto, talvez seja necessário usar a opção `-I` de apontar o compilador para o diretório correto (por exemplo,`-I/usr/local/pgsql/include`).

Bibliotecas

Os programas que usam código C com SQL incorporado precisam ser vinculados à biblioteca `libecpg`. Por exemplo, você pode usar as opções `-L/usr/local/pgsql/lib -lecpg` do vinculador.

Os aplicativos ECPG convertidos chamam funções na biblioteca `libpq` por meio da biblioteca SQL incorporada (`ecpglib`) e se comunicam com o servidor do PostgreSQL usando o protocolo padrão de frontend/backend.

Migre colunas geradas virtualmente do Oracle para o PostgreSQL

Criado por Veeranjaneyulu Grandhi (AWS), Rajesh Madiwale (AWS) e Ramesh Pathuri (AWS)

Resumo

Na versão 11 e nas anteriores, o PostgreSQL não fornece um atributo que seja diretamente equivalente a uma coluna virtual Oracle. Lidar com colunas geradas virtualmente durante a migração do banco de dados Oracle para o PostgreSQL versão 11 ou anterior é difícil por dois motivos:

- As colunas virtuais não são visíveis durante a migração.
- O PostgreSQL não suporta a expressão `generate` em versões anteriores à versão 12.

No entanto, existem soluções alternativas para emular funcionalidades semelhantes. Ao usar o AWS Database Migration Service (AWS DMS) para migrar dados do banco de dados do Oracle para PostgreSQL versão 11 ou anterior, você pode usar funções de gatilho para preencher os valores em colunas geradas virtualmente. Esse padrão fornece exemplos do banco de dados Oracle e do código PostgreSQL que você pode usar para essa finalidade. Na AWS, você pode usar o Amazon Relational Database Service (Amazon RDS) para PostgreSQL ou Amazon Aurora Edição Compatível com PostgreSQL para o seu banco de dados PostgreSQL.

A partir da versão 12 do PostgreSQL, as colunas geradas são suportadas. As colunas geradas podem ser calculadas a partir de outros valores de coluna em tempo real ou calculadas e armazenadas. As colunas geradas do PostgreSQL são semelhantes às colunas virtuais do Oracle.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle de origem
- Bancos de dados PostgreSQL de destino (no Amazon RDS para PostgreSQL ou Aurora compatível com PostgreSQL)
- Experiência em codificação PL/pgSQL

Limitações

- Aplica-se somente às versões do PostgreSQL anteriores à versão 12.

- Aplica-se ao Oracle Database versão 11g ou superior.
- As colunas virtuais não são suportadas nas ferramentas de migração de dados.
- Aplica-se somente às colunas definidas na mesma tabela.
- Se uma coluna virtual gerada se referir a uma função determinística definida pelo usuário, ela não poderá ser usada como uma coluna principal de particionamento.
- A saída da expressão deve ser um valor escalar. Ele não pode retornar um tipo de dados fornecido pelo Oracle, um tipo definido pelo usuário, `LOB` ou `LONG RAW`.
- Os índices definidos em colunas virtuais são equivalentes aos índices baseados em funções no PostgreSQL.
- As estatísticas da tabela devem ser coletadas.

Ferramentas

- O pgAdmin 4 é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Essa ferramenta fornece uma interface gráfica que simplifica a criação, manutenção e uso de objetos de banco de dados.
- O Oracle SQL Developer é um ambiente de desenvolvimento gratuito e integrado para trabalhar com SQL em bancos de dados Oracle em implantações tradicionais e em nuvem.

Épicos

Crie tabelas de banco de dados de origem e destino

Tarefa	Descrição	Habilidades necessárias
Crie uma tabela de origem do Oracle Database.	No Oracle Database, crie uma tabela com colunas geradas virtuais usando a instrução a seguir. `CREATE TABLE test.generated_column ( CODE NUMBER, STATUS VARCHAR2(12) DEFAULT 'PreOpen', FLAG CHAR(1) GENERATED ALWAYS AS (CASE`	DBA, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`UPPER(STATUS) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) VIRTUAL VISIBLE );` Nessa tabela de origem, os dados na coluna `STATUS` são migrados pelo AWS DMS para o banco de dados de destino. No entanto, a coluna `FLAG` é preenchida usando a funcionalidade `generate by`, portanto, essa coluna não fica visível para o AWS DMS durante a migração. Para implementar a funcionalidade de `generated by`, você deve usar gatilhos e funções no banco de dados de destino para preencher os valores na coluna `FLAG`, conforme mostrado no próximo épico.	

Tarefa	Descrição	Habilidades necessárias
Crie uma tabela PostgreSQL de destino na AWS.	Crie uma tabela PostgreSQL na AWS usando a instrução a seguir. `CREATE TABLE test.generated_column ( code integer not null, status character varying(12) not null , flag character(1) );` Nessa tabela, a coluna `status` é uma coluna padrão. A coluna `flag` será uma coluna gerada com base nos dados da coluna `status`.	DBA, desenvolvedor de aplicativos

Crie uma função de gatilho para lidar com a coluna virtual no PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Crie um gatilho do PostgreSQL.	No PostgreSQL, crie um gatilho. `CREATE TRIGGER tgr_gen_column AFTER INSERT OR UPDATE OF status ON test.generated_column FOR EACH ROW EXECUTE FUNCTION test.tgf_gen_column();`	DBA, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Crie uma função de gatilho do PostgreSQL.	No PostgreSQL, crie uma função para o gatilho. Essa função preenche uma coluna virtual que é inserida ou atualizada pelo aplicativo ou pelo AWS DMS e valida os dados. `CREATE OR REPLACE FUNCTION test.tgf_gen_column() RETURNS trigger AS $VIRTUAL_COL$ BEGIN IF (TG_OP = 'INSERT') THEN IF (NEW.flag IS NOT NULL) THEN RAISE EXCEPTION 'ERROR: cannot insert into column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF (TG_OP = 'UPDATE') THEN IF (NEW.flag::VARCHAR != OLD.flag::varchar) THEN RAISE EXCEPTION 'ERROR: cannot update column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF TG_OP IN ('INSERT','UPDATE') THEN`	DBA, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`IF (old.flag is NULL) OR (coalesce(old.status,'') != coalesce(new.status,'')) THEN UPDATE test.generated_column SET flag = (CASE UPPER(status) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) WHERE code = new.code; END IF; END IF; RETURN NEW; END $VIRTUAL_COL$ LANGUAGE plpgsql;`	

Teste a migração de dados usando o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de replicação.	Para criar uma instância de replicação, siga as instruções na documentação do AWS DMS. A instância de replicação deve estar na mesma nuvem privada virtual (VPC) que os bancos de dados de origem e de destino.	DBA, desenvolvedor de aplicativos
Criar endpoints de origem e de destino.	Para criar endpoints, siga as instruções na documentação do AWS DMS.	DBA, desenvolvedor de aplicativos
Testar as conexões do endpoint.	Você pode testar as conexões do endpoint especificando a	DBA, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	VPC e a instância de replicaçã o e escolhendo Executar teste.	
Crie e inicie uma tarefa de carga completa.	Para obter instruções, consulte Criação de uma tarefa e Configurações de tarefa de carga completa na documentação do AWS DMS.	DBA, desenvolvedor de aplicativos
Valide os dados da coluna virtual.	Compare os dados na coluna virtual nos bancos de dados de origem e de destino. Você pode validar os dados manualmente ou escrever um script para essa etapa.	DBA, desenvolvedor de aplicativos

Recursos relacionados

- Introdução ao AWS Database Migration Service (documentação do AWS DMS)
- Uso de um banco de dados Oracle como origem para o AWS DMS (documentação do AWS DMS)
- Uso de um banco de dados PostgreSQL como destino para o AWS DMS (documentação do AWS DMS)
- Colunas geradas no PostgreSQL (documentação do PostgreSQL)
- Funções de gatilho (documentação do PostgreSQL)
- Colunas virtuais no banco de dados Oracle (documentação do Oracle)

Configure a funcionalidade Oracle UTL_FILE no Aurora compatível com PostgreSQL

Criado por Rakesh Raghav (AWS) e anuradha chintha (AWS)

Resumo

Como parte de sua jornada de migração da Oracle para Amazon Aurora Edição Compatível com PostgreSQL na nuvem da Amazon Web Services (AWS), você pode encontrar vários desafios. Por exemplo, migrar código que depende do utilitário `UTL_FILE` do Oracle é sempre um desafio. No Oracle PL/SQL, o pacote `UTL_FILE` é usado para operações de arquivo, como leitura e gravação, em conjunto com o sistema operacional subjacente. O utilitário `UTL_FILE` funciona tanto para sistemas de servidores quanto para máquinas clientes.

O Amazon Aurora compatível com PostgreSQL é uma oferta de banco de dados gerenciado. Por causa disso, não é possível acessar arquivos no servidor do banco de dados. Esse padrão orienta você na integração do Amazon Simple Storage Service (Amazon S3) e o Amazon Aurora compatível com PostgreSQL para obter um subconjunto da funcionalidade `UTL_FILE`. Usando essa integração, podemos criar e consumir arquivos sem usar ferramentas ou serviços de extração, transformação e carregamento (ETL) de terceiros.

Opcionalmente, você pode configurar o CloudWatch monitoramento da Amazon e as notificações do Amazon SNS.

Recomendamos testar minuciosamente essa solução antes de implementá-la em um ambiente de produção.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Database Migration Service (AWS DMS)
- Experiência em codificação PL/pgSQL
- Um cluster Amazon Aurora compatível com PostgreSQL
- Um bucket do S3

Limitações

Esse padrão não fornece a funcionalidade para atuar como um substituto para o utilitário `UTL_FILE` do Oracle. No entanto, as etapas e o código de amostra podem ser aprimorados ainda mais para atingir suas metas de modernização do banco de dados.

Versões do produto

- Amazon Aurora compatível com PostgreSQL Edição 11.9

Arquitetura

Pilha de tecnologias de destino

- Amazon Aurora compatível com PostgreSQL
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon S3

Arquitetura de destino

O diagrama a seguir mostra uma representação de alto nível da solução.

1. Os arquivos são enviados do aplicativo para o bucket do S3.
2. A extensão `aws_s3` acessa os dados, usando PL/pgSQL, e carrega os dados para o Aurora compatível com PostgreSQL.

Ferramentas

- Amazon Aurora compatível com PostgreSQL: Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado, compatível com PostgreSQL e compatível com ACID. Ele combina a velocidade e a confiabilidade dos bancos de dados comerciais de ponta com a relação custo-benefício dos bancos de dados de código aberto.
- AWS CLI: o AWS Command Line Interface (AWS CLI) é uma ferramenta unificada para gerenciar os serviços da AWS. Com apenas uma ferramenta para fazer o download e configurar, você poderá controlar vários serviços da AWS pela linha de comando e automatizá-los usando scripts.
- Amazon CloudWatch — A Amazon CloudWatch monitora os recursos e o uso do Amazon S3.

- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet. Nesse padrão, o Amazon S3 fornece uma camada de armazenamento para receber e armazenar arquivos para consumo e transmissão de e para o cluster compatível com o Aurora PostgreSQL.
- aws_s3: a extensão `aws_s3` integra o Amazon S3 e o Aurora compatível com PostgreSQL.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) coordena e gerencia a entrega ou envio de mensagens entre publicadores e clientes. Nesse padrão, o Amazon SNS é usado para enviar notificações.
- pgAdmin: o pgAdmin é uma ferramenta de gerenciamento de código aberto para o Postgres. O pgAdmin 4 fornece uma interface gráfica para criar, manter e usar objetos de banco de dados.

Código

Para obter a funcionalidade necessária, o padrão cria várias funções com nomenclatura semelhante a `UTL_FILE`. A seção Informações adicionais contém a base de código para essas funções.

No código, substitua `testaurorabucket` pelo nome do bucket do S3 de teste. Substitua `us-east-1` pela região da AWS em que está localizado o bucket do S3 de teste.

Épicos

Integre o Amazon S3 e o Aurora compatível com PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Configurar políticas do IAM.	Crie políticas do AWS Identity and Access Management (IAM) que concedam acesso ao bucket S3 e aos objetos nele contidos. Para obter o código, consulte a seção Informações adicionais.	Administrador da AWS, DBA
Adicione perfis de acesso do Amazon S3 ao Aurora PostgreSQL.	Crie dois perfis do IAM: um para leitura e outro para acesso de gravação ao Amazon S3. Anexe os dois	Administrador da AWS, DBA

Tarefa	Descrição	Habilidades necessárias
	perfis ao cluster compatível com o Aurora PostgreSQL: • Um perfil para o atributo S3Export • Um perfil para o atributo S3Import Para obter mais informaçõ es, consulte a documentação do Aurora compatível com PostgreSQL sobre importação e exportação de dados para o Amazon S3.	

Configure as extensões no Aurora compatível com PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Crie a extensão aws_commo ns.	A extensão `aws_commons` é uma dependência da extensão `aws_s3`.	DBA, Desenvolvedor
Crie a extensão aws_s3.	A extensão `aws_s3` interage com o Amazon S3.	DBA, Desenvolvedor

Valide a integração do Amazon S3 e do Aurora compatível com PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Teste a importação de arquivos do Amazon S3 para o Aurora PostgreSQL.	Para testar a importação de arquivos para o Aurora compatível com PostgreSQ L, crie um arquivo CSV de	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	amostra e carregue-o no bucket do S3. Crie uma definição de tabela com base no arquivo CSV e carregue o arquivo na tabela usando a função `aws_s3.table_import_from_s3` .	
Teste a exportação de arquivos do Aurora PostgreSQL para o Amazon S3.	Para testar a exportação de arquivos do Aurora compatível com PostgreSQL, crie uma tabela de teste, preencha-a com dados e, em seguida, exporte os dados usando a função `aws_s3.query_export_to_s3` .	DBA, Desenvolvedor

Para imitar o utilitário UTL_FILE, crie funções de encapsulamento

Tarefa	Descrição	Habilidades necessárias
Crie o esquema utl_file_utility.	O esquema mantém as funções de encapsulamento juntas. Para criar o esquema, execute o seguinte comando. `CREATE SCHEMA utl_file_utility;`	DBA, Desenvolvedor
Crie o tipo file_type.	Para criar o tipo `file_type` , use o código a seguir. `CREATE TYPE utl_file_utility.file_type AS (`	DBA/Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`p_path character varying(30), p_file_name character varying );`	
Crie a função init.	A função `init` inicializa uma variável comum, como `bucket` ou `region`. Para obter o código, consulte a seção Informações adicionais.	DBA/Desenvolvedor
Crie as funções de encapsulamento.	Crie as funções de encapsulamento `fopen`, `put_line` e `fclose`. Para obter o código, consulte a seção Informações adicionais.	DBA, Desenvolvedor

Teste as funções de encapsulamento

Tarefa	Descrição	Habilidades necessárias
Teste as funções de encapsulamento no modo de gravação.	Para testar as funções de encapsulamento no modo de gravação, use o código fornecido na seção Informações adicionais.	DBA, Desenvolvedor
Teste as funções de encapsulamento no modo de acréscimo.	Para testar as funções de encapsulamento no modo de acréscimo, use o código fornecido na seção Informações adicionais.	DBA, Desenvolvedor

Recursos relacionados

- Integração do Amazon S3
- Amazon S3
- Aurora
- Amazon CloudWatch
- Amazon SNS

Mais informações

Configurar políticas do IAM

Crie as políticas a seguir.

Nome da política	JSON
S3 IntRead	`{ "Version": "2012-10-17", "Statement": [ { "Sid": "S3integrationtest", "Effect": "Allow", "Action": [ "s3:GetObject", "s3:ListBucket" ], "Resource": [ "arn:aws:s3:::testaurorabucket/*", "arn:aws:s3:::testaurorabucket" ] } ] }`
S3 IntWrite	`{ "Version": "2012-10-17",`

```
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",

                "s3:ListBucket"
            ],
            "Resource": [
    "arn:aws:s3:::testaurorabucket/
*",                "arn:aws:s3:::test
aurorabucket"
            ]
        }
    ]
}
```

Crie a função init

Para inicializar variáveis comuns, como `bucket` ou `region`, crie a função `init` usando o código a seguir.

```
CREATE OR REPLACE FUNCTION utl_file_utility.init(
    )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
BEGIN
      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 'region' )
      , 'us-east-1'::text
      , false );

      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 's3bucket' )
      , 'testaurorabucket'::text
      , false );
```

```
END;
$BODY$;
```

Criar as funções de encapsulamento

Crie as funções `fopen`, `put_line` e `fclose` de encapsulamento

fopen

```
CREATE OR REPLACE FUNCTION utl_file_utility.fopen(
    p_file_name character varying,
    p_path character varying,
    p_mode character DEFAULT 'W'::bpchar,
    OUT p_file_type utl_file_utility.file_type)
    RETURNS utl_file_utility.file_type
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
declare
    v_sql character varying;
    v_cnt_stat integer;
    v_cnt integer;
    v_tabname character varying;
    v_filewithpath character varying;
    v_region character varying;
    v_bucket character varying;

BEGIN
    /*initialize common variable */
    PERFORM utl_file_utility.init();
    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    /* set tabname*/
    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;
    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region;
```

```
   /* APPEND MODE HANDLING; RETURN EXISTING FILE DETAILS IF PRESENT ELSE CREATE AN
EMPTY FILE */
   IF p_mode = 'A' THEN
       v_sql := concat_ws('','create temp table if not exists ', v_tabname,' (col1
text)');
       execute v_sql;

       begin
       PERFORM aws_s3.table_import_from_s3
           ( v_tabname,
           '',
           'DELIMITER AS ''#''',
           aws_commons.create_s3_uri
           (     v_bucket,
               v_filewithpath ,
               v_region)
           );
       exception
           when others then
            raise notice 'File load issue ,%',sqlerrm;
            raise;
       end;
       execute concat_ws('','select count(*) from ',v_tabname) into v_cnt;

       IF v_cnt > 0
       then
           p_file_type.p_path := p_path;
           p_file_type.p_file_name := p_file_name;
       else
           PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
v_region)
                             );

           p_file_type.p_path := p_path;
           p_file_type.p_file_name := p_file_name;
       end if;
       v_sql := concat_ws('','drop table ', v_tabname);
       execute v_sql;
   ELSEIF p_mode = 'W' THEN
           PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
v_region)
                             );
```

```
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
    END IF;

EXCEPTION
        when others then
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
            raise notice 'fopenerror,%',sqlerrm;
            raise;
END;
$BODY$;
```

put_line

```
CREATE OR REPLACE FUNCTION utl_file_utility.put_line(
    p_file_name character varying,
    p_path character varying,
    p_line text,
    p_flag character DEFAULT 'W'::bpchar)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
/*****************************************************************************
* Write line, p_line in windows format to file, p_fp - with carriage return
* added before new line.
*****************************************************************************/
declare
    v_sql varchar;
    v_ins_sql varchar;
    v_cnt INTEGER;
    v_filewithpath character varying;
    v_tabname  character varying;
    v_bucket character varying;
    v_region character varying;

BEGIN
 PERFORM utl_file_utility.init();

/* check if temp table already exist */
```

```
 v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );

 v_sql := concat_ws('','select count(1) FROM pg_catalog.pg_class c LEFT JOIN
 pg_catalog.pg_namespace n ON n.oid = c.relnamespace where n.nspname like ''pg_temp_
%'''
                        ,' AND pg_catalog.pg_table_is_visible(c.oid) AND
 Upper(relname) = Upper( '''
                        ,  v_tabname ,''' ) ');

 execute v_sql into v_cnt;

  IF v_cnt = 0 THEN
         v_sql := concat_ws('','create temp table ',v_tabname,' (col text)');
        execute v_sql;
        /* CHECK IF APPEND MODE */
        IF upper(p_flag) = 'A' THEN
            PERFORM utl_file_utility.init();
            v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 'region' ) );
            v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 's3bucket' ) );

            /* set tabname*/
            v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

            begin
               PERFORM aws_s3.table_import_from_s3
                     ( v_tabname,
                          '',
                       'DELIMITER AS ''#''',
                        aws_commons.create_s3_uri
                           ( v_bucket,
                               v_filewithpath,
                               v_region    )
                    );
            exception
                when others then
                    raise notice  'Error Message : %',sqlerrm;
                    raise;
            end;
        END IF;
```

```
    END IF;
    /* INSERT INTO TEMP TABLE */
    v_ins_sql := concat_ws('','insert into ',v_tabname,' values(''',p_line,''')');
    execute v_ins_sql;
    RETURN TRUE;
    exception
            when others then
                raise notice  'Error Message : %',sqlerrm;
                raise;
END;
$BODY$;
```

fclose

```
CREATE OR REPLACE FUNCTION utl_file_utility.fclose(
    p_file_name character varying,
    p_path character varying)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
DECLARE
    v_filewithpath character varying;
    v_bucket character varying;
    v_region character varying;
    v_tabname character varying;
    v_sql character varying;
BEGIN
      PERFORM utl_file_utility.init();

    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region ;
```

```
    /* exporting to s3 */
    perform aws_s3.query_export_to_s3
        (concat_ws('','select * from ',v_tabname,'  order by ctid asc'),
            aws_commons.create_s3_uri(v_bucket, v_filewithpath, v_region)
        );
    v_sql := concat_ws('','drop table ', v_tabname);
    execute v_sql;
    RETURN TRUE;
EXCEPTION
       when others then
     raise notice 'error fclose %',sqlerrm;
     RAISE;
END;
$BODY$;
```

Teste suas funções de configuração e encapsulamento

Use os seguintes blocos de código anônimo para testar sua configuração.

Teste o modo de gravação

O código a seguir grava um arquivo chamado `s3inttest` no bucket do S3.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'W';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;
```

```
end;
$$
```

Teste o modo de acréscimo

O código a seguir acrescenta linhas ao arquivo `s3inttest` que foi criado no teste anterior.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'A';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;


select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose : append 1', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket : for
 test purpose : append 2', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Notificações do Amazon SNS

Opcionalmente, você pode configurar o CloudWatch monitoramento da Amazon e as notificações do Amazon SNS no bucket do S3. Para obter mais informações, consulte Monitoramento do Amazon S3 e Configuração das notificações do Amazon SNS.

Valide objetos de banco de dados após migrar do Oracle para o Amazon Aurora PostgreSQL

Criado por Venkatramana Chintha (AWS) e Eduardo Valentim (AWS)

Resumo

Esse padrão descreve uma step-by-step abordagem para validar objetos após a migração de um banco de dados Oracle para a edição compatível com o Amazon Aurora PostgreSQL.

Este padrão descreve cenários de uso e etapas para validação de objetos de banco de dados; para informações mais detalhadas, consulte Validar objetos de banco de dados após a migração usando o AWS SCT e o AWS DMS no blog do AWS Database.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle on-premises que foi migrado para um banco de dados Aurora compatível com PostgreSQL.
- Credenciais de login com a RDSData FullAccess política da Amazon aplicada para o banco de dados compatível com o Aurora PostgreSQL.
- Este padrão usa o editor de consultas para clusters de banco de dados do Aurora Serverless, que está disponível no console do Amazon Relational Database Service (Amazon RDS). No entanto, você pode usar esse padrão com qualquer outro editor de consultas.

Limitações

- Os objetos SYNONYM do Oracle não estão disponíveis no PostgreSQL, mas podem ser parcialmente validados por meio de visualizações ou consultas SET search_path.
- O editor de consultas do Amazon RDS está disponível somente em determinadas regiões da AWS e para determinadas versões do MySQL e do PostgreSQL.

Arquitetura

Ferramentas

Ferramentas

- Amazon Aurora Edição Compatível com PostgreSQL: o Aurora compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado, compatível com o PostgreSQL e em conformidade com ACID, que combina a velocidade e a confiabilidade de bancos de dados comerciais de ponta com a simplicidade e a economia de bancos de dados de código aberto.
- Amazon RDS: o Amazon Relational Database Service (Amazon RDS) facilita a configuração, a operação e escalabilidade de um banco de dados relacional na Nuvem AWS. Ele fornece capacidade econômica e redimensionável para um banco de dados relacional padrão do setor e gerencia tarefas comuns de administração de banco de dados.
- Editor de consultas para Aurora Serverless: o editor de consultas ajuda você a executar consultas SQL no console do Amazon RDS. Execute qualquer instrução SQL válida no cluster de banco de dados do Aurora Serverless, inclusive instruções de manipulação e definição de dados.

Para validar os objetos, use os scripts completos no arquivo "Scripts de validação de objetos" na seção "Anexos". Use a tabela a seguir como referência.

Objeto Oracle	Script a ser usado
Pacotes	Consulta 1
Tabelas	Consulta 3
Visões	Consulta 5
Sequências	Consulta 7
Acionadores	Consulta 9
Chaves primárias	Consulta 11
Índices	Consulta 13
Restrições de verificação	Consulta 15
Chaves externas	Consulta 17

Objeto PostgreSQL	Script a ser usado
Pacotes	Consulta 2
Tabelas	Consulta 4
Visões	Consulta 6
Sequências	Consulta 8
Acionadores	Consulta 10
Chaves primárias	Consulta 12
Índices	Consulta 14
Restrições de verificação	Consulta 16
Chaves externas	Consulta 18

Épicos

Validar objetos no banco de dados Oracle de origem

Tarefa	Descrição	Habilidades necessárias
Execute a consulta de validação de “pacotes” no banco de dados Oracle de origem.	Baixe e abra o arquivo “Scripts de validação de objetos” na seção “Anexos”. Conecte-s e ao banco de dados Oracle de origem por meio de seu programa cliente. Execute o script de validação “Consulta 1” a partir do arquivo “Scripts de validação de objetos”. Importante: insira seu nome de usuário Oracle em vez de “your_schema” nas consultas.	Desenvolvedor, DBA

Tarefa	Descrição	Habilidades necessárias
	Certifique-se de registrar seus resultados da consulta.	
Execute a consulta de validação de “tabelas”.	Execute o script “Consulta 3” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação de “visões”.	Execute o script “Consulta 5” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a validação da contagem de “sequências”.	Execute o script “Consulta 7” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação “acionadores”.	Execute o script “Consulta 9” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação de “chaves primárias”.	Execute o script “Consulta 11” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA

Tarefa	Descrição	Habilidades necessárias
Execute a consulta de validação de “índices”.	Execute o script de validação “Consulta 13” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação de “restrições de verificação”.	Execute o script “Consulta 15” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação de “chaves externas”.	Execute o script de validação “Consulta 17” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA

Valide objetos no banco de dados Aurora de destino compatível com PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao banco de dados Aurora de destino compatível com PostgreSQL usando o editor de consultas.	Faça login no Console de Gerenciamento da AWS e abra o console do Amazon RDS. No canto superior direito, escolha a região da AWS em que o banco de dados Aurora compatível com PostgreSQL foi criado. No painel de navegação, escolha “Bancos de dados”, e escolha o banco de dados Aurora	Desenvolvedor, DBA

Tarefa	Descrição	Habilidades necessárias
	de destino compatível com o PostgreSQL. Em “Ações”, escolha “Consulta”. Importante: Caso ainda não tenha se conectado ao banco de dados, a página “Connect to database” (Conectar ao banco de dados) é aberta. Em seguida, você precisa inserir as informações do banco de dados, como nome de usuário e senha.	
Execute a consulta de validação de “pacotes”.	Execute o script “Consulta 2” a partir do arquivo “Scripts de validação de objetos” na seção “Anexos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação de “tabelas”.	Retorne ao editor de consultas do banco de dados Aurora compatível com PostgreSQL e execute o script “Consulta 4” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA

Tarefa	Descrição	Habilidades necessárias
Execute a consulta de validação de “visões”.	Retorne ao editor de consultas do banco de dados Aurora compatível com PostgreSQL e execute o script “Consulta 6” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a validação da contagem de “sequências”.	Retorne ao editor de consultas do banco de dados Aurora compatível com PostgreSQL e execute o script “Consulta 8” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação “acionadores”.	Retorne ao editor de consultas do banco de dados Aurora compatível com PostgreSQL e execute o script “Consulta 10” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação de “chaves primárias”.	Retorne ao editor de consultas do banco de dados Aurora compatível com PostgreSQL e execute o script “Consulta 12” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA

Tarefa	Descrição	Habilidades necessárias
Execute a consulta de validação de “índices”.	Retorne ao editor de consultas do banco de dados Aurora compatível com PostgreSQL e execute o script “Consulta 14” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação de “restrições de verificação”.	Execute o script “Consulta 16” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA
Execute a consulta de validação de “chaves externas”.	Execute o script de validação “Consulta 18” a partir do arquivo “Scripts de validação de objetos”. Certifique-se de registrar seus resultados da consulta.	Desenvolvedor, DBA

Compare os registros de validação do banco de dados de origem e destino

Tarefa	Descrição	Habilidades necessárias
Compare e valide ambos os resultados da consulta.	Compare os resultados da consulta dos bancos de dados Oracle e Aurora compatíveis com PostgreSQL para validar todos os objetos. Se todos corresponderem, todos os objetos foram validados com sucesso.	Desenvolvedor, DBA

Recursos relacionados

- Validar objetos de banco de dados após uma migração usando o AWS SCT e o AWS DMS
- Atributos do Amazon Aurora: Edição compatível com PostgreSQL

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Redefinir a hospedagem

Tópicos

- Acelere a descoberta e a migração de cargas de trabalho da Microsoft para a AWS
- Automatize as atividades de pré-ingestão de workload para o AWS Managed Services no Windows
- Crie um processo de aprovação para solicitações de firewall durante uma migração de rehospedagem para AWS
- Ingira e migre instâncias EC2 do Windows para uma conta do AWS Managed Services
- Migrar um banco de dados do Couchbase Server para a Amazon EC2
- Migre o Db2 for LUW para a Amazon EC2 usando o envio de registros para reduzir o tempo de interrupção
- Migre o Db2 for LUW para a Amazon EC2 com recuperação de desastres de alta disponibilidade
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2 usando o Application Migration Service
- Migre VMware VMs com o HCX Automation usando o PowerCLI
- Migre uma workload do F5 BIG-IP para o F5 BIG-IP VE na Nuvem AWS
- Migrar um aplicativo web do Go on-premises para AWS Elastic Beanstalk usando o método binário
- Migrar um servidor SFTP local para usar AWSAWS Transfer for SFTP
- Migre uma VM local para a Amazon EC2 usando o AWS Application Migration Service
- Migre pequenos conjuntos de dados on-premises para o Amazon S3 usando o AWS SFTP
- Migre da Oracle GlassFish para o AWS Elastic Beanstalk
- Migre um banco de dados Oracle local para o Oracle na Amazon EC2
- Migre um banco de dados Oracle local para a Amazon EC2 usando o Oracle Data Pump
- Migre sistemas RHEL BYOL para instâncias com licença incluída da AWS usando o AWS MGN
- Migre um banco de dados SAP ASE local para a Amazon EC2
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2
- Migre um banco de dados MySQL local para a Amazon EC2
- Reduza o tempo de substituição homogêneo da migração do SAP usando o Application Migration Service
- Redefinir a hospedagem de workloads on-premises na Nuvem AWS: lista de verificação de migração
- Configure a infraestrutura Multi-AZ para um SQL Server Always On FCI usando a Amazon FSx

- Use as consultas do BMC Discovery para extrair dados de migração para o planejamento da migração

Acelere a descoberta e a migração de cargas de trabalho da Microsoft para a AWS

Criado por Ali Alzand

Resumo

Esse padrão mostra como usar o PowerShell módulo Migration Validator Toolkit para descobrir e migrar suas cargas de trabalho da Microsoft para a AWS. O módulo funciona executando várias verificações e validações para tarefas comuns associadas a qualquer workload da Microsoft. Por exemplo, o módulo verifica se há instâncias que podem ter vários discos conectados a ele ou instâncias que usam muitos endereços IP. Para obter uma lista completa das verificações que o módulo pode realizar, consulte a seção Verificações na GitHub página do módulo.

O PowerShell módulo Migration Validator Toolkit pode ajudar sua organização a reduzir o tempo e o esforço envolvidos na descoberta de quais aplicativos e serviços estão sendo executados em suas cargas de trabalho da Microsoft. O módulo também pode ajudar a identificar as configurações de suas workloads para que você possa descobrir se há suporte para suas configurações na AWS. O módulo também fornece recomendações para as próximas etapas e ações de mitigação, para que você possa evitar configurações incorretas antes, durante ou depois da migração.

Pré-requisitos e limitações

Pré-requisitos

- Conta de administrador local
- PowerShell 4.0

Limitações

- Funciona somente no Microsoft Windows Server 2012 R2 ou posterior

Ferramentas

Ferramentas

- PowerShell 4.0

Repositório de código

O PowerShell módulo Migration Validator Toolkit para esse padrão está disponível no repositório GitHub migration-validator-toolkit-for-microsoft-workloads.

Épicos

Execute o PowerShell módulo Migration Validator Toolkit em um único destino

Tarefa	Descrição	Habilidades necessárias

Baixe, extraia, importe e invoque o módulo.	Escolha um dos métodos a seguir para baixar e implantar o módulo:
	• Execute o PowerShell script
	• Baixe e extraia o arquivo.zip
	• Clone o repositório GitHub
	
	Execute o PowerShell script
	
	Em PowerShell, execute o seguinte código de exemplo:
	
	`#MigrationValidatorToolkit`
	`$uri = 'https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads/archive/refs/heads/main.zip'`
	`$destination = (Get-Location).Path`
	`if ((Test-Path -Path "$destination\MigrationValidatorToolkit.zip" -PathType Leaf) -or (Test-Path -Path "$destination\MigrationValidatorToolkit")) {`
		Administrador de sistema

Tarefa	Descrição	Habilidades necessárias

	`write-host "File $destination\MigrationValidatorToolkit.zip or folder $destination\MigrationValidatorToolkit found, exiting"`
	`}else {`
	`Write-host "Enable TLS 1.2 for this PowerShell session only."`
	`[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`
	`$webClient = New-Object System.Net.WebClient`
	`Write-host "Downloading MigrationValidatorToolkit.zip"`
	`$webClient.DownloadFile($uri, "$destination\MigrationValidatorToolkit.zip")`
	`Write-host "MigrationValidatorToolkit.zip download successfully"`
	`Add-Type -Assembly "system.io.compression.filesystem"`
	`[System.IO.Compression.ZipFile]::ExtractToDirectory("$destination\MigrationValidatorToolkit.zip","$destination\MigrationValidatorToolkit")`	

Tarefa	Descrição	Habilidades necessárias

	<pre>Write-host
	"Extracting Migration
	ValidatorToolkit.zip
	complete successfully"
	Import-Module
	"$destination\Migr
	ationValidatorToolkit
	\migration-validator-
	toolkit-for-microsoft
	-workloads-main\Mi
	grationValidatorTo
	olkit.psm1"; Invoke-
	MigrationValidatorTo
	olkit
	}</pre>
	O código baixa o módulo de um arquivo.zip. Em seguida, o código extrai, importa e invoca o módulo.
	Baixe e extraia o arquivo.zip
	1. Baixe o arquivo.zip (download).
	2. Extraia o arquivo .zip.
	3. Siga as etapas na história Invocar o módulo manualmente deste guia.
	Clone o repositório GitHub
	1. Para clonar o repositório GitHub migration-validator-toolkit-for-microsoft-workloads, execute o seguinte	

Tarefa	Descrição	Habilidades necessárias
	comando Git em uma janela de terminal: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git` 2. Siga as etapas na história Invocar o módulo manualmente deste guia.	

Tarefa	Descrição	Habilidades necessárias

Invoque o módulo manualmente.	1. Vá para o diretório em que o módulo baixado está armazenado.
	2. Para gerar a saída de sua escolha, execute um dos seguintes comandos como administrador em PowerShell:
	
	Formato - Formato da tabela:
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit`
	
	Formato da lista de formatos:
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -List`
	
	GridViewFormato externo:
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -GridView`
	
	ConvertTo-Formato CSV:
	`Import-Module .\MigrationValidatorToolkit`
		Administrador de sistema

Tarefa	Descrição	Habilidades necessárias
	`.psm1;Invoke-Migra tionValidatorToolkit -csv`	

Execute o PowerShell módulo Migration Validator Toolkit em vários destinos

Tarefa	Descrição	Habilidades necessárias
Baixe o arquivo.zip ou clone o GitHub repositório.	Escolha uma das seguintes opções: • Baixe o arquivo zip. (baixar). • Para clonar o repositório GitHub migration-validator-toolkit-for-microsoft-workloads, execute o seguinte comando Git em uma janela de terminal: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git`	Administrador de sistema
Atualize a lista server.csv.	Se você baixou o arquivo.zip, siga estas etapas: 1. Extraia o arquivo .zip. 2. Acesse o diretório `MigrationValidatorToolkit\Inputs\` .	Administrador de sistema

Tarefa	Descrição	Habilidades necessárias
	3. Atualize `serverlist.csv` com o nome do host dos computadores de destino.	
Invoque o módulo.	Você pode usar qualquer computador dentro do domínio que use um usuário de domínio que tenha acesso de administrador aos computadores de destino. 1. Baixe o código-fonte como um arquivo.zip e extraia o arquivo. 2. Como administrador em PowerShell, execute o seguinte comando: `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-DomainComputers` O arquivo.csv de saída é salvo `MigrationValidatorToolkit\Outputs\folder` com o nome do prefixo. `DomainComputers_MigrationAutomations_YYYY-MM-DDTHH-MM-SS`	Administrador de sistema

Solução de problemas

Problema	Solução
`MigrationValidatorToolkit` grava informações sobre execuções, comandos e erros nos arquivos de log no host em execução.	Você pode visualizar os arquivos de log manualmente no seguinte local: 1. Acesse o diretório `MigrationValidatorToolkit\logs\` . 2. Localize o arquivo de log. O formato do nome do arquivo de log é: `ComputerName_MigrationValidatorToolkit_YYYY-MM-SSTHH-MM-SS.log`

Recursos relacionados

- Opções, ferramentas e melhores práticas para migrar cargas de trabalho da Microsoft para a AWS (AWS Prescriptive Guidance)
- Padrões de migração da Microsoft (AWS Prescriptive Guidance)
- Serviços gratuitos de migração para a nuvem na AWS (documentação da AWS)
- Ações predefinidas de pós-lançamento (documentação de marketing de aplicativos)

Mais informações

Perguntas frequentes

Onde posso executar o módulo Migration Validator Toolkit PowerShell ?

Você pode executar o módulo no Microsoft Windows Server 2012 R2 ou posterior.

Quando eu executo esse módulo?

Recomendamos que você execute o módulo durante a fase de avaliação da jornada de migração.

O módulo modifica meus servidores existentes?

Não. Todas as ações neste módulo são somente para leitura.

Quanto tempo é necessário para executar o módulo?

Normalmente, a execução do módulo leva de 1 a 5 minutos, mas isso depende da alocação de recursos do seu servidor.

Quais permissões o módulo precisa para ser executado?

Você deve executar o módulo a partir de uma conta de administrador local.

Posso executar o módulo em servidores físicos?

Sim, desde que o sistema operacional seja o Microsoft Windows Server 2012 R2 ou posterior.

Como faço para executar o módulo em grande escala para vários servidores?

Para executar o módulo em vários computadores associados a um domínio em grande escala, siga as etapas do PowerShell módulo Executar o kit de ferramentas do Migration Validator em vários destinos, épico deste guia. Para computadores não associados a um domínio, use uma invocação remota ou execute o módulo localmente seguindo as etapas do módulo Executar o kit de ferramentas do Migration Validator em um único épico de PowerShell destino deste guia.

Automatize as atividades de pré-ingestão de workload para o AWS Managed Services no Windows

Criado por Jacob Zhang (AWS), Calvin Yeh (AWS) e Dwayne Bordelon (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), o AWS Managed Services (AMS) usa a ingestão de workload do AMS (WIGS) para mover as workloads existentes para uma VPC gerenciada pelo AMS. Esse padrão descreve uma solução para automatizar atividades comuns de pré-ingestão de carga de trabalho, como atualizar o.NET e Windows PowerShell e executar a validação de pré-ingestão do Windows WIGS mantida pelo AMS. O padrão também fornece uma interface de usuário unificada para os resultados da execução. Ele empacota um documento do AWS Systems Manager Command, que executa as atividades de pré-ingestão, em um modelo da AWS CloudFormation . O modelo pode ser implantado repetidamente sem exigir acesso ao próprio Systems Manager ou entrar em conflito com as automações do AMS.

Histórico de negócios

As migrações para o AMS exigem o fornecimento de novas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) usando Amazon Machine Images (AMIs) gerenciadas pelo AMS que incluem componentes do AMS. Quaisquer cargas de trabalho ou aplicativos em execução nos datacenters existentes devem ser reimplantados em novas EC2 instâncias iniciadas a partir desses AMS. AMIs Para evitar a quantidade potencialmente enorme de trabalho manual durante o processo, a equipe do AMS criou o fluxo de trabalho de ingestão de workload do AMS (WIGS) para integrar suas imagens personalizadas ao AMS.

As instâncias do Windows devem atender a alguns pré-requisitos antes que o processo WIGS ocorra. Os PowerShell scripts do Windows geralmente são usados para realizar os preparativos necessários (preparação do WIGS) e verificar se as instâncias estão prontas WIGs (validação de pré-ingestão do WIGS). Os processos de preparação e validação requerem que um engenheiro passe de 15 a 30 minutos em cada servidor, fazendo login manualmente e executando os scripts um por um.

Condutor de negócios

Tradicionalmente, usando o Systems Manager, você pode automatizar tarefas operacionais, como executar PowerShell scripts do Windows. No entanto, devido aos riscos elevados e aos conflitos frequentes entre as automações do AMS e as dos usuários, o AMS geralmente não concede aos usuários acesso ao Systems Manager.

Para migrações em massa usando o AWS Application Migration Service (AWS MGN), os PowerShell scripts do Windows `C:\Program Files (x86)\AWS Replication Agent\post_launch folder` geralmente são executados automaticamente quando uma instância de teste ou substituição é iniciada. No entanto, esses scripts, se executados imediatamente durante a inicialização de uma instância, costumam entrar em conflito com as automações do AMS. Assim, o lançamento pode falhar sem fornecer os resultados de execução necessários para solucionar a falha.

Esse padrão resolve esses problemas e fornece uma solução automatizada funcional.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da AWS com a integração do AMS concluída.
- Um bucket do Amazon Simple Storage Service (Amazon S3) na conta AWS. Se não houver um bucket do S3 sobre o qual você tenha controle na conta, use uma solicitação de alteração (RFC) para criar um.
- O modelo Pre WIGs _CFN.json baixado do repositório. ams-auto-prewigs-windows
- Um servidor ao qual esse padrão foi aplicado deve atender aos seguintes requisitos:
  - Executar Windows Server 2012 ou versão posterior.
  - Ser iniciador ou estar pronto para ser iniciado na sub-rede de migração de VPC do sandbox.
  - Ter um AWS Systems Manager Agent (SSM Agent) instalado.
  - Ter um perfil de instância do AWS Identity and Access Management (IAM) anexado. O perfil de instância deve ter permissões para baixar arquivos de buckets do S3 na mesma conta AWS. Um perfil de instância que satisfaça o requisito mencionado acima geralmente já foi estabelecido durante as configurações anteriores de uma migração.
  - Ser visível no AWS Systems Manager Fleet Manager.

Limitações

- As atividades pré-WIGS variam de acordo com o ambiente e os requisitos comerciais. Talvez seja necessário fazer pequenas modificações nesse padrão para atender às suas necessidades específicas.

Versões do produto

- O padrão foi testado com o Windows Server 2012, 2012 R2, 2016 e 2019. Teoricamente, ele funciona com versões mais recentes do Windows. Ele não funciona com versões anteriores do Windows.

Arquitetura

O diagrama da arquitetura mostra o seguinte:

1. Uma VPC de sandbox com uma sub-rede de migração contendo servidores que não foram preparados.
2. O bucket do S3 que armazena scripts usados pelo CloudFormation modelo.
3. O CloudFormation modelo implanta o documento Systems Manager Command. O processo é iterado até que as etapas sejam concluídas.
4. As instâncias são preparadas e, RFCs para o WIGS, são feitas.
5. Na VPC gerenciada pelo AMS, a sub-rede gerenciada pelo AMS contém os servidores após a ingestão da workload.

Como funciona

- Esse padrão é empacotado em um CloudFormation modelo da AWS que permite implantações repetíveis de infraestrutura como código (IaC). Você precisa implantar esse modelo apenas uma vez para cada conta AWS que requer essa automação.
- A automação é aplicada a todas as EC2 instâncias com uma chave de tag AutoPreWIGsna conta da AWS em que esse padrão é implantado. Na primeira vez em que uma instância EC2 do Amazon Windows com a chave de tag AutoPreWIGsé iniciada, a automação executa as seguintes tarefas.
    1. Atualiza o Windows PowerShell para a versão 5.1 e o.NET para a versão 4.5.2. A instância pode ser reinicializada várias vezes, dependendo das versões existentes do Windows PowerShell e.NET. Após cada reinicialização, as atualizações continuam até serem concluídas. Essa etapa usa código incorporado no CloudFormation modelo modificado a partir de um PowerShell script do Windows, bem como orientações específicas do Systems Manager sobre reinicializações de servidores.

2. Faz o download do Amazon S3 e executa um PowerShell script do Windows que você personalizou para preparar a instância EC2 do Amazon Windows para o WIGS. Para obter mais informações, consulte a seção Épicos.
3. Instala o módulo PowerShell de validação de pré-ingestão do Windows WIGS da AWS.
4. Executa a validação de pré-ingestão do Windows WIGS e torna os resultados visíveis no Systems Manager State Manager.

Ferramentas

- AWS CloudFormation — CloudFormation A AWS é um serviço que ajuda você a modelar e configurar seus recursos da AWS. Você pode usar um que descreva todos os recursos da AWS que você deseja e suas dependências, para que você possa iniciar e configurar esses recursos como uma pilha. Esse padrão usa um CloudFormation modelo para automatizar a implantação dos recursos nesse padrão.
- AWS Managed Services: o AWS Managed Services (AMS) é um serviço corporativo que fornece gerenciamento contínuo de sua infraestrutura da AWS. As alterações feitas na infraestrutura em um ambiente AMS devem ser feitas por meio de um RFC.
- AWS Systems Manager: o AWS Systems Manager (Conhecido anteriormente como SSM) é um serviço da que você pode usar para visualizar e controlar sua infraestrutura na . Usando o console do Systems Manager, você pode visualizar dados operacionais de vários serviços da AWS e automatizar tarefas operacionais nos recursos da AWS. Esse padrão usa o Systems Manager para executar e visualizar os resultados das atividades pré-WIGS.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade líder do setor, disponibilidade de dados, segurança e performance. Esse padrão usa o Amazon S3 para armazenar o CloudFormation modelo e um PowerShell script do Windows que é baixado.

Épicos

Crie um PowerShell script personalizado do Windows para automatizar tarefas adicionais

Tarefa	Descrição	Habilidades necessárias
Execute as alterações necessárias nos servidores	Se você precisar que as alterações sejam aplicadas automaticamente aos	PowerShell criação de scripts

Tarefa	Descrição	Habilidades necessárias
com base nas necessidades comerciais.	seus servidores antes de serem ingeridas, crie um PowerShell script do Windows chamado`ingestion-prep.ps1` . **Important** O script não deve conter instruções para reinicializar o servidor e não deve exigir privilégios de administrador.	
Remova o software que não é compatível com o AMS.	O AMS exige que determinados softwares, como aplicativos antivírus e VMware ferramentas, sejam removidos antes da execução do WIGS. Inclua a desinstalação no script `ingestion-prep.ps1` . Para obter mais informações sobre software incompatível, consulte a Documentação da AWS.	PowerShell criação de scripts

Faça o upload do CloudFormation modelo e do PowerShell script opcional do Windows para o Amazon S3

Tarefa	Descrição	Habilidades necessárias
Crie uma pasta no S3.	Em um bucket do S3 na mesma conta AWS em que	AWS geral

Tarefa	Descrição	Habilidades necessárias
	esse padrão foi implantado, crie uma pasta.	
Faça o upload de scripts	Faça o upload do `PreWIGs_CFN.json` CloudFormation modelo e do PowerShell script `ingestion-prep.ps1` do Windows, que você criou no épico anterior, para a pasta Amazon S3.	AWS geral

Implante a CloudFormation pilha

Tarefa	Descrição	Habilidades necessárias
Selecione o tipo de alteração.	Navegue até o console AMS para criar um RFC. Use o tipo de alteração Create Stack from CloudFormation (CFN) Template.	AMS geral
Defina os parâmetros de execução para o caminho até o CloudFormation modelo.	Na seção Configurações de execução, expanda Configuração do resultado da consulta. Na caixa de endpoint do CloudFormation modelo S3, cole a URL no modelo. CloudFormation	AMS geral
Especificar o caminho a pasta Amazon S3.	Em Parâmetros, use ScriptSourcecomo Nome. Em Valor, insira o caminho para a pasta S3 que contém os PowerShell scripts do Windows. Certifique-se de	AMS geral

Tarefa	Descrição	Habilidades necessárias
	usar o `https://xxx` URL em vez do `s3://xxx` URI e inclua o `/` no final.	
Implante a pilha.	Selecione Criar para implantar a stack.	AMS geral
Escale o RFC para o AMS Ops.	A RFC deve ser implementada manualmente pela equipe de operações do AMS porque ela usa o Systems Manager para implantar recursos e exige uma análise de segurança . Assim que você criar o RFC, ele será automatic amente rejeitado pelo sistema. Escolha o RFC e adicione uma correspondência ao RFC indicando Execute manualmen te. Anote o ID do RFC e escale-o com uma solicitação de serviço.	AMS geral

Aplique a automação às instâncias

Tarefa	Descrição	Habilidades necessárias
Adicione a AutoPre WIGs tag às instâncias.	Anote IDs todas as instância s às quais você deseja aplicar essa automação e aguarde pelo menos 30 minutos para que a instância conclua as automações implementadas pelo AMS. Envie um RFC automatizado para adicionar a	AMS geral

Tarefa	Descrição	Habilidades necessárias
	tag AutoPreWIGscomo chave e qualquer string, como 1, como valor. A automação será aplicada alguns minutos depois de você adicionar a tag.	
Verifique os resultados da automação.	Abra o console do Systems Manager e escolha o State Manager. Escolha o ID da associação com o nome AMS-Prewig-Prep-and-Validation-Association. Na guia Histórico de execução, você pode ver os resultados da automação.	AMS geral
Corrija todos os erros.	Se a automação falhar, escolha sua ID de execução. Você pode ver os resultado s da execução de cada EC2 instância. Para ver os detalhes de cada etapa da automação , escolha Saída. Se uma etapa específica falhar, use as informações nas seções Saída e Erro para diagnosticar o problema.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Remova a AutoPre WIGs etiqueta.	**Important** Depois de corrigir os erros, se houver, envie uma RFC automátic a para remover a AutoPreWIGstag. O WIGS falhará se você não remover a etiqueta.	AMS geral

Ingira as instâncias preparadas

Tarefa	Descrição	Habilidades necessárias
Envie RFCs para o WIGS.	Agora que as instâncias estão prontas para a ingestão da carga de trabalho, envie-as RFCs para o WIGS.	AMS geral

Recursos relacionados

- Ingestão de workload do AMS (WIGS)
- Migração de workloads: validação de pré-ingestão do Windows
- Guia de início rápido do AWS Application Migration Service
- Comece a usar a AWS CloudFormation
- Configurar o AWS Systems Manager

Crie um processo de aprovação para solicitações de firewall durante uma migração de rehospedagem para AWS

Criado por Srikanth Rangavajhala (AWS)

Resumo

Se você quiser usar AWS Application Migration Serviceo Cloud Migration Factory ativado AWS para rehospedar a migração para o Nuvem AWS, um dos pré-requisitos é manter as portas TCP 443 e 1500 abertas. Normalmente, a abertura dessas portas de firewall requer a aprovação da equipe de segurança da informação (InfoSec).

Esse padrão descreve o processo para obter a aprovação de uma solicitação de firewall de uma InfoSec equipe durante uma migração de rehospedagem para o. Nuvem AWS Você pode usar esse processo para evitar rejeições de sua solicitação de firewall pela InfoSec equipe, o que pode se tornar caro e demorado. O processo de solicitação de firewall tem duas etapas de revisão e aprovação entre consultores de AWS migração e líderes que trabalham com você InfoSec e com as equipes de aplicativos para abrir as portas do firewall.

Esse padrão pressupõe que você esteja planejando uma migração de rehospedagem com AWS consultores ou especialistas em migração da sua organização. Você pode usar esse padrão se sua organização não tiver um processo de aprovação de firewall ou um formulário de aprovação geral de solicitação de firewall. Para obter mais informações sobre isso, consulte a seção Limitações desse padrão. Para obter mais informações sobre os requisitos de rede do Application Migration Service, consulte Requisitos de rede na documentação do Application Migration Service.

Pré-requisitos e limitações

Pré-requisitos

- Uma migração planejada de rehospedagem com AWS consultores ou especialistas em migração de sua organização
- As informações de porta e IP necessárias para migrar a pilha
- Diagramas de arquitetura de estado existentes e futuros
- Informações de firewall sobre a infraestrutura local e de destino, portas e zone-to-zone fluxo de tráfego
- Uma lista de verificação de revisão de solicitações de firewall (anexada)
- Um documento de solicitação de firewall, configurado de acordo com os requisitos da sua organização

- Uma lista de contatos para os revisores e aprovadores do firewall, incluindo as seguintes funções:
  - Remetente da solicitação de firewall — especialista ou consultor em AWS migração. O remetente da solicitação de firewall também pode ser um especialista em migração da sua organização.
  - Revisor de solicitações de firewall — Normalmente, esse é o ponto único de contato (SPOC) de. AWS
  - Aprovador da solicitação de firewall — Um membro InfoSec da equipe.

Limitações

- Esse padrão descreve um processo genérico de aprovação de solicitações de firewall. Os requisitos podem variar para organizações individuais.
- Certifique-se de monitorar as alterações em seu documento de solicitação de firewall.

A tabela a seguir mostra os casos de uso desse padrão.

Sua organização tem um processo de aprovação de firewall existente?	Sua organização tem um formulário de solicitação de firewall existente?	Ação sugerida
Sim	Sim	Colabore com AWS consultor es ou especialistas em migração para implementar o processo de sua organização.
Não	Sim	Use o processo de aprovação do firewall desse padrão. Use um AWS consultor ou um especialista em migração da sua organização para enviar o formulário de aprovação geral de solicitação de firewall.
Não	Não	Use o processo de aprovação do firewall desse padrão. Use um AWS consultor ou um

	especialista em migração da sua organização para enviar o formulário de aprovação geral de solicitação de firewall.

Arquitetura

O diagrama a seguir mostra as etapas do processo de aprovação da solicitação do firewall.

Ferramentas

Você pode usar ferramentas de scanner, como a Palo Alto Networks, ou SolarWindspara analisar e validar firewalls e endereços IP.

Épicos

Analise a solicitação de firewall

Tarefa	Descrição	Habilidades necessárias
Analise as portas e os endereços IP.	O remetente da solicitação de firewall conclui uma análise inicial para entender as portas de firewall e os endereços IP necessários. Depois que isso for concluído, eles solicitam que sua InfoSec equipe abra as portas necessárias e mapeie os endereços IP.	Engenheiro de nuvem AWS, especialista em migração

Valide a solicitação de firewall

Tarefa	Descrição	Habilidades necessárias
Valide as informações do firewall.	O Nuvem AWS engenheir o agenda uma reunião com sua InfoSec equipe. Durante	Engenheiro de nuvem AWS, especialista em migração

Tarefa	Descrição	Habilidades necessárias
	essa reunião, o engenheiro examina e valida as informaçõ es da solicitação do firewall. Normalmente, o remetente da solicitação de firewall é a mesma pessoa que o solicitante do firewall. Essa fase de validação pode se tornar iterativa com base no feedback dado pelo aprovador , caso algo seja observado ou recomendado.	
Atualize o documento de solicitação do firewall.	Depois que a InfoSec equipe compartilha seus comentários, o documento de solicitação do firewall é editado, salvo e reenviado. Este documento é atualizado após cada iteração. Recomendamos que você armazene esse documento em uma pasta de armazenam ento com controle de versão. Isso significa que todas as alterações são rastreadas e aplicadas corretamente.	Engenheiro de nuvem AWS, especialista em migração

Envie a solicitação de firewall

Tarefa	Descrição	Habilidades necessárias
Envie a solicitação de firewall.	Depois que o aprovador da solicitação de firewall aprova a	Engenheiro de nuvem AWS, especialista em migração

Tarefa	Descrição	Habilidades necessárias
	solicitação de aprovação geral do firewall, o Nuvem AWS engenheiro envia a solicitaç ão de firewall. A solicitaç ão especifica as portas que devem estar abertas e os endereços IP necessários para mapear e atualizar o. Conta da AWS Você pode fazer sugestões ou fornecer feedback após o envio da solicitação do firewall. Recomendamos que você automatize esse processo de feedback e envie qualquer edição por meio de um mecanismo de fluxo de trabalho definido.	

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Ingira e migre instâncias EC2 do Windows para uma conta do AWS Managed Services

Criado por Anil Kunapareddy (AWS) e Venkatramana Chintha (AWS)

Resumo

Esse padrão explica o step-by-step processo de migração e ingestão de instâncias Windows do Amazon Elastic Compute Cloud (Amazon EC2) em uma conta do Amazon Web Services (AWS) Managed Services (AMS). O AMS pode ajudar você a gerenciar a instância com mais eficiência e segurança. O AMS fornece flexibilidade operacional, aprimora a segurança e a conformidade, além de ajudar a otimizar a capacidade e reduzir custos.

Esse padrão começa com uma instância EC2 do Windows que você migrou para uma sub-rede de teste na sua conta do AMS. Vários serviços e ferramentas de migração estão disponíveis para realizar essa tarefa, como o AWS Application Migration Service.

Para fazer uma alteração em seu ambiente gerenciado pelo AMS, você cria e envia uma solicitação de alteração (RFC) para uma operação ou ação específica. Usando uma RFC de ingestão de workload (WIGS) do AMS, você ingere a instância na conta do AMS e cria uma imagem de máquina da Amazon (AMI) personalizada. Em seguida, você cria a EC2 instância gerenciada pelo AMS enviando outra RFC para criar uma pilha. EC2 Para obter mais informações, consulte Ingestão de workload AMS na documentação do AMS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da AWS ativa e gerenciada pelo AMS
- Uma zona de pouso existente
- Permissões para fazer alterações na VPC gerenciada pelo AMS
- Uma instância EC2 do Amazon Windows em uma sub-rede de teste em sua conta AMS
- Conclusão dos pré-requisitos gerais para migrar workloads usando a WIGS do AMS
- Conclusão dos pré-requisitos do Windows para migrar workloads usando a WIGS do AMS

Limitações

- Esse padrão é para EC2 instâncias que operam o Windows Server. Este padrão não se aplica a instâncias que executam outros sistemas operacionais, como Linux.

Arquitetura

Pilha de tecnologia de origem

Instância EC2 do Amazon Windows em uma sub-rede de teste em sua conta AMS

Pilha de tecnologias de destino

Instância EC2 do Amazon Windows gerenciada pelo AWS Managed Services (AMS)

Arquitetura de destino

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode usar EC2 a Amazon para lançar quantos servidores virtuais precisar e pode expandir ou aumentar a escala.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Managed Services (AMS) ajuda você a operar com mais eficiência e segurança ao fornecer gerenciamento contínuo da sua infraestrutura da AWS, incluindo monitoramento, gerenciamento de incidentes, orientação de segurança, suporte a patches e backup para workloads da AWS.

Outros serviços

- PowerShellé um programa de gerenciamento de automação e configuração da Microsoft executado em Windows, Linux e macOS.

Épicos

Definir configurações na instância

Tarefa	Descrição	Habilidades necessárias
Altere as configurações do Cliente DNS.	1. Na EC2 instância de origem, abra o Prompt de	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	Comando como administr adorgpedit.msc , digite e pressione Enter. 2. No Editor de política de grupo local, navegue até Configuração do computador, Modelos administrativos, Rede, Cliente DNS. 3. Em Sufixo de DNS primário, escolha Não configurado. 4. Para Sufixo de DNS primário, escolha Não configurado.	

Tarefa	Descrição	Habilidades necessárias
Altere as configurações do Windows Update.	1. Em Editor de política de grupo local, navegue até Configuração do computador, Modelos administrativos, Componentes do Windows, Atualizações do Windows. 2. Em Especificar a localização do serviço Microsoft Update na intranet, escolha Não configurado. 3. Para Configurar atualizações automáticas, escolha Não configurado. 4. Para Frequência de deteção de atualizações automáticas, escolha Não configurado. 5. Feche o Editor de política de grupo local.	Engenheiro de migração
Ativar o firewall.	1. Na EC2 instância de origem, abra o Prompt de Comando como administrador`services.msc`, digite e pressione Enter. 2. Nos Serviços do Windows, habilite Firewall. 3. Feche os Serviços do Windows.	Engenheiro de migração

Prepare a instância para o WIGS do AMS

Tarefa	Descrição	Habilidades necessárias
Limpe e prepare a instância.	1. Usando um host Bastion e credenciais locais, crie uma conexão RDP (Remote Desktop Protocol) com a EC2 instância na sub-rede de teste. 2. Remova todo o software herdado, o software antivírus e as soluções de backup que não são necessários no AMS.	Engenheiro de migração

Repare o arquivo sppnp.dll.	1. Acesse `C:\Windows\System32\sppnp.dll` .
	2. Renomeie `sppnp.dll` para `sppnp_old.dll` .
	3. Usando PowerShell as credenciais de administrador, digite os seguintes comandos:
	`dism /online /cleanup-image /restorehealth`
	`sfc /scannnow`
	4. Reinicie a instância EC2 do Windows.
		Engenheiro de migração

Execute o script de validação pré-WIG.	1. Baixe o arquivo zip de validação de pré-ingestão WIGS do Windows (`windows-prewings-`	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	`valication.zip`) em Migração de workloads: validação de pré-ingestão do Windows na documentação do AMS. 2. Execute o script de validação pré-WIG do Windows e verifique os resultados. 3. Se a validação falhar, corrija o problema e execute novamente o script de validação até obter êxito.	
Crie a AMI à prova de falhas.	Depois que a validação pré-WIG for aprovada, crie uma AMI de pré-ingestão da seguinte forma: 1. Escolha Implantação, Componentes avançados de pilha, AMI e Criar. 2. Durante a criação, adicione uma tag `Key=Name, Value=APPLICATION-ID_IngestReady` . 3. Espere até que a AMI seja criada antes de continuar. Para obter mais informaçõ es, consulte AMI | Criar na documentação do AMS.	Engenheiro de migração

Ingerir e validar a instância

Tarefa	Descrição	Habilidades necessárias
Envie a RFC para criar a pilha de ingestão de workload.	Envie uma solicitação de alteração (RFC) para iniciar a WIGS do AMS. Para obter instruções, consulte Pilha de ingestão de workload: criação na documentação do AMS. Isso inicia a ingestão da carga de trabalho e instala todo o software exigido pelo AMS, incluindo ferramentas de backup, software de EC2 gerenciamento da Amazon e software antivírus.	Engenheiro de migração
Valide a migração bem-sucedida.	Depois que a ingestão de workload for concluída, você poderá ver a instância gerenciada pelo AMS e a AMI ingerida pelo AMS. 1. Faça login na instância gerenciada pelo AMS com as credenciais do domínio. 2. Valide a adesão ao domínio da seguinte forma: a. No Windows Explorer, clique com o botão direito do mouse em Este PC e escolha Propriedades. b. Na seção Especificação do dispositivo, confirme se o domínio aparece	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	no Nome completo do dispositivo. 3. Valide as unidades de disco de origem e de destino.	

Executar a instância na conta da AMS de destino

Tarefa	Descrição	Habilidades necessárias
Envie o RFC para criar uma EC2 pilha.	1. Usando a AMI ingerida pelo AMS da instância do Windows, prepare uma RFC para EC2 uma pilha de acordo com as instruções em EC2 Criar instância de pilha na documentação do AMS. Na EC2 pilha RFC, forneça todos os parâmetros, incluindo nome do servidor, tags, VPC de destino, sub-rede de destino, tipo de instância, grupos de segurança de destino, AMI de ingestão e função. 2. Envie o RFC para a EC2 pilha e aguarde até que a instância seja criada com sucesso.	Engenheiro de migração

Recursos relacionados

Recomendações da AWS

- Automatize as atividades de pré-ingestão de workload para o AWS Managed Services no Windows
- Crie automaticamente uma RFC no AMS usando Python

Documentação do AMS

- Ingestão de workload do AMS
- Como a migração altera seu recurso
- Migração de workloads: processo padrão

Recursos de marketing

- AWS Managed Services
- AWS Managed Services FAQs
- Recursos do AWS Managed Services
- Atributos do AWS Managed Services

Migrar um banco de dados do Couchbase Server para a Amazon EC2

Criado por Subhani Shaik (AWS)

Resumo

Esse padrão descreve como você pode migrar o Couchbase Server de um ambiente local para o Amazon Elastic Compute Cloud (Amazon) em. EC2 AWS

O Couchbase Server é um banco de dados NoSQL (documento JSON) distribuído que fornece recursos de banco de dados relacional. A migração de um banco de dados do Couchbase Server AWS pode fornecer maior escalabilidade, melhor desempenho, eficiência de custos, segurança aprimorada, gerenciamento simplificado e alcance global, o que pode beneficiar aplicativos que exigem alta disponibilidade e acesso a dados de baixa latência. Você também obtém acesso a recursos avançados por meio de serviços AWS gerenciados.

O Couchbase Server on AWS fornece os seguintes recursos principais:

- Arquitetura que prioriza a memória
- Alta disponibilidade, recuperação de desastres e balanceamento de carga
- Implantação em vários mestres e várias regiões para um desempenho ideal

Para obter mais informações sobre os principais benefícios, consulte a seção Informações adicionais e o site do Couchbase.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS com uma nuvem privada virtual (VPC), duas zonas de disponibilidade, sub-redes privadas e um grupo de segurança. Para obter instruções, consulte Criar uma VPC na documentação da Amazon Virtual Private Cloud (Amazon VPC).
- Conectividade habilitada entre os ambientes de origem e de destino. Para obter informações sobre as portas TCX usadas pelo Couchbase Server, consulte a documentação do Couchbase.

Arquitetura

O diagrama a seguir mostra a arquitetura de alto nível para a migração do Couchbase Server para o. AWS

Do cluster local do Couchbase, os dados são movidos por um gateway do cliente usando. AWS Direct Connect Os dados passam por um roteador e uma AWS Direct Connect rota e chegam à VPC por meio de um gateway AWS Virtual Private Network (AWS VPN). A VPC contém uma EC2 instância que está executando o Couchbase Server. A AWS infraestrutura também inclui AWS Identity and Access Management (IAM) para controle de acesso, AWS Key Management Service (AWS KMS) para criptografia de dados, Amazon Elastic Block Store (Amazon EBS) para armazenamento em blocos e Amazon Simple Storage Service (Amazon S3) para armazenamento de dados.

Ferramentas

Serviços da AWS

- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- AWS Direct Connectconecta sua rede interna a um AWS Direct Connect local por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para o público, Serviços da AWS ignorando os provedores de serviços de Internet em seu caminho de rede.

Práticas recomendadas

- Instalando e configurando o Couchbase em diferentes plataformas operacionais
- Melhores práticas para implantar o Couchbase Server em AWS
- Criação de um cluster Couchbase
- Melhores práticas de desempenho para aplicativos Couchbase
- Melhores práticas de segurança para o Couchbase Server
- Práticas recomendadas de armazenamento para bancos de dados do Couchbase Server

Épicos

Implemente uma EC2 instância da Amazon para o Couchbase Server

Tarefa	Descrição	Habilidades necessárias
Abra o EC2 console da Amazon.	Faça login no AWS Management Consolee abra o EC2 console da Amazon.	DevOps engenheiro, administrador do Couchbase
Implante uma EC2 instância da Amazon.	Execute uma EC2 instância que corresponda às configurações locais do Couchbase Server. Para obter mais informações sobre como implantar uma EC2 instância, consulte Iniciar uma EC2 instância da Amazon na EC2 documentação da Amazon.	DevOps engenheiro, administrador do Couchbase

Instale e configure o Couchbase Server na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Instale um cluster Couchbase.	Revise as diretrizes de implantação do Couchbase Server antes de instalar o Couchbase Server na Amazon. EC2 Para instalar o Couchbase Server, consulte a documentação do Couchbase Server	Administrador do Couchbase
Configure o cluster.	Para configurar o cluster, consulte Opções de configura	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	ção do cluster na documenta ção do Couchbase.	

Adicione um novo nó e reequilibre o cluster do Couchbase

Tarefa	Descrição	Habilidades necessárias
Adicione um nó para a EC2 instância.	Adicione a EC2 instância recém-implantada que tem o Couchbase instalado no cluster local existente. Para obter instruções, consulte Adicionar um nó e rebalance ar na documentação do Couchbase Server.	Administrador do Couchbase
Rebalanceie o cluster.	O processo de rebalance amento torna o nó recém-adi cionado com a EC2 instância um membro ativo do cluster Couchbase. Para obter instruções, consulte Adicionar um nó e rebalancear na documentação do Couchbase Server	Administrador do Couchbase

Reconfigurar conexões

Tarefa	Descrição	Habilidades necessárias
Remova os nós locais e reequilibre.	Agora você pode remover os nós locais do cluster. Depois de remover os nós, siga o processo de rebalance	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	amento para redistribuir dados, índices, processam ento de eventos e processam ento de consultas entre os nós disponíveis no cluster. Para obter instruções, consulte Remover um nó e reequilib rar na documentação do Couchbase Server.	
Atualize os parâmetros de conexão.	Atualize os parâmetros de conexão do seu aplicativo para usar o novo endereço EC2 IP da Amazon, para que seu aplicativo possa se conectar ao novo nó.	Desenvolvedor de aplicativos Couchbase

Recursos relacionados

- Serviços de servidor Couchbase
- Implemente o Couchbase Server usando AWS Marketplace
- Conecte-se ao Couchbase Server
- Gerenciar buckets
- Replicação entre data centers (XDCR)
- Contrato de licença da Couchbase Inc.

Mais informações

Benefícios principais

A migração do seu banco de dados Couchbase AWS oferece as seguintes vantagens:

Escalabilidade. Você pode escalar seu cluster Couchbase para cima ou para baixo com base na demanda, sem precisar gerenciar hardware físico, para acomodar facilmente volumes de dados flutuantes e uso de aplicativos. AWS fornece:

- Opções de escala vertical e horizontal
- Capacidades de implantação global
- Balanceamento de carga em todo Regiões da AWS
- Soluções de escalabilidade de banco de dados
- Otimização da entrega de conteúdo

Otimização do desempenho. AWS fornece uma infraestrutura de rede de alto desempenho e tipos de instância otimizados para garantir acesso rápido aos dados e baixa latência para seu banco de dados Couchbase.

- Opções de computação de alto desempenho (HPC)
- Entrega global de conteúdo pela Amazon CloudFront
- Várias opções de armazenamento
- Serviços avançados de banco de dados, incluindo Amazon Relational Database Service (Amazon RDS) e Amazon DynamoDB
- Conexões de baixa latência com AWS Direct Connect

Otimização de custo. Selecione o tipo de instância e a configuração apropriados para equilibrar desempenho e custo com base em sua carga de trabalho. Pague somente pelos recursos que você usa. Isso pode reduzir potencialmente seus custos operacionais, eliminando a necessidade de gerenciar hardware local e aproveitando Nuvem AWS as economias de escala.

- As instâncias reservadas podem ajudá-lo a planejar com antecedência e reduzir substancialmente seus custos ao usar o Couchbase on. AWS
- O escalonamento automático evita o provisionamento excessivo e ajuda você a otimizar sua utilização e eficiência de custos.

Segurança aprimorada. Beneficie-se dos recursos de segurança robustos AWS, como criptografia de dados, controles de acesso e grupos de segurança, para ajudar a proteger os dados confidenciais que você armazena no Couchbase. Benefícios adicionais:

- O Modelo de Responsabilidade AWS Compartilhada diferencia claramente entre a segurança da nuvem (AWS responsabilidade) e a segurança na nuvem (responsabilidade do cliente).
- AWS a conformidade suporta os principais padrões de segurança.

- AWS fornece opções avançadas de criptografia.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar o acesso seguro aos seus recursos.

Gerenciamento simplificado. AWS fornece serviços gerenciados para o Couchbase, para que você possa se concentrar no desenvolvimento de aplicativos em vez de gerenciar a infraestrutura subjacente.

Alcance global. Você pode implantar seu cluster Couchbase em vários Regiões da AWS para obter baixa latência para usuários em todo o mundo. Você pode implantar seus bancos de dados inteiramente na nuvem ou em um ambiente híbrido. Você pode proteger seus dados com segurança integrada de nível corporativo e sincronização bidirecional rápida e eficiente dos dados da borda até a nuvem. Ao mesmo tempo, você pode simplificar o desenvolvimento com um modelo de programação consistente para criar aplicativos web e móveis.

Continuidade de negócios:

- Backup e recuperação de dados. Em caso de problema, você pode usar AWS Backuppara garantir a resiliência dos dados e a fácil recuperação. Para opções de recuperação de desastres, consulte a documentação do AWS Well-Architected Framework.
- Implantação multirregional do Couchbase: Para implantar um banco de dados do Couchbase em um AWS ambiente multirregional, você pode assinar o Couchbase Server em, usar AWS CloudFormationmodelos para criar clusters separados do Couchbase em cada região e AWS Marketplace, em seguida, configurar a replicação entre regiões para sincronizar dados entre regiões. Essa configuração garante alta disponibilidade e redundância geográfica em várias regiões. Para obter mais informações, consulte Implantar o Couchbase Server usando AWS Marketplace na documentação do Couchbase.

Agilidade da infraestrutura:

- Provisionamento e desprovisionamento rápidos de recursos
- Alcance da infraestrutura global
- Dimensionamento automático com base na demanda
- Infraestrutura como Código (IaC) para implantações consistentes
- Vários tipos de instância otimizados para cargas de trabalho diferentes

Capacitação da inovação:

- Acesso às tecnologias mais recentes, incluindo IA/ML, IoT e análises
- Serviços gerenciados, que reduzem a sobrecarga operacional
- Práticas modernas de desenvolvimento de aplicativos
- Opções de computação sem servidor

Excelência operacional:

- Monitoramento e registro centralizados
- Gerenciamento automatizado de recursos
- Capacidades de manutenção preditiva
- Visibilidade aprimorada do uso de recursos
- Processos de implantação simplificados

Oportunidades de modernização:

- Arquitetura de microsserviços
- DevOpsimplementação de práticas
- Desenvolvimento de aplicativos nativos em nuvem
- Modernização de aplicativos antigos

Vantagens competitivas:

- Tempo de comercialização mais rápido
- Experiência aprimorada do cliente
- Tomada de decisão baseada em dados
- Inteligência de negócios aprimorada

Migre o Db2 for LUW para a Amazon EC2 usando o envio de registros para reduzir o tempo de interrupção

Criado por Feng Cai (AWS), Ambarish Satarkar (AWS) e Saurabh Sharma (AWS)

Resumo

Quando os clientes migram suas cargas de trabalho do IBM Db2 for LUW (Linux, UNIX e Windows) para a Amazon Web Services (AWS), usar o Amazon Elastic Compute Cloud (Amazon) com o modelo Bring Your Own License (BYOL EC2) é a maneira mais rápida. No entanto, migrar grandes quantidades de dados do Db2 local para a AWS pode ser um desafio, especialmente quando a janela de interrupção é curta. Muitos clientes tentam definir a janela de interrupção para menos de 30 minutos, o que deixa pouco tempo para o banco de dados em si.

Esse padrão aborda como realizar uma migração do Db2 com uma pequena janela de interrupção usando o envio do log de transações. Essa abordagem se aplica ao Db2 em uma plataforma Linux little-endian.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância do Db2 em execução em uma EC2 instância que corresponde aos layouts do sistema de arquivos local
- Um bucket do Amazon Simple Storage Service (Amazon S3) acessível à instância EC2
- Uma política e uma função do AWS Identity and Access Management (IAM) para fazer chamadas programáticas para o Amazon S3
- Fuso horário e relógios do sistema sincronizados na Amazon EC2 e no servidor local
- A rede local conectada à AWS por meio do AWS Site-to-SiteVPN ou do AWS Direct Connect

Limitações

- A instância local do Db2 e a Amazon EC2 devem estar na mesma família de plataformas.
- O workload on-premises do Db2 deve ser registrado. Defina `blocknonlogged=yes` na configuração do banco de dados para bloquear qualquer transação não registrada.

Versões do produto

- Db2 for LUW versão 11.5.9 e posterior

Arquitetura

Pilha de tecnologia de origem

- Db2 em Linux x86_64

Pilha de tecnologias de destino

- Amazon EBS
- Amazon EC2
- AWS Identity and Access Management (IAM)
- Amazon S3
- AWS Site-to-Site VPN ou Direct Connect

Arquitetura de destino

O diagrama a seguir mostra uma instância do Db2 em execução local com uma conexão de rede privada virtual (VPN) com o Db2 na Amazon. EC2 As linhas pontilhadas representam o túnel VPN entre seu datacenter e a nuvem AWS.

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O AWS Direct Connect conecta sua rede interna a um local do Direct Connect por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para serviços públicos da AWS, ignorando provedores de serviço da internet no caminho da sua rede.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (Amazon). EC2

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Site-to-Site VPN ajuda você a transmitir tráfego entre instâncias que você executa na AWS e sua própria rede remota.

Outras ferramentas

- db2cli é o comando da CLI interativa do Db2.

Práticas recomendadas

- No banco de dados de destino, use endpoints de gateway para o Amazon S3 para acessar a imagem de backup do banco de dados e os arquivos de log no Amazon S3.
- No banco de dados de origem, use a AWS PrivateLink para o Amazon S3 para enviar a imagem de backup do banco de dados e os arquivos de log para o Amazon S3.

Épicos

Definição de variáveis de ambiente

Tarefa	Descrição	Habilidades necessárias
Definição de variáveis de ambiente.	Seu nome usa o padrão a seguir. • Nome da instância: `db2inst1` • Nome do banco de dados: `SAMPLE`	DBA

Tarefa	Descrição	Habilidades necessárias
	Você pode alterá-los para se adequarem ao seu ambiente.	

Configurar o servidor Db2 on-premises

Tarefa	Descrição	Habilidades necessárias

Configure a CLI da AWS.	Para baixar e instalar a versão mais recente da AWS CLI, execute os seguintes comandos:
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Administrador do Linux

Configure um destino local para os logs de arquivamento do Db2.	Para manter o banco de dados de destino EC2 na Amazon sincronizado com o banco de dados de origem local, os registros de transações mais recentes precisam ser recuperados da fonte. Nesta configuração, `/db2logs` é definido por `LOGARCHMETH2` na fonte como uma área de preparação. Os registros arquivados nesse diretório serão sincronizados com o Amazon S3	DBA

Tarefa	Descrição	Habilidades necessárias

	e acessados pelo Db2 na Amazon. EC2 O padrão é usado `LOGARCHMETH2` porque `LOGARCHMETH1` pode ter sido configurado para usar uma ferramenta de um fornecedor terceiriz ado que o comando da AWS CLI não pode acessar. Para recuperar os registros, execute o seguinte comando:
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	

Execute um backup de banco de dados on-line.	Execute um backup de banco de dados on-line e salve-o no sistema de arquivos de backup local: `db2 backup db sample online to /backup`	DBA

Configurar o bucket do S3 e a política do IAM

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Crie um bucket S3 para o servidor on-premises para enviar as imagens de backup do Db2 e os arquivos de log para a AWS. O bucket	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	também será acessado pela Amazon EC2: `aws s3api create-bucket --bucket logshipmig-db2 --region us-east-1`	

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM.	O `db2bucket.json` arquivo contém a política do IAM para acessar o bucket do Amazon S3: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts" ], "Resource": [`	Administrador da AWS, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>"arn:aws:s3:::logshipmig-db2/*",
	
	"arn:aws:s3:::logshipmig-db2"
	]
	}
	]
	}</pre>
	Para criar a política, use o seguinte comando da AWS CLI:
	<pre>aws iam create-policy \
	--policy-name db2s3policy \
	--policy-document file://db2bucket.json</pre>
	A saída JSON mostra o Amazon Resource Name (ARN) da política, `aws_account_id` onde representa o ID da sua conta:
	<pre>"Arn": "arn:aws:iam::aws_account_id:policy/db2s3policy"</pre>	

Tarefa	Descrição	Habilidades necessárias
Anexe a política do IAM à função do IAM usada pela EC2 instância.	Na maioria dos ambientes da AWS, uma EC2 instância em execução tem uma função do IAM definida pelo administr ador do sistema. Se a função do IAM não estiver definida, crie a função e escolha Modificar função do IAM no EC2 console para associar a função à EC2 instância que hospeda o banco de dados Db2. Anexe a política do IAM à função do IAM com o ARN da política: `aws iam attach-role-policy \ --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3policy" \ --role-name db2s3role` Depois que a política for anexada, qualquer EC2 instância associada à função do IAM poderá acessar o bucket do S3.	Administrador da AWS, administrador de sistemas da AWS

Envie a imagem de backup e os arquivos de log do banco de dados de origem para o Amazon S3

Tarefa	Descrição	Habilidades necessárias

Configure a AWS CLI no servidor Db2 local.	Configure a AWS CLI com o `Access Key ID` e `Secret Access Key` gerado na etapa anterior:
	`$ aws configure`
	`AWS Access Key ID`
	`[None]: **********`
	`AWS Secret Access Key`
	`[None]: **********`
	`Default region name`
	`[None]: us-east-1`
	`Default output format`
	`[None]: json`
		Administrador da AWS, administrador de sistemas da AWS

Envie a imagem de backup para o Amazon S3.	Anteriormente, um backup de banco de dados on-line foi salvo no diretório local `/backup`. Para enviar essa imagem de backup para o bucket do S3, execute o seguinte comando: `aws s3 sync /backup s3://logshipmig-db2/SAMPLE_backup`	Administrador da AWS, engenheiro de migração
Envie os logs do Db2 para o Amazon S3.	Sincronize os registros do arquivamento local do Db2 com o bucket do S3 que pode ser acessado pela instância do Db2 de destino na Amazon: EC2	Administrador da AWS, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	`aws s3 sync /db2logs s3://logshipmig-db2/SAMPLE_LOG` Execute esse comando periodicamente usando o cron ou outras ferramentas de agendamento. A frequência depende da frequência com que o banco de dados de origem arquiva os arquivos de log de transações.	

Conecte o Db2 na Amazon EC2 ao Amazon S3 e inicie a sincronização do banco de dados

Tarefa	Descrição	Habilidades necessárias

Crie um repositório de PKCS12 chaves.	O Db2 usa um repositório de chaves de criptografia de chave pública (PKCS) para manter a chave de acesso da AWS segura. Crie um keystore e configure a instância Db2 de origem para usá-lo:
	
	`gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`
	
	`db2 "update dbm cfg using keystore_location /home/db2`
		DBA

Tarefa	Descrição	Habilidades necessárias
	`inst1/.keystore/db2s3.p12 keystore_type pkcs12"`	

Crie o alias de acesso ao armazenamento do Db2.	Para criar o alias de acesso ao armazenamento, use a seguinte sintaxe de script:
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"`
	Por exemplo, seu script pode ter a seguinte aparência:
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'logshipmig-db2'"`
		DBA

Tarefa	Descrição	Habilidades necessárias
Defina a área de espera.	Por padrão, o Db2 usa `DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH` como área de preparação para carregar e baixar arquivos de e para o Amazon S3. O caminho padrão está `sqllib/tmp/RemoteStorage.xxxx` no diretório inicial da instância, com `xxxx` referência ao número da partição Db2. Observe que a área de preparação deve ter capacidade suficiente para armazenar as imagens de backup e os arquivos de log. Você pode usar o registro para apontar a área de preparação para um diretório diferente. Também recomendamos usar`DB2_ENABLE_COS_SDK=ON` ,`DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` , e o link para a `awssdk` biblioteca para ignorar a área de armazenamento do Amazon S3 para backup e restauração do banco de dados: `#By root:`	DBA

Tarefa	Descrição	Habilidades necessárias

	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`Db2set DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore`
	`db2stop`
	`db2start`	

Restaure o banco de dados a partir da imagem de backup.	Restaure o banco de dados de destino na Amazon a EC2 partir da imagem de backup no bucket do S3: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup replace existing`	DBA

Tarefa	Descrição	Habilidades necessárias

Avance o banco de dados.	Depois que a restauração for concluída, o banco de dados de destino será colocado no estado pendente de rollforwa rd. Configure `LOGARCHME TH1` e `LOGARCHMETH2` para que o Db2 saiba onde obter os arquivos de log de transações:
	`db2 update db cfg for SAMPLE using LOGARCHME TH1 'DB2REMOTE://DB2AW SS3//SAMPLE_LOGS/'`
	`db2 update db cfg for SAMPLE using LOGARCHME TH2 OFF`
	Inicie o rollforward do banco de dados:
	`db2 ROLLFORWARD DATABASE sample to END OF LOGS`
	Esse comando processa todos os arquivos de log que foram transferidos para o bucket do S3. Execute-o periodica mente com base na frequênci a do `s3 sync` comando nos servidores Db2 on-premises. Por exemplo, se for `s3 sync` executado a cada hora e levar 10 minutos para sincroniz ar todos os arquivos de log, defina o comando para ser
		DBA

Tarefa	Descrição	Habilidades necessárias
	executado 10 minutos após cada hora.	

Coloque o Db2 na Amazon EC2 on-line durante a janela de transição

Tarefa	Descrição	Habilidades necessárias

Coloque o banco de dados de destino on-line.	Na janela de substituição, siga um destes procedimentos:
	• Coloque o banco de dados on-premises em `ADMIN MODE` e execute o comando `s3 sync` para forçar o arquivamento do último log de transações.
	• Encerre o banco de dados.
	
	Depois que o último registro de transações for sincronizado com o Amazon S3, execute `ROLLFORWARD` o comando pela última vez:
	
	`db2 rollforward DB sample to END OF LOGS`
	`db2 rollforward DB sample complete`
	
	`Rollforward Status`
	`....`
	`Rollforward status = not pending`
		DBA

Tarefa	Descrição	Habilidades necessárias

	`....`
	`DB20000I  The ROLLFORWARD command completed successfully.`
	
	`db2 activate db sample`
	`DB20000I  The ACTIVATE DATABASE command completed successfully.`
	
	Coloque o banco de dados de destino on-line e direcione as conexões do aplicativo para o Db2 na Amazon EC2.	

Solução de problemas

Problema	Solução
Se vários bancos de dados tiverem o mesmo nome de instância e nome de banco de dados em hosts diferentes (DEV, QA, PROD), os backups e os logs poderão ir para o mesmo subdiretório.	Use diferentes buckets do S3 para DEV, QA e PROD e adicione o nome do host como prefixo do subdiretório para evitar confusão.
Se houver várias imagens de backup no mesmo local, você receberá o seguinte erro ao restaurar: `SQL2522N More than one backup file matches the time stamp value provided for the backed up database image.`	No `restore` comando, adicione o timestamp do backup: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup taken at 20230628164042 replace existing`

Recursos relacionados

- Operações de backup e restauração do Db2 entre diferentes sistemas operacionais e plataformas de hardware
- Configurar Db2 STORAGE ACCESS ALIAS e REMOTE DB2
- Comando Db2 ROLLFORWARD
- Método de arquivamento de log secundário do Db2

Migre o Db2 for LUW para a Amazon EC2 com recuperação de desastres de alta disponibilidade

Criado por Feng Cai (AWS), Aruna Gangireddy (AWS) e Venkatesan Govindan (AWS)

Resumo

Quando os clientes migram sua carga de trabalho do IBM Db2 LUW (Linux, UNIX e Windows) para a Amazon Web Services (AWS), usar o Amazon Elastic Compute Cloud (Amazon) com o modelo Bring Your Own License (BYOL EC2) é a maneira mais rápida. No entanto, migrar grandes quantidades de dados do Db2 local para a AWS pode ser um desafio, especialmente quando a janela de interrupção é curta. Muitos clientes tentam definir a janela de interrupção para menos de 30 minutos, o que deixa pouco tempo para o banco de dados em si.

Esse padrão aborda como realizar uma migração do Db2 com uma pequena janela de interrupção usando a recuperação de desastres de alta disponibilidade (HADR) do Db2. Essa abordagem se aplica aos bancos de dados Db2 que estão na plataforma Linux little-endian e não estão usando o Atributo de Particionamento de Dados (DPF - Data Partitioning Feature).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância do Db2 em execução em uma EC2 instância da Amazon que corresponde aos layouts do sistema de arquivos local
- Um bucket do Amazon Simple Storage Service (Amazon S3) acessível à instância EC2
- Uma política e uma função do AWS Identity and Access Management (IAM) para fazer chamadas programáticas para o Amazon S3
- Fuso horário e relógios do sistema sincronizados na Amazon EC2 e no servidor local
- A rede local conectada à AWS por meio do AWS Site-to-SiteVPN ou do AWS Direct Connect
- Comunicação entre o servidor local e a Amazon EC2 em portas HADR

Limitações

- A instância local do Db2 e a Amazon EC2 devem estar na mesma família de plataformas.
- O HADR não é suportado em um ambiente de banco de dados particionado.

- O HADR não suporta o uso de E/S bruta (acesso direto ao disco) para arquivos de log do banco de dados.
- O HADR não é compatível com registro infinito.
- `LOGINDEXBUILD` deve ser definido como `YES`, o que aumentará o uso do log para reconstruir o índice.
- O workload on-premises do Db2 deve ser registrado. Defina `blocknonlogged=yes` na configuração do banco de dados para bloquear qualquer transação não registrada.

Versões do produto

- Db2 for LUW versão 11.5.9 e posterior

Arquitetura

Pilha de tecnologia de origem

- Db2 em Linux x86_64

Pilha de tecnologias de destino

- Amazon EC2
- AWS Identity and Access Management (IAM)
- Amazon S3
- Site-to-SiteVPN AWS

Arquitetura de destino

No diagrama a seguir, o Db2 on-premises está sendo executado em `db2-server1` como principal. Ele tem dois alvos de espera do HADR. Um alvo em espera está on-premises e é opcional. O outro alvo de espera,`db2-ec2`, está na Amazon EC2. Depois que o banco de dados é transferido para a AWS, `db2-ec2` ele se torna o principal.

1. Os registros são transmitidos do banco de dados on-premises primário para o banco de dados on-premises em espera.

2. Usando o Db2 HADR, os registros são transmitidos do banco de dados local principal por meio de Site-to-Site VPN para o Db2 na Amazon. EC2
3. Os registros de backup e arquivamento do Db2 são enviados do banco de dados on-premises principal para o bucket do S3 na AWS.

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O AWS Direct Connect conecta sua rede interna a um local do Direct Connect por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para serviços públicos da AWS, ignorando provedores de serviço da internet no caminho da sua rede.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Site-to-Site VPN ajuda você a transmitir tráfego entre instâncias que você executa na AWS e sua própria rede remota.

Outras ferramentas

- db2cli é o comando da CLI interativa do Db2.

Práticas recomendadas

- No banco de dados de destino, use endpoints de gateway para o Amazon S3 para acessar a imagem de backup do banco de dados e os arquivos de log no Amazon S3.
- No banco de dados de origem, use a AWS PrivateLink para o Amazon S3 para enviar a imagem de backup do banco de dados e os arquivos de log para o Amazon S3.

Épicos

Definição de variáveis de ambiente

Tarefa	Descrição	Habilidades necessárias
Definição de variáveis de ambiente.	Esse padrão usa os seguintes nomes e portas: 1. Nome do host on-premises do Db2: `db2-server1` 2. Nome do host em espera do HADR: `db2-server2` (se o HADR estiver atualmente em execução on-premises) 3. EC2 Nome do host da Amazon: `db2-ec2` 4. Nome da instância: `db2inst1` 5. Nome do banco de dados: `SAMPLE` 6. Portas HADR: • `db2-server1: 50010` • `db2-server2: 50011` • `db2-ec2: 50012` Você pode alterá-los para se adequarem ao seu ambiente.	DBA

Configurar o servidor Db2 on-premises

Tarefa	Descrição	Habilidades necessárias

Configurar a AWS CLI	Para baixar e instalar a versão mais recente da AWS CLI, execute os seguintes comandos:
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Administrador do Linux

Configure um destino local para os logs de arquivamento do Db2.	Condições como trabalhos pesados de atualização em lote e lentidão na rede podem fazer com que o servidor em espera do HADR tenha um atraso. Para se atualizar, o servidor em espera precisa dos registros de transações do servidor primário. A sequência de locais para solicitar registros é a seguinte: • O diretório de log ativo no servidor primário • A localização `LOGARCHMETH1` ou `LOGARCHMETH2` no servidor em espera • A localização `LOGARCHMETH1` ou `LOGARCHMETH2` no servidor primário	DBA

Tarefa	Descrição	Habilidades necessárias

	Nesta configuração, `/db2logs` é definido por `LOGARCHMETH2` na fonte como uma área de preparação. Os registros arquivados nesse diretório serão sincronizados com o Amazon S3 e acessados pelo Db2 na Amazon. EC2 O padrão é usado `LOGARCHMETH2` porque `LOGARCHMETH1` pode ter sido configurado para usar uma ferramenta de um fornecedor terceirizado que o comando da AWS CLI não pode acessar:
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	

Execute um backup de banco de dados on-line.	Execute um backup de banco de dados on-line e salve-o no sistema de arquivos de backup local: `db2 backup db sample online to /backup`	DBA

Configurar o bucket do S3 e a política do IAM

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Crie um bucket S3 para o servidor on-premises para enviar as imagens de backup do Db2 e os arquivos de log para a AWS. O bucket será acessado pela Amazon EC2: `aws s3api create-bucket --bucket hadrmig-db2 --region us-east-1`	Administrador da AWS
Crie uma política do IAM.	O `db2bucket.json` arquivo contém a política do IAM para acessar o bucket do S3: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket",`	Administrador da AWS, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>"s3:DeleteObject",
	
	"s3:GetObjectVersion",
	
	"s3:ListMultipartUploadParts"
	],
	"Resource":
	[
	
	"arn:aws:s3:::hadrmig-db2/*",
	
	"arn:aws:s3:::hadrmig-db2"
	]
	}
	]
	}</pre>
	Para criar a política, use o seguinte comando da AWS CLI:
	<pre>aws iam create-policy \
	--policy-name
	db2s3hapolicy \
	--policy-document
	file://db2bucket.json</pre>
	A saída JSON mostra o Amazon Resource Name (ARN) da política, `aws_account_id` onde representa o ID da sua conta:	

Tarefa	Descrição	Habilidades necessárias
	`"Arn": "arn:aws:iam::aws_account_id:policy/db2s3hapolicy"`	
Anexe a política do IAM à função do IAM.	Normalmente, a EC2 instância com o Db2 em execução teria uma função do IAM atribuída pelo administrador do sistema. Se nenhuma função do IAM for atribuída, você poderá escolher Modificar função do IAM no EC2 console da Amazon. Anexe a política do IAM à função do IAM associada à EC2 instância. Depois que a política for anexada, a EC2 instância poderá acessar o bucket do S3: `aws iam attach-role-policy --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3hapolicy" --role-name db2s3harole`	

Envie a imagem de backup e os arquivos de log do banco de dados de origem para o Amazon S3

Tarefa	Descrição	Habilidades necessárias

Configure a AWS CLI no servidor Db2 on-premises.	Configure o AWS CLI com o `Access Key ID` e `Secret Access Key` que você gerou anteriormente:
	`$ aws configure`
	`AWS Access Key ID [None]: **********`
	`AWS Secret Access Key [None]: ********** **********`
	`Default region name [None]: us-east-1`
	`Default output format [None]: json`
		Administrador da AWS, administrador de sistemas da AWS

Envie a imagem de backup para o Amazon S3.	Anteriormente, um backup de banco de dados on-line foi salvo no diretório local `/backup`. Para enviar essa imagem de backup para o bucket do S3, execute o seguinte comando: `aws s3 sync /backup s3://hadrmig-db2/SAMPLE_backup`	Administrador da AWS, administrador de sistemas da AWS
Envie os logs do Db2 para o Amazon S3.	Sincronize os registros do arquivo Db2 local com o bucket do Amazon S3 que pode ser acessado pela instância do Db2 de destino na Amazon: EC2	

Tarefa	Descrição	Habilidades necessárias
	`aws s3 sync /db2logs s3://hadrmig-db2/SAMPLE_LOGS` Execute esse comando periodicamente usando o cron ou outras ferramentas de agendamento. A frequência depende da frequência com que o banco de dados de origem arquiva os arquivos de log de transações.	

Conecte o Db2 na Amazon EC2 ao Amazon S3 e inicie a sincronização inicial do banco de dados

Tarefa	Descrição	Habilidades necessárias

Crie um armazenamento de PKCS12 chaves.	O Db2 usa um repositório de chaves de criptografia de chave pública (PKCS) para manter a chave de acesso da AWS segura. Crie um keystore e configure o Db2 de origem para usá-lo:
	
	`gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`
	
	`db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db`
		DBA

Tarefa	Descrição	Habilidades necessárias
	`2s3.p12 keystore_type pkcs12"`	

Crie o alias de acesso ao armazenamento do Db2.	O Db2 usa um alias de acesso ao armazenamento para acessar o Amazon S3 diretamente com os comandos `INGEST`, `LOAD`, `BACKUP DATABASE`, ou `RESTORE DATABASE`.
	
	Como você atribuiu uma função do IAM à EC2 instância `USER` e `PASSWORD` não é necessário:
	
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"`
	
	Por exemplo, seu script pode ter a seguinte aparência:
	
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'hadrmig-db2'"`
		DBA

Tarefa	Descrição	Habilidades necessárias

Defina a área de espera.	Recomendamos usar `DB2_ENABLE_COS_SDK=ON DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` , e o link para a `awssdk` biblioteca para ignorar a área de armazenamento do Amazon S3 para backup e restauração do banco de dados:
	
	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2stop`
	`db2start`
		DBA

Tarefa	Descrição	Habilidades necessárias

Restaure o banco de dados a partir da imagem de backup.	Restaure o banco de dados de destino na Amazon a EC2 partir da imagem de backup no bucket do S3:
	
	`db2 create db sample on /data1`
	`db2 restore db sample from DB2REMOTE://DB2AWSS3/hadrmig-db2/SAMPLE_backup replace existing`
		DBA

Configure o HADR sem o HADR on-premises

Tarefa	Descrição	Habilidades necessárias
Configure o servidor Db2 on-premises como principal.	Atualize as configurações do banco de dados para HADR on `db2-server1` (a fonte on-premises) como principal . `HADR_SYNCMODE` Defina para o `SUPERASYNC` modo, que tem o menor tempo de resposta da transação: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-server1 HADR_LOCAL_SVC 50010 HADR_REMOTE_HOST db2-ec2 HADR_REMOTE_SVC 50012 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE`	DBA

Tarefa	Descrição	Habilidades necessárias
	`SUPERASYNC DB20000 I The UPDATE DATABASE CONFIGURATION command completed successfu lly` Alguns atrasos de rede entre o datacenter on-premises e a AWS são esperados. (É possível definir um valor `HADR_SYNCMODE` diferente com base na confiabilidade da rede. Para obter mais informações, consulte a seção Recursos relacionados).	
Altere o destino do arquivamento do log do banco de dados de destino.	Altere o destino do arquivo de log do banco de dados de destino para corresponder ao EC2 ambiente da Amazon: `db2 update db cfg for SAMPLE using LOGARCHMETH1 'DB2REMOTE://DB2AWSS3//SAMPLE_LOGS/' LOGARCHMETH2 OFF DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully`	DBA

Tarefa	Descrição	Habilidades necessárias
Configure o HADR para Db2 no servidor Amazon EC2 .	Atualize a configuração do banco de dados para HADR em `db2-ec2` espera: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully`	DBA

Tarefa	Descrição	Habilidades necessárias

Verifique a configuração do HADR.	Verifique os parâmetros do HADR nos servidores Db2 de origem e de destino.
	
	Para verificar a configuração ativada`db2-server1`, execute o seguinte comando:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = PRIMARY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-server1`
	`HADR local service name (HADR_LOCAL_SVC) = 50010`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-ec2`
	`HADR remote service name (HADR_REMOTE_SVC) = 50012`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) =`
	`HADR log write synchronization mode`
		DBA

Tarefa	Descrição	Habilidades necessárias

	(HADR_SYNCMODE) = NEARSYNC
	HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000)
	HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0
	HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0
	HADR SSL certificate label (HADR_SSL_LABEL) =
	HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF
	
	Para verificar a configuração ativada`db2-ec2`, execute o seguinte comando:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = STANDBY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-ec2`
	`HADR local service name (HADR_LOCAL_SVC) = 50012`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server1`	

Tarefa	Descrição	Habilidades necessárias
	HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TARGET_LIST) = HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Os parâmetros `HADR_LOCAL_HOST`, `HADR_LOCAL_SVC`, `HADR_REMOTE_HOST`, e `HADR_REMO`	

Tarefa	Descrição	Habilidades necessárias
	TE_SVC indicam uma configuração de HADR primária e uma de espera.	

Inicie a instância Db2 HADR.	Inicie primeiro a instância Db2 HADR no servidor em espera: db2-ec2
	
	`db2 start hadr on db sample as standby`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	
	Inicie o Db2 HADR no servidor primário (de origem): db2-server1
	
	`db2 start hadr on db sample as primary`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	
	A conexão HADR entre o Db2 no local e na Amazon agora EC2 foi estabelecida com sucesso. O servidor primário do Db2 db2-server1 começa a transmitir os registros do log de transações db2-ec2 em tempo real.
		DBA

Configure o HADR quando o HADR existir on-premises

Tarefa	Descrição	Habilidades necessárias
Adicione o Db2 na Amazon EC2 como um modo de espera auxiliar.	Se o HADR estiver em execução na instância local do Db2, você poderá adicionar o Db2 na EC2 Amazon como um modo de espera auxiliar `HADR_TARGET_LIST` usando a execução dos seguintes comandos em: `db2-ec2` `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. db2 update db cfg for sample using HADR_TARGET_LIST "db2-server1:50010|db2-server2:50011" DB20000I The UPDATE DATABASE CONFIGURATION command`	DBA

Tarefa	Descrição	Habilidades necessárias
	`completed successfully.`	

Tarefa	Descrição	Habilidades necessárias
Adicione as informações auxiliares de espera aos servidores on-premises.	Atualização de `HADR_TARGET_LIST` nos dois servidores on-premises (primário e em espera). `db2-server1` Ativado, execute o seguinte código: `db2 update db cfg for sample using HADR_TARGET_LIST "db2-server2:50011|db2-ec2:50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`  `db2-server2` Ativado, execute o seguinte código:  `db2 update db cfg for sample using HADR_TARG`	DBA

Tarefa	Descrição	Habilidades necessárias
	ET_LIST "db2-serv er1:50010|db2-ec2: 50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfu lly. SQL1363W One or more of the parameter s submitted for immediate modificat ion were not changed dynamically. For these configura tion parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.	

Tarefa	Descrição	Habilidades necessárias

Verifique a configuração do HADR.	Verifique os parâmetros do HADR nos servidores Db2 de origem e de destino.
	
	`db2-server1` Ativado, execute o seguinte código:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = PRIMARY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-server1`
	`HADR local service name (HADR_LOCAL_SVC) = 50010`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server2`
	`HADR remote service name (HADR_REMOTE_SVC) = 50011`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server2:50011|db2-ec2:50012`	

Tarefa	Descrição	Habilidades necessárias
	HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF `db2-server2` Ativado, execute o seguinte código: `db2 get db cfg for sample|grep HADR` HADR database role = STANDBY HADR local host name (HADR_LOCAL_HOST) = db2-server2 HADR local service name (HADR_LOCAL_SVC) = 50011 HADR remote host name (HADR_REMOTE_HOST) = db2-server1	

Tarefa	Descrição	Habilidades necessárias
	``` HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TAR GET_LIST) = db2-serve r1:50010|db2-ec2:5 0012 HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REP LAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certifica te label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF ``` db2-ec2Ativado, execute o seguinte código:	

Tarefa	Descrição	Habilidades necessárias

	`db2 get db cfg for sample|grep HADR`
	`HADR database role = STANDBY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-ec2`
	`HADR local service name (HADR_LOCAL_SVC) = 50012`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server1`
	`HADR remote service name (HADR_REMOTE_SVC) = 50010`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server1:50010|db2-server2:50011`
	`HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC`
	`HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000)`	

Tarefa	Descrição	Habilidades necessárias
	HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Os parâmetros HADR_LOCAL_HOST , HADR_LOCAL_SVC , HADR_REMOTE_HOST , HADR_REMOTE_SVC , e HADR_TARGET_LIST indicam a configuração de um HADR primário e dois em espera.	

Tarefa	Descrição	Habilidades necessárias

Pare e inicie o Db2 HADR.	`HADR_TARGET_LIST` agora está configurado em todos os três servidores. Cada servidor Db2 está ciente dos outros dois. Pare e reinicie o HADR (breve interrupção) para aproveitar a nova configura ção.
	
	`db2-server1` Ativado, execute os seguintes comandos:
	
	`db2 stop hadr on db sample`
	`db2 deactivate db sample`
	`db2 activate db sample`
	
	`db2-server2` Ativado, execute os seguintes comandos:
	
	`db2 deactivate db sample`
	`db2 start hadr on db sample as standby`
	`SQL1766W The command completed successfully`
	
	`db2-ec2`Ativado, execute os seguintes comandos:
	
	`db2 start hadr on db sample as standby`
		DBA

Tarefa	Descrição	Habilidades necessárias

	`SQL1766W The command completed successfully`
	
	`db2-server1` Ativado, execute os seguintes comandos:
	
	`db2 start hadr on db sample as primary`
	`SQL1766W The command completed successfully`
	
	A conexão HADR entre o Db2 no local e na Amazon EC2 agora foi estabelecida com sucesso. O servidor primário do Db2 `db2-server1` começa a transmitir registros de log de transações para `db2-server2` e `db2-ec2` em tempo real.	

Torne o Db2 na Amazon EC2 como principal durante a janela de transição

Tarefa	Descrição	Habilidades necessárias
Garanta que não haja atraso de HADR no servidor em espera.	Verifique o status do HADR no servidor primário `db2-server1`. Não se assuste quando `HADR_STATE` estiver no status`REMOTE_CATCHUP`, o que é normal quando `HADR_SYNCMODE` está definido como `SUPERASYNC`. O `PRIMARY_LOG_TIME`	DBA

Tarefa	Descrição	Habilidades necessárias

	e STANDBY_REPLAY_LOG _TIME mostra que eles estão sincronizados:
	
	`db2pd -hadr -db sample`
	
	`HADR_ROLE = PRIMARY`
	
	`REPLAY_TYPE = PHYSICAL`
	
	`HADR_SYNCMODE = SUPERASYNC`
	
	`STANDBY_ID = 2`
	
	`LOG_STREAM_ID = 0`
	
	`HADR_STATE = REMOTE_CATCHUP`
	`.....`
	
	`PRIMARY_LOG_TIME = 10/26/2022 02:11:32. 000000 (1666750292)`
	
	`STANDBY_LOG_TIME = 10/26/2022 02:11:32. 000000 (1666750292)`
	`STANDBY_R EPLAY_LOG_TIME = 10/26/2022 02:11:32. 000000 (1666750292)`	

Tarefa	Descrição	Habilidades necessárias

Execute a aquisição da HADR.	Para concluir a migração, torne `db2-ec2` o banco de dados primário executando o comando HADR takeover. Use o comando db2pd para verificar o `HADR_ROLE` valor:
	
	`db2 TAKEOVER HADR ON DATABASE sample`
	`DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.`
	
	`db2pd -hadr -db sample`
	`Database Member 0 -- Database SAMPLE -- Active -- Up 0 days 00:03:25 -- Date 2022-10-26-02.46.45.048988`
	
	`HADR_ROLE = PRIMARY`
	`REPLAY_TYPE = PHYSICAL`
	
	Para concluir a migração para a AWS, aponte as conexões do aplicativo para o Db2 na Amazon EC2.	

Solução de problemas

Problema	Solução
Se você usa o NAT por motivos de firewall e segurança, o host pode ter dois endereços IP (um interno e outro externo), o que pode causar uma falha na verificação do endereço IP do HADR. O `START HADR ON DATABASE` comando retornará a seguinte mensagem: `HADR_LOCAL_HOST:HADR_LOCAL_SVC (-xx-xx-xx-xx.:50011 (xx.xx.xx .xx:50011)) on remote database is different from HADR_REMOTE_HOST:H ADR_REMOTE_SVC (xx-xx-xx- xx.:50011 (x.x.x.x:50011)) on local database.`	Para oferecer suporte ao HADR em um ambiente NAT, você pode configurar `HADR_LOCAL_HOST` com o endereço interno e externo. Por exemplo, se o servidor Db2 tiver o nome interno `host1` e o nome externo`host1E`, `HADR_LOCAL_HOST` pode ser `HADR_LOCAL_HOST: "host1 | host1E"`.

Recursos relacionados

- Operações de backup e restauração do Db2 entre diferentes sistemas operacionais e plataformas de hardware
- Configurar Db2 STORAGE ACCESS ALIAS e REMOTE DB2
- Recuperação de desastres de alta disponibilidade do Db2
- hadr_syncmode – Modo de sincronização HADR para gravações de log no parâmetro de configuração de estado de mesmo nível

Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2 usando o Application Migration Service

Criado por Senthil Ramasamy (AWS)

Resumo

Esse padrão descreve as etapas para migrar um banco de dados Microsoft SQL Server de um data center local para uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Ele usa o AWS Application Migration Service (AWS MGN) para rehospedar seu banco de dados usando uma migração automatizada lift-and-shift. AWS O MGN executa a replicação em nível de bloco do seu servidor de banco de dados de origem.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um banco de dados Microsoft SQL Server de origem em um datacenter on-premises

Limitações

- A largura de banda da sua rede pode ser limitada entre o data center local e. AWS
- AWS O MGN está limitado a bancos de dados hospedados em servidores autônomos com armazenamento dedicado. Ele não suporta a migração de sistemas de banco de dados em cluster e sistemas de banco de dados em que a taxa de alteração excede a taxa de transferência de uma rede.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Versões do produto

- Todas as versões do banco de dados Microsoft SQL Server
- Sistemas operacionais Windows e Linux que suportam AWS MGN

Arquitetura

Pilha de tecnologia de origem

Um banco de dados Microsoft SQL Server on-premises

Pilha de tecnologias de destino

Um banco de dados Microsoft SQL Server em uma EC2 instância da Amazon

Arquitetura de destino

Essa arquitetura usa o AWS MGN para replicar dados de um data center corporativo local para. AWS O diagrama mostra o processo de replicação de dados, as comunicações da API e as fases de teste e transição.

1. Replicação de dados:
   - AWS A MGN replica dados do data center corporativo local AWS e inicia a replicação contínua das alterações.
   - Os servidores de replicação na sub-rede intermediária recebem e processam os dados.
2. Comunicação de API:
   - Os servidores de replicação se conectam aos AWS endpoints da API MGN EC2, Amazon e Amazon Simple Storage Service (Amazon S3) por meio da porta TCP 443.
   - AWS A MGN gerencia a migração.
   - A Amazon EC2 gerencia as operações da instância.
3. Teste e transição:
   - As instâncias de teste são iniciadas na sub-rede operacional usando dados replicados.
   - Após o teste bem-sucedido, o AWS MGN cria instâncias de transição para a migração final.

Ferramentas

- AWS Application Migration Service (AWS MGN) ajuda você a rehospedar (elevar e deslocar) aplicativos Nuvem AWS sem alterações e com o mínimo de tempo de inatividade.
- AWS Direct Connectconecta sua rede interna a um local do Direct Connect por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para AWS serviços públicos, ignorando os provedores de serviços de Internet em seu caminho de rede.

- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Práticas recomendadas

- Configure endpoints regionais de API para AWS MGN EC2, Amazon e Amazon S3 na nuvem privada virtual (VPC) para proibir o acesso público da Internet.
- Defina as configurações de inicialização do AWS MGN para iniciar servidores de banco de dados de destino em uma sub-rede privada.
- Permita somente as portas necessárias nos grupos de segurança do banco de dados.
- Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Configurar o AWS MGN

Tarefa	Descrição	Habilidades necessárias
Configure o AWS MGN.	Pesquise o AWS Application Migration Service no AWS Management Console e inicie o processo de configuração. Isso criará um modelo de replicação e o redirecionará para a página Servidores de origem do console MGN. Ao configurar o serviço MGN, escolha uma função de serviço na lista gerada.	DBA, Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Adicione o servidor de origem.	Adicione detalhes do seu servidor de banco de dados de origem local e, em seguida, adicione o servidor.	DBA, Engenheiro de migração
Instale o agente AWS MGN no servidor de origem.	Baixe o instalador do agente AWS MGN em seu sistema local e transfira o instalador para seu servidor de banco de dados de origem. Para validar o hash do instalador, consulte Validando o instalador do Agente de AWS Replicação baixado para Windows 2012.	DBA, Engenheiro de migração

Instale o agente AWS MGN nas máquinas de origem

Tarefa	Descrição	Habilidades necessárias
Gere credenciais do IAM do cliente.	Antes de instalar o agente AWS MGN, gere AWS credenciais criando um novo usuário do IAM com as permissões apropriadas. Para obter mais informações, consulte as políticas gerenciadas pela AWS AWS Application Migration Service e a geração das AWS credenciais necessárias.	DBA, Engenheiro de migração
Instale o agente no servidor de origem.	Instale o agente na máquina de origem que hospeda o banco de dados Microsoft	Proprietário do aplicativo, DBA, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	SQL Server. Para obter mais informações, consulte Instalando o Agente AWS de Replicação em servidores Windows. Forneça as seguintes credenciais da AWS: • Região da AWS • AWS ID da chave de acesso • AWS chave de acesso secreta Suas AWS credenciais exclusivas permitem que o agente da AWS MGN autentique e execute tarefas de migração.	

Tarefa	Descrição	Habilidades necessárias
Escolha discos para replicar.	Depois de inserir suas AWS credenciais, o instalador verifica se o servidor atende aos requisitos mínimos para a instalação do agente (por exemplo, se o servidor tem espaço em disco suficiente para instalar o agente AWS MGN). O instalador exibe os rótulos do volume e os detalhes de armazenamento. Para replicar seu banco de dados usando o serviço AWS MGN, selecione os discos aplicáveis em seu servidor de origem. Insira o caminho de cada disco, separado por vírgulas. Se você quiser replicar todos os discos, deixe o caminho em branco. Depois de confirmar os discos selecionados, a instalação prossegue.	DBA, Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Monitore o progresso da sincronização.	AWS O Agente de Replicação inicia o processo de sincroniz ação tirando primeiro um instantâneo dos discos selecionados e depois replicando os dados. Você pode monitorar o progresso da sincronização na página do servidor de origem no console do AWS MGN. Para obter mais informações, consulte Monitorar o servidor no ciclo de vida da migração.	DBA, Engenheiro de migração

Replicação usando o AWS MGN

Tarefa	Descrição	Habilidades necessárias
Gerencie o progresso da replicação.	Depois de iniciar a sincroniz ação inicial, seu servidor de origem aparece no console do AWS MGN, onde você pode gerenciar e monitorar a migração. O console exibe um tempo estimado para a replicação completa, que se baseia no tamanho total dos discos selecionados e na largura de banda de rede disponível.	DBA, Engenheiro de migração
Verifique a sincronização.	Depois que os discos no servidor de origem estiverem totalmente sincronizados,	Proprietário do aplicativo, DBA, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	verifique se todos os discos selecionados estão listados como totalmente sincroniz ados e se nenhum erro foi relatado no console. O console AWS MGN então fará a transição automátic a do status do ciclo de vida da migração para Pronto para teste, indicando que o ambiente replicado AWS está preparado para testes de desempenho e funcionalidade.	

Teste e corte

Tarefa	Descrição	Habilidades necessárias
Defina as configurações de lançamento.	Escolha o servidor de origem no console do AWS MGN e atualize as configurações de execução da instância de teste de destino. Na página de detalhes do servidor de origem, navegue até a guia Configurações do Launch para configurar a instância de teste. Escolha um tipo de instância econômico e o tipo de volume do Amazon Elastic Block Store (Amazon EBS) e, em seguida, configure os grupos de segurança e os	DBA, Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	requisitos de rede. Para obter mais informações, consulte Configurações do Launch.	
Inicie a instância de teste de destino.	Navegue até o console AWS MGN da sua máquina de origem sincronizada e inicie uma instância de teste de destino escolhendo Testar e recortar e, em seguida, Iniciar instâncias de teste. Isso cria um trabalho de inicialização que implanta a instância de teste usando suas configurações definidas . A instância é executada Nuvem AWS e replica o ambiente do servidor de banco de dados de origem. Monitore o progresso do lançamento na página Histórico do lançamento, onde você pode acompanhar a criação da instância e resolver quaisquer problemas.	DBA, Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Valide a instância de teste de destino.	Valide o servidor de EC2 banco de dados da Amazon: 1. Certifique-se de que o console AWS MGN mostre que a instância de teste está sendo executada com êxito. 2. Use um cliente RDP para fazer login. 3. No menu Iniciar, abra o SQL Server Configuration Manager. 4. Verifique o status dos serviços do SQL Server, incluindo o SQL Server (`MSSQLSERVER`) e o SQL Server Agent, garantind o que estejam intactos e configurados para o tipo de inicialização correto. 5. Compare as configurações do disco entre a instância de teste e o servidor do banco de dados de origem, confirmando se as letras das unidades, os volumes, as alocações de disco e os diretórios necessários estão mapeados corretamente. 6. Conecte-se ao SQL Server na EC2 instância de teste da Amazon e verifique se todos os bancos de	DBA, Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	dados de origem migraram e aparecem na lista de bancos de dados. Realize testes de validação para garantir que o banco de dados funcione conforme o esperado.	

Tarefa	Descrição	Habilidades necessárias

Renomeie o servidor.	AWS A migração do MGN envolve uma cópia em nível de armazenamento do seu servidor de origem local. Sua EC2 instância do SQL Server contém somente os detalhes do servidor de origem original em seus binários, portanto, atualize as informações binárias para refletir o nome do novo servidor.
	1. Use o SQL Server Management Studio (SSMS) para se conectar à sua EC2 instância do SQL Server.
	2. Verifique o nome do servidor:
	`SELECT @@SERVERNAME AS 'Current Server Name';`
	3. Renomeie a instância do SQL Server `NEW_SERVER_NAME` substituindo-a pelo nome do seu servidor:
	`EXEC sp_dropserver 'OLD_SERVER_NAME'`
	`EXEC sp_addserver 'NEW_SERVER_NAME', 'local';`
	4. Verifique se o nome do servidor está correto:
		DBA, Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	``` SELECT @@SERVERNAME AS 'Updated Server Name'; ``` 5. Reinicie a instância do SQL Server.	

Tarefa	Descrição	Habilidades necessárias
Inicie a instância de transferência.	No console AWS MGN, na página Servidores de origem, confirme se o status do ciclo de vida da migração do servidor está Pronto para transferência. Defina as configurações de execução para a instância de transferência, garantindo que as configurações espelhem seu ambiente local. Antes de iniciar a transição, encerre seu banco de dados local, o que garante o seguinte: • Todas as transações em andamento estão concluídas. • Nenhuma nova transação ocorrerá durante o processo de transição. • A sincronização de dados entre os discos de origem e de destino foi concluída. Inicie a instância de transferência no console MGN. AWS Quando a instância de transferência estiver operacional, faça login na instância e realize os seguintes testes:	Proprietário do aplicativo, DBA, engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	1. Certifique-se de que o SQL Server seja iniciado corretamente e que os bancos de dados estejam acessíveis. 2. Valide se seus dados estão intactos e consistentes com o servidor de origem. 3. Execute qualquer teste de aplicativo para confirmar se eles funcionam conforme o esperado. 4. No console AWS MGN, defina o estado da migração como Cutover complete. 5. Comece a rotear o tráfego para a EC2 instância.	

Solução de problemas

Problema	Solução
A sincronização inicial falha na etapa de autenticação.	Esse é um problema de conectividade de rede. O servidor de replicação não consegue se conectar ao AWS MGN.

Recursos relacionados

Documentação da AWS

- Começando com AWS Application Migration Service
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2

- O que é o Microsoft SQL Server na Amazon EC2?

Vídeos

- Executando uma migração Lift and Shift com AWS Application Migration Service (vídeo)

Migre VMware VMs com o HCX Automation usando o PowerCLI

Criado por Giri Nadiminty (AWS), Hassan Adekoya (AWS) e Naveen Deshwal

Resumo

Aviso: a partir de 30 de abril de 2024, o VMware Cloud on não AWS é mais revendido AWS nem por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu AWS representante para obter detalhes.

Esse padrão descreve como migrar máquinas virtuais VMware locais (VMs) para a VMware nuvem na AWS usando a automação VMware Hybrid Cloud Extension (HCX) baseada em scripts PowerCLI. VMware O PowerCLI é uma ferramenta de linha de comando criada no Windows. PowerShell Ele ajuda você a gerenciar o VMware software e automatiza as tarefas de infraestrutura e migração.

Você pode adaptar esse padrão para migração entre qualquer combinação de vCenters, data centers definidos por software (SDDCs) e ambientes em nuvem. Os scripts PowerCLI incluídos nesse padrão usam automação em vez de cliques do mouse para todas as tarefas de configuração e agendamento da VM, portanto, proporcionam economia de tempo nas atividades de migração e ajudam a reduzir o risco de erro humano.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta VMware Cloud on AWS com SDDC
- Um vCenter ou SDDC existente on-premises ou baseado na nuvem
- Uma conta de usuário com as permissões necessárias para vCenters de origem e destino ou SDDCs
- Emparelhamento de sites HCX com extensão de rede HCX (HCX-NE) configurada entre vCenters de origem e destino ou SDDCs
- VMware PowerCli instalado no servidor de sua escolha

Limitações

- Se o vCenter de origem usar o Cross-vCenter NSX, o módulo PowerCLI não funcionará. Use um método de script (como Python) com a API HCX em vez do PowerCLI.

- Se os migrados VMs precisarem de novos nomes ou endereços IP, use um método de script (como Python) com a API HCX.
- Este padrão não preenche o arquivo.csv, o que é obrigatório. Você pode preencher o arquivo usando o VMware vRealize Network Insight (vRNi) ou algum outro método.

Versões do produto

- VMware vSphere versão 5 ou posterior
- VMware HCX versão 4.4 ou posterior
- VMware PowerCLI versão 12.7 ou posterior

Arquitetura

Pilha de tecnologia de origem

- No local ou na nuvem VMware

Pilha de tecnologias de destino

- VMware Nuvem na AWS

Arquitetura de destino

Ferramentas

Serviços da AWS

- VMware O Cloud on AWS é um serviço desenvolvido em conjunto pela AWS para ajudar você a VMware migrar e estender seus ambientes locais VMware baseados no vSphere para a nuvem da AWS.

Outras ferramentas

- VMware O Hybrid Cloud Extension (HCX) é um utilitário para migrar cargas de trabalho do seu VMware ambiente local para a nuvem VMware na AWS sem alterar a plataforma subjacente.

Observação: esse produto era conhecido anteriormente como Hybrid Cloud Extension e NSX Hybrid Connect. Esse padrão usa HCX para migração de VM.

- VMware O PowerCLI é uma ferramenta de linha de comando para automatizar o gerenciamento do vSphere e do vCloud. VMware Você executa comandos PowerCLI no Windows PowerShell usando PowerShell cmdlets. Esse padrão usa o PowerCLI para executar comandos de migração.

Código

Script simples e independente

Recomendamos que você use esse script de máquina única para testes iniciais, para verificar se as opções de configuração são aceitas e se comportam conforme o esperado. Para obter instruções, consulte a seção Épicos.

```
<# Manual Variables #>
$HcxServer = "[enterValue]"
$SrcNetworkName = "[enterValue]"
$DstNetworkName = "[enterValue]"
$DstComputeName = "[enterValue]"
$DstDSName = "[enterValue]"
$DstFolderName = "[enterValue]"
$vmName = "[enterValue]"

<# Environment Setup #>
Connect-HCXServer -Server $HcxServer
$HcxDstSite = Get-HCXSite -Destination
$HcxSrcSite = Get-HCXSite -Source
$SrcNetwork = Get-HCXNetwork -Name $SrcNetworkName -Type VirtualWire -Site $HcxSrcSite
$DstNetwork = Get-HCXNetwork -Name $DstNetworkName -Type NsxtSegment -Site $HcxDstSite
$DstCompute = Get-HCXContainer -Name $DstComputeName -Site $HcxDstSite
$DstDS = Get-HCXDatastore -Name $DstDSName -Site $HcxDstSite
$DstFolder = Get-HCXContainer -name $DstFolderName -Site $HcxDstSite
$vm = Get-HCXVM -Name $vmName

<# Migration #>
$NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -DestinationNetwork
 $DstNetwork
$NewMigration = New-HCXMigration -VM $vm -MigrationType vMotion -SourceSite $HcxSrcSite
 -DestinationSite $HcxDstSite -Folder $DstFolder -TargetComputeContainer $DstCompute
 -TargetDatastore $DstDS -NetworkMapping $NetworkMapping -DiskProvisionType Thin
```

```
 -UpgradeVMTools $True -RemoveISOs $True -ForcePowerOffVm $True -RetainMac $True -
UpgradeHardware $True -RemoveSnapshots $True
```

Script completo baseado em .csv

Depois que o teste for concluído, você poderá usar o script a seguir em seus ambientes de produção. Para obter instruções, consulte a seção Épicos.

```
<# Schedule #>
write-host("Getting Time for Scheduling")
$startTime = [DateTime]::Now.AddDays(12)
$endTime = [DateTime]::Now.AddDays(15)

<# Migration #>
Connect-HCXServer -Server [enterValue]
write-host("Getting Source Site")
$HcxSrcSite = Get-HCXSite
write-host("Getting Target Site")
$HcxDstSite = Get-HCXSite -Destination
$HCXVMS = Import-CSV .\Import_VM_list.csv
ForEach ($HCXVM in $HCXVMS) {
    $DstFolder = Get-HCXContainer $HCXVM.DESTINATION_VM_FOLDER -Site $HcxDstSite
    $DstCompute = Get-HCXContainer $HCXVM.DESTINATION_COMPUTE  -Site $HcxDstSite
    $DstDatastore = Get-HCXDatastore $HCXVM.DESTINATION_DATASTORE -Site $HcxDstSite
    $SrcNetwork = Get-HCXNetwork $HCXVM.SOURCE_NETWORK -Type VirtualWire -Site
 $HcxSrcSite
    $DstNetwork = Get-HCXNetwork $HCXVM.DESTINATION_NETWORK -Type NsxtSegment -Site
 $HcxDstSite
    $NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -
DestinationNetwork $DstNetwork
    $NewMigration = New-HCXMigration -VM (Get-HCXVM $HCXVM.VM_NAME) -MigrationType
 Bulk -SourceSite $HcxSrcSite -DestinationSite $HcxDstSite -Folder $DstFolder -
TargetComputeContainer $DstCompute -TargetDatastore $DstDatastore -NetworkMapping
 $NetworkMapping -DiskProvisionType Thin -UpgradeVMTools $True -RemoveISOs $True -
ForcePowerOffVm $True -RetainMac $True -UpgradeHardware $True -RemoveSnapshots $True -
ScheduleStartTime $startTime -ScheduleEndTime $endTime
    Start-HCXMigration -Migration $NewMigration -Confirm:$false
}
```

Épicos

Coletar informações para variáveis manuais

Tarefa	Descrição	Habilidades necessárias
Encontrar os nomes dos servidores vCenter e SDDC de origem e destino.	Os scripts do PowerCLI exigem as variáveis descritas neste épico. Você pode coletar essas informaçõ es com antecedência para facilitar o uso do script. Na seção HCX do console vSphere, escolha Infraestr utura, Emparelhamento de site. Anote os nomes dos servidores de origem e destino que são exibidos.	Arquiteto de nuvem
Encontrar os nomes dos HCX de origem e destino.	Na seção HCX do console vSphere, escolha Sistema, Administração. Anote os nomes dos HCX de origem e destino que são exibidos.	Arquiteto de nuvem
Encontrar os nomes das redes de origem e destino.	Na seção HCX do console vSphere, escolha Sistema, Extensão de rede. Anote os nomes da rede de origem e destino. **Note** Como alternativa, você pode obter os nomes da rede de origem e destino	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	usando os comandos Get- HCXNetwork e Get- HCXNetwor k -Destination do PowerCLI depois de se conectar ao servidor HCX.	
Reunir informações adicionais no console do vSphere.	No console do vSphere, colete as seguintes informações: • Nomes dos VMs que você deseja migrar • Ambiente computacional de destino (cluster/host) • Datastore de destino • Nome da pasta da VM de destino	Arquiteto de nuvem

Tomar decisões de migração

Tarefa	Descrição	Habilidades necessárias
Determinar as opções de migração.	Determine o seguinte: • `MigrationType` : os tipos de migração assistida por HCX são vMotion, bulk, cold e RAV. Sua escolha depende dos requisitos de tempo de inatividade, da largura de banda da rede, do período de migração e do tipo de workload. Para	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	obter mais informações, consulte a postagem do blog da AWS Migrando cargas de trabalho para a VMware nuvem na AWS com a extensão de nuvem híbrida (HCX). • `DiskProvisionType (Thin, Thick)` • `UpgradeVMTools ($True, $False)` • `RemoveISOs ($True, $False)` • `ForcePowerOffVm ($True, $False)` • `RetainMac ($True, $False)` • `UpgradeHardware ($True, $False)` • `RemoveSnapshots ($True, $False)` Para obter mais informações sobre cada opção, consulte a documentação do VMware desenvolvedor.	

Execute o script simples para o teste inicial

Tarefa	Descrição	Habilidades necessárias
Copiar o script.	A versão simples do script é independente em um único arquivo. Você pode usá-lo para testar a migração de uma única máquina. Copie o primeiro script da seção Código desse padrão e armazene-o no computador que tem o módulo VMware PowerCLI instalado. (Para instalar o PowerCLI, siga as instruções na VMware documentação.)	Arquiteto de nuvem
Definir as variáveis do script.	Defina todas as variáveis na seção `Manual Variables` do script.	Arquiteto de nuvem
Definir as variáveis de migração.	Defina todas as configurações `New-HCXMigration` na seção `Migration` do script.	Arquiteto de nuvem
Especificar os sites.	(Opcional) Se a origem ou o destino tiver vários sites, especifique os sites manualmente na seção `Environment Setup` do script. Se a origem e o destino tiverem sites únicos, o script pesquisará automaticamente as informações.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Executar o script.	No servidor em que o PowerCLI está instalado, em uma PowerShell janela elevada, execute o script e insira suas credenciais quando solicitado.	Arquiteto de nuvem
Validar o script.	Confirme se a migração da VM foi iniciada.	Arquiteto de nuvem

Execute o script completo para migrar vários VMs

Tarefa	Descrição	Habilidades necessárias
Criar e preencher o arquivo .csv.	Crie um arquivo.csv chamado `Import_VM_list.csv` em seu computador e preencha-o com o seguinte conteúdo de amostra: `VM_NAME,DESTINATIO N_VM_FOLDER,DESTIN ATION_COMPUTE,DEST INATION_DATASTORE, SOURCE_NETWORK,DES TINATION_NETWORK [enterValue],[enter Value],[enterValue ],[enterValue],[en terValue],[enterVa lue]` Substitua cada `[enterVal ue]` no arquivo.csv pelas informações coletadas anteriormente.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Note Você pode preencher o arquivo.csv usando o VMware vRealize Network Insight (vRNi) ou algum outro método.	
Copiar o script.	A versão completa do script usa informações de um arquivo.csv externo para migrar automaticamente vários. VMs Copie o segundo script da seção Código desse padrão e armazene-o no computador que tem o módulo VMware PowerCLI instalado, na mesma pasta do arquivo.csv.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Modificar o script.	Edite o script para fazer as seguintes alterações: • Linha 7: defina a variável do servidor HCX (`Connect-HCXServer`). • Linha 12: (opcional) se você definiu o nome do arquivo.csv de forma diferente, atualize-o. • Linhas 3-4: (opcional) defina o cronograma. • Linha 20: (opcional) especifique as configurações `New-HCXMigration` na seção `Migration` . • Linhas 9 e 11: (opcional) se a origem ou o destino incluir vários sites, especifique os sites desejados manualmente.	Arquiteto de nuvem
Executar o script.	No servidor em que o PowerCLI está instalado, em uma PowerShell janela elevada, execute o script e insira suas credenciais quando solicitado.	Arquiteto de nuvem
Validar o script.	Confirme se a migração da VM foi iniciada.	Arquiteto de nuvem

Solução de problemas

Problema	Solução
O script falha com a mensagem de erro: “Todas as redes de origem não estão mapeadas para o destino!”	Se o vCenter de origem usar o Cross-vCenter NSX, o módulo PowerCLI não funcionará. Use um método de script (como Python) com a API HCX em vez do PowerCLI. Essa é uma limitação conhecida do script PowerCLI.
O script falha com a mensagem de erro: “HCXServer Erro de conexão: não autorizado”	As credenciais que você inseriu não fornecem as permissões necessárias.

Recursos relacionados

- Migração de cargas de trabalho para a VMware nuvem na AWS com a extensão de nuvem híbrida (HCX) (publicação no blog da AWS)
- Escolha de uma abordagem de migração para realocar seus VMware aplicativos e cargas de trabalho para a nuvem da AWS (AWS Prescriptive Guidance)
- Migre o VMware SDDC para a VMware nuvem na AWS usando o VMware HCX (AWS Prescriptive Guidance)
- Introdução ao módulo HCX (postagem VMware no blog)

Migre uma workload do F5 BIG-IP para o F5 BIG-IP VE na Nuvem AWS

Criado por Will Bauer (AWS)

Resumo

As organizações estão buscando migrar para a Nuvem da Amazon Web Services (AWS) para aumentar sua agilidade e resiliência. Depois de migrar suas soluções de segurança e gerenciamento de tráfego F5 BIG-IP para a Nuvem AWS, você pode se concentrar na agilidade e na adoção de modelos operacionais de alto valor em toda a sua arquitetura corporativa.

Esse padrão descreve como migrar uma workload F5 BIG-IP para uma workload F5 BIG-IP Virtual Edition (VE) na Nuvem AWS. A workload será migrada por meio da redefinição da hospedagem do ambiente existente e da implantação de aspectos da redefinição da plataforma, como descoberta de serviços e integrações de API. CloudFormation Os modelos da AWS aceleram a migração da sua carga de trabalho para a nuvem da AWS.

Esse padrão é destinado às equipes técnicas de engenharia e arquitetura que estão migrando soluções de segurança e gerenciamento de tráfego F5 e acompanha o guia Migração do F5 BIG-IP para o F5 BIG-IP VE na Nuvem AWS no site Recomendações da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma workload F5 BIG-IP existente on-premises.
- Licenças F5 existentes para versões do BIG-IP VE.
- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) existente configurada com uma saída por meio de um gateway NAT ou endereço IP elástico e configurada com acesso aos seguintes endpoints: Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon), AWS Security Token EC2 Service (AWS STS) e Amazon. CloudWatch Você também pode modificar o Início rápido da arquitetura VPC modular e escalável como um alicerce para suas implantações.
- Uma ou duas zonas de disponibilidade existentes, dependendo de suas necessidades.
- Três sub-redes privadas existentes em cada zona de disponibilidade.
- CloudFormation Modelos da AWS, disponíveis no GitHub repositório F5.

Durante a migração, você também pode usar o seguinte, dependendo de seus requisitos:

- Uma extensão de failover de nuvem F5 para gerenciar mapeamento de endereços IP elásticos, mapeamento de IP secundário e alterações na tabela de rotas.
- Se você usar várias zonas de disponibilidade, precisará usar as extensões de failover de nuvem F5 para lidar com o mapeamento de IP elástico para servidores virtuais.
- Você deve considerar o uso de F5 Application Services 3 (AS3), F5 Application Services Templates (FAST) ou outro modelo de infraestrutura como código (IaC) para gerenciar as configurações. Preparar as configurações em um modelo de IaC e usar repositórios de código ajudará na migração e em seus esforços contínuos de gerenciamento.

Experiência

- Esse padrão exige familiaridade com a forma como um ou mais VPCs podem ser conectados aos data centers existentes. Para obter mais informações sobre isso, consulte as opções de conectividade da Network-to-Amazon VPC na documentação da Amazon VPC.
- Também é necessária familiaridade com os produtos e módulos da F5, incluindo Sistema Operacional de Gerenciamento de Tráfego (TMOS), Gerenciador de Tráfego Local (LTM), Gerenciador de Tráfego Global (GTM), Gerenciador de Política de Acesso (APM), Gerenciador de Segurança de Aplicativos (ASM), Gerenciador de Firewall Avançado (AFM)(AFM), e BIG-IQ.

Versões do produto

- Recomendamos que você use F5 BIG-IP versão 13.1 ou superior, embora o padrão suporte F5 BIG-IP versão 12.1 ou superior.

Arquitetura

Pilha de tecnologia de origem

- Workload F5 BIG-IP

Pilha de tecnologias de destino

- Amazon CloudFront
- Amazon CloudWatch
- Amazon EC2
- Amazon S3

- Amazon VPC
- AWS Global Accelerator
- AWS STS
- AWS Transit Gateway
- F5 BIG-IP VE

Arquitetura de destino

Ferramentas

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- A Amazon CloudFront acelera a distribuição do seu conteúdo da web entregando-o por meio de uma rede mundial de data centers, o que reduz a latência e melhora o desempenho.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Security Token Service (AWS STS) ajuda você a solicitar credenciais temporárias com privilégios limitados para os usuários.
- O AWS Transit Gateway é um hub central que conecta nuvens privadas virtuais (VPCs) e redes locais.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Épicos

Descoberta e avaliação

Tarefa	Descrição	Habilidades necessárias
Avalie o desempenho do F5 BIG-IP.	Colete e registre as métricas de desempenho dos aplicativos no servidor virtual e as métricas dos sistemas que serão migrados. Isso ajudará a dimensionar corretamente a infraestrutura da AWS de destino para uma melhor otimização de custos.	Arquiteto F5, engenheiro e arquiteto de rede, engenheiro
Avalie o sistema operacional e a configuração do F5 BIG-IP.	Avalie quais objetos serão migrados e se uma estrutura de rede precisa ser mantida, como VLANs.	Arquiteto F5, engenheiro
Avalie as opções de licença F5.	Avalie qual licença e modelo de consumo você precisará. Essa avaliação deve ser baseada em sua avaliação do sistema operacional e da configuração do F5 BIG-IP.	Arquiteto F5, engenheiro
Avalie os aplicativos públicos.	Determine quais aplicativos exigirão endereços IP públicos. Alinhe esses aplicativos às instâncias e clusters necessários para atender aos requisitos de desempenho e Acordo de Serviço (SLA).	Arquiteto F5, arquiteto de nuvem, arquiteto de rede, engenheiro, equipes de aplicativos

Tarefa	Descrição	Habilidades necessárias
Avalie os aplicativos internos.	Avalie quais aplicativos serão usados pelos usuários internos. Certifique-se de saber onde esses usuários internos estão na organizaç ão e como esses ambientes se conectam à Nuvem AWS. Você também deve garantir que esses aplicativos possam usar o sistema de nomes de domínio (DNS) como parte do domínio padrão.	Arquiteto F5, arquiteto de nuvem, arquiteto de rede, engenheiro, equipes de aplicativos
Finalize a AMI.	Nem todas as versões F5 BIG-IP são criadas como Amazon Machine Images (). AMIs Você pode usar a ferramenta de geração de imagens F5 BIG-IP se tiver versões específicas de engenharia de correção rápida (QFE) necessárias. Para obter mais informações sobre essa ferramenta, consulte a seção “Recursos relacionados”.	Arquiteto F5, arquiteto de nuvem, engenheiro
Finalize os tipos e a arquitetu ra da instância.	Decida sobre os tipos de instância, a arquitetura VPC e a arquitetura interconectada.	Arquiteto F5, arquiteto de nuvem, arquiteto de rede, engenheiro

Atividades completas relacionadas à segurança e conformidade

Tarefa	Descrição	Habilidades necessárias
Documente as políticas de segurança F5 existentes.	Colete e documente as políticas de segurança F5 existentes. Certifique-se de criar uma cópia deles em um repositório de código seguro.	Arquiteto F5, engenheiro
Criptografe a AMI.	(Opcional) Sua organização pode exigir criptografia de dados em repouso. Para obter mais informações sobre como criar uma imagem personalizada traga a sua própria licença (BYOL), consulte a seção “Recursos relacionados”.	Arquiteto F5, engenheiro, arquiteto de nuvem, engenheiro
Conclua os dispositivos.	Isso ajudará a proteger contra possíveis vulnerabilidades.	Arquiteto F5, engenheiro

Configure seu novo ambiente da AWS

Tarefa	Descrição	Habilidades necessárias
Crie contas periféricas e de segurança.	Faça login no Console de Gerenciamento da AWS e crie as contas da AWS que fornecerão e operarão os serviços de borda e segurança. Essas contas podem ser diferentes das contas que operam VPCs para serviços e aplicativos compartilhados. Essa etapa pode ser	Arquiteto de nuvem, engenheiro

Tarefa	Descrição	Habilidades necessárias
	concluída como parte de uma zona de pouso.	
Implemente a vantagem e a segurança VPCs.	Configure e configure o VPCs necessário para fornecer serviços de ponta e segurança .	Arquiteto de nuvem, engenheiro
Conecte-se ao datacenter de origem.	Conecte-se ao datacenter de origem que hospeda sua workload F5 BIG-IP.	Arquiteto de nuvem, arquiteto de rede, engenheiro
Implante as conexões VPC.	Conecte o serviço de borda e segurança VPCs ao aplicativo VPCs.	Arquiteto de rede, engenheiro
Implante as instâncias.	Implante as instâncias usando os CloudFormation modelos da AWS na seção “Recursos relacionados”.	Arquiteto F5, engenheiro
Teste e configure o failover da instância.	Certifique-se de que o modelo AWS Advanced HA iApp ou a extensão F5 Cloud Failover estejam configurados e operando corretamente.	Arquiteto F5, engenheiro

Configurar redes

Tarefa	Descrição	Habilidades necessárias
Prepare a topologia da VPC.	Abra o console da Amazon VPC e certifique-se de que sua VPC tenha todas as sub-redes e proteções necessárias	Arquiteto de rede, arquiteto F5, arquiteto de nuvem, engenheiro

Tarefa	Descrição	Habilidades necessárias
	para a implantação do F5 BIG-IP VE.	
Prepare seus endpoints de VPC.	Prepare os endpoints VPC para Amazon, Amazon EC2 S3 e AWS STS se uma carga de trabalho F5 BIG-IP não tiver acesso a um gateway NAT ou endereço IP elástico em uma interface TMM.	Arquiteto de nuvem, engenheiro

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Migre a configuração.	Migre a configuração F5 BIG-IP para F5 BIG-IP VE na nuvem AWS.	Arquiteto F5, engenheiro
Associe o secundário IPs.	Os endereços IP do servidor virtual têm uma relação com os endereços IP secundários atribuídos às instâncias. Atribua endereços IP secundários e verifique se a opção “Permitir remapeamento/reatribuição” está selecionada.	Arquiteto F5, engenheiro

Testar as configurações

Tarefa	Descrição	Habilidades necessárias
Valide as configurações do servidor virtual.	Teste os servidores virtuais.	Arquiteto F5, equipes de aplicativos

Finalize as operações

Tarefa	Descrição	Habilidades necessárias
Crie a estratégia de backup.	Os sistemas devem ser desligados para criar um instantâneo completo. Para obter mais informações, consulte “Atualizar uma máquina virtual F5 BIG-IP” na seção “Recursos relaciona dos”.	Arquiteto F5, arquiteto de nuvem, engenheiro
Crie o runbook de execução de failover do cluster.	Certifique-se de que o processo do runbook de failover esteja concluído.	Arquiteto F5, engenheiro
Configure e valide o registro em log.	Configure o F5 Telemetry Streaming para enviar registros para os destinos necessários.	Arquiteto F5, engenheiro

Concluir a substituição

Tarefa	Descrição	Habilidades necessárias
Passe para a nova implantaç ão.		Arquiteto F5, arquiteto de nuvem, arquiteto de rede, engenheiro, AppTeams

Recursos relacionados

Guia de migração

- Migração do F5 BIG-IP para o F5 BIG-IP VE na Nuvem AWS

Recursos do F5

- CloudFormation Modelos da AWS no repositório F5 GitHub
- F5 no AWS Marketplace
- Visão geral do F5 BIG-IP VE
- Exemplo de início rápido - Edição virtual BIG-IP com WAF (LTM + ASM)
- Serviços de aplicativos F5 na AWS: uma visão geral (vídeo)
- Guia do usuário sobre extensão dos serviços de aplicativos F5
- Documentação da nuvem F5
- Wiki REST do iControl F5
- Visão geral de arquivos de configuração únicos F5 (11.x - 15.x)
- Laboratório de topologia F5
- Documentos técnicos da F5
- Ferramenta de geração de imagens F5 BIG-IP
- Atualizando uma máquina virtual F5 BIG-IP VE
- Visão geral da opção “migração de plataforma” do arquivo UCS

Migrar um aplicativo web do Go on-premises para AWS Elastic Beanstalk usando o método binário

Criado por Suhas Basavaraj (AWS) e Shumaz Mukhtar Kazi (AWS)

Resumo

Esse padrão descreve como migrar um aplicativo web do Go on-premises para o AWS Elastic Beanstalk. Depois que o aplicativo é migrado, o Elastic Beanstalk cria o binário para o pacote de origem e o implanta em uma instância do Amazon Elastic Compute Cloud (Amazon). EC2

Como estratégia de migração para redefinir a hospedagem, a abordagem desse padrão é rápida e não requer alterações no código, o que significa menos tempo de teste e migração.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo web do Go on-premise
- Um GitHub repositório que contém o código-fonte do seu aplicativo Go. Se você não usa GitHub, há outras maneiras de criar um pacote de origem de aplicativos para o Elastic Beanstalk.

Versões do produto

- A versão do Go mais recente compatível com o Elastic Beanstalk. Para obter mais informações, consulte a Documentação do Elastic Beanstalk.

Arquitetura

Pilha de tecnologia de origem

- Um aplicativo web do Go on-premise

Pilha de tecnologias de destino

- AWS Elastic Beanstalk
- Amazon CloudWatch

Arquitetura de destino

Ferramentas

- Com o AWS Elastic Beanstalk, é possível implantar e gerenciar rapidamente aplicativos na Nuvem AWS sem que os usuários tenham que se preocupar com a infraestrutura que os executa. O Elastic Beanstalk reduz a complexidade de gerenciamento sem restringir as escolhas nem o controle.
- GitHubé um sistema de controle de versão distribuído de código aberto.

Épicos

Crie o arquivo .zip do pacote de origem do aplicativo web do Go

Tarefa	Descrição	Habilidades necessárias
Crie o pacote de origem do aplicativo web do Go	Abra o GitHub repositór io que contém o código-fo nte do seu aplicativo Go e prepare o pacote de origem. O pacote de origem contém um arquivo de origem `applicati on.go` no diretório raiz, que hospeda o pacote principal do seu aplicativo Go. Se você não usa GitHub, consulte a seção Pré-requisitos anteriorm ente neste padrão para ver outras formas de criar seu pacote de origem do aplicativ o.	Administrador do sistema, desenvolvedor de aplicativos
Criar um arquivo de configura ção.	Crie uma pasta `.ebextens ions` em seu pacote de origem e, em seguida, crie um arquivo `options.c onfig` dentro dessa pasta.	Administrador do sistema, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte a Documentação do Elastic Beanstalk.	
Crie o arquivo .zip do pacote de origem.	Execute o seguinte comando: `git archive -o ../godemoapp.zip HEAD` Isso cria o arquivo .zip do pacote de origem. Baixe e salve o arquivo .zip como um arquivo local. **Important** O arquivo.zip não pode exceder 512 MB e não pode incluir uma pasta principal ou um diretório de nível superior.	Administrador do sistema, desenvolvedor de aplicativos

Migrar um aplicativo web do Go para o Elastic Beanstalk

Tarefa	Descrição	Habilidades necessárias
Selecione o aplicativo do Elastic Beanstalk.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Elastic Beanstalk. 2. A partir da lista de Regiões, selecione a sua Região da AWS.	Administrador do sistema, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	3. No painel de navegação, selecione Aplicativos e, em seguida, um aplicativo do Elastic Beanstalk existente ou crie um. Para obter instruções sobre como criar um aplicativo do Elastic Beanstalk, consulte a documentação do Elastic Beanstalk.	
Inicie o ambiente de servidor web do Elastic Beanstalk.	1. Na página de visão geral do aplicativo, selecione Criar um novo ambiente e, em seguida, selecione Ambiente de servidor Web. 2. Preencha os campos Nome do ambiente e Nome do domínio. 3. Escolha a versão da plataforma e selecione Go como sua plataforma.	Administrador do sistema, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Faça upload do arquivo .zip do pacote de origem no Elastic Beanstalk.	1. Para Código do aplicativo, escolha Faça upload do seu código e, em seguida, escolha Arquivo local. 2. Selecione o arquivo .zip que contém o pacote de origem. 3. Em Rótulo da versão, dê um nome exclusivo ao arquivo e escolha Criar ambiente.	Administrador do sistema, desenvolvedor de aplicativos
Teste o aplicativo web do Go implantado.	Você será redirecionado para a página de visão geral do aplicativo do Elastic Beanstalk. Na parte superior da visão geral, ao lado de ID do ambiente, escolha a URL que termina em `elasticbeanstalk.com` com para navegar até seu aplicativo. Seu aplicativo deve usar esse nome em seu arquivo de configuração como uma variável de ambiente e exibi-lo na página web.	Administrador do sistema, desenvolvedor de aplicativos

Solução de problemas

Problema	Solução
Não é possível acessar o aplicativo por meio de um Application Load Balancer.	Verifique o grupo de destino que contém o aplicativo do Elastic Beanstalk. Se não estiver íntegro, faça login na sua instância do Elastic

Problema	Solução
	Beanstalk e verifique a configuração do arquivo `nginx.conf` para verificar se ele é roteado para a URL correta do status de integridade. Você pode precisar alterar a URL de verificação de integridade do grupo de destino.

Recursos relacionados

- Versões da plataforma Go compatíveis com o Elastic Beanstalk
- Usando arquivos de configuração com o Elastic Beanstalk
- Criação de um aplicativo de exemplo no Elastic Beanstalk

Migrar um servidor SFTP local para usar AWSAWS Transfer for SFTP

Criado por Akash Kumar (AWS)

Resumo

Esse padrão descreve como migrar uma solução de transferência de arquivos local que usa o protocolo de transferência de arquivos (SFTP) do Secure Shell (SSH) para o Nuvem AWS usando o serviço. AWS Transfer for SFTP Os usuários geralmente se conectam a um servidor SFTP por meio de seu nome de domínio ou por IP fixo. Esse padrão abrange os dois casos.

AWS Transfer for SFTP é membro do AWS Transfer Family. É um serviço de transferência seguro que você pode usar para transferir arquivos para dentro e para fora dos serviços de AWS armazenamento via SFTP. Você pode usar AWS Transfer for SFTP com o Amazon Simple Storage Service (Amazon S3) ou o Amazon Elastic File System (Amazon EFS). Esse padrão usa o Amazon S3 para armazenamento.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Um nome de domínio SFTP existente ou IP fixo do SFTP.

Limitações

- O maior objeto que você pode transferir em uma solicitação atualmente é de 5 GiB. Para arquivos maiores que 100 MiB, considere usar o upload de várias partes do Amazon S3.

Arquitetura

Pilha de tecnologia de origem

- Arquivos simples on-premises ou arquivos de despejo de banco de dados.

Pilha de tecnologias de destino

- AWS Transfer for SFTP
- Amazon S3

- Amazon Virtual Private Cloud (Amazon VPC)
- AWS Identity and Access Management Funções e políticas (IAM)
- Endereços IP elásticos
- Grupos de segurança
- Amazon CloudWatch Logs (opcional)

Arquitetura de destino

Automação e escala

Para automatizar a arquitetura de destino desse padrão, use os AWS CloudFormation modelos anexados:

- `amazon-vpc-subnets.yml` provisiona uma nuvem privada virtual (VPC) com duas sub-redes públicas e duas privadas.
- `amazon-sftp-server.yml` provisiona o servidor SFTP.
- `amazon-sftp-customer.yml` adiciona usuários.

Ferramentas

Serviços da AWS

- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas e aplicativos, Serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados. Esse padrão usa o Amazon S3 como sistema de armazenamento para transferências de arquivos.
- AWS Transfer for SFTPajuda você a transferir arquivos para dentro e para fora dos serviços de AWS armazenamento pelo protocolo SFTP.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Épicos

Crie uma VPC

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC com sub-redes.	Abra o console da Amazon VPC. Criar uma nuvem privada virtual (VPC) com duas sub-redes públicas. (A segunda sub-rede fornece alta disponibilidade.) —ou— Você pode implantar o CloudFormation modelo em anexo`amazon-vpc-subnets.yml` ,, no CloudFormation console para automatizar as tarefas neste épico.	Desenvolvedor, administrador de sistemas
Um gateway da internet.	Forneça um gateway da Internet e anexe-o à VPC.	Desenvolvedor, administrador de sistemas
Migre um IP existente.	Anexe um IP existente ao endereço IP elástico. É possível criar um endereço IP elástico de seu grupo de endereços e usá-lo.	Desenvolvedor, administrador de sistemas

Provisione um servidor SFTP.

Tarefa	Descrição	Habilidades necessárias
Crie um servidor SFTP.	Abra o console de AWS Transfer Family. Siga as	Desenvolvedor, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	instruções em Criar um endpoint voltado para a Internet para seu servidor na AWS Transfer Family documentação para criar um servidor SFTP com um endpoint voltado para a Internet. Em Tipo de endpoint, selecione VPC hospedada. Em Acesso, escolha Voltado para internet. Para VPC, escolha a VPC que você criou no épico anterior. —ou— Você pode implantar o CloudFormation modelo em anexo`amazon-sftp-server.yml` ,, no CloudFormation console para automatizar as tarefas neste épico.	

Tarefa	Descrição	Habilidades necessárias
Migre o nome do domínio.	Anexe o nome de domínio existente ao nome de host personalizado. Se você estiver usando um novo nome de domínio, use o alias do DNS do Amazon Route 53. Para um nome de domínio existente, escolha Outro DNS. Para obter mais informaçõ es, consulte Trabalho com nomes de host personalizados na AWS Transfer Family documentação.	Desenvolvedor, administrador de sistemas
Adicione uma função de CloudWatch registro.	(Opcional) se você quiser ativar o CloudWatch registro, crie um `Transfer` papel com as operações da API CloudWatch Logs `logs:CreateLogGrou p logs:CreateLogStre am logs:Desc ribeLogStreams ,, logs:PutLogEvents e`. Para obter mais informações, consulte Registrar atividades CloudWatch na AWS Transfer Family documentação.	Desenvolvedor, administrador do sistema
Salve e envie.	Escolha Salvar. Em Ações, escolha Iniciar e aguarde até que o servidor SFTP seja criado com o status Online.	Desenvolvedor, administrador de sistemas

Mapeie endereços IP elásticos para o servidor SFTP

Tarefa	Descrição	Habilidades necessárias
Pare o servidor para que você possa modificar as configurações.	No AWS Transfer Family console, escolha Servidores e selecione o servidor SFTP que você criou. Em Ações, escolha Interromper. Quando o servidor estiver off-line, escolha Editar para modificar suas configurações.	Desenvolvedor, administrador do sistema
Escolha zonas de disponibilidade e sub-redes.	Na seção Zonas de disponibilidade, escolha suas Zonas de Disponibilidade e sub-redes para sua VPC.	Desenvolvedor, administrador de sistemas
Adicionar endereços IP elásticos.	Em IPv4 Endereços, escolha um endereço IP elástico para cada sub-rede e escolha Salvar.	Desenvolvedor, administrador de sistemas

Adicionar usuários

Tarefa	Descrição	Habilidades necessárias
Crie um perfil do IAM para que os usuários acessem o bucket do S3.	Crie um perfil do IAM para `Transfer` e adicione `s3:ListBucket` , `s3:GetBucketLocation` e `s3:PutObject` com o nome do bucket do S3 como recurso. Para obter mais informações, consulte Criar uma função e uma política do	Desenvolvedor, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	IAM na AWS Transfer Family documentação. —ou— Você pode implantar o CloudFormation modelo em anexo`amazon-sftp-customer.yml` ,, no CloudFormation console para automatizar as tarefas neste épico.	
Criar um bucket do S3.	Crie um bucket do S3 para o aplicativo.	Desenvolvedor, administrador de sistemas
Crie uma pasta opcional.	(Opcional) Se você quiser armazenar arquivos para usuários separadamente, em pastas específicas do Amazon S3, adicione pastas conforme apropriado.	Desenvolvedor, administrador de sistemas
Crie uma chave pública SSH.	Para criar um par de chaves SSH, consulte Gerar chaves SSH na AWS Transfer Family documentação.	Desenvolvedor, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Adicionar usuários.	No AWS Transfer Family console, escolha Servidores, selecione o servidor SFTP que você criou e escolha Adicionar usuário. Para Diretório inicial, escolha o bucket S3 que você criou. Em chave pública SSH, especifique a parte da chave pública SSH do par de chaves SSH. Adicione usuários ao servidor SFTP e escolha Adicionar.	Desenvolvedor, administrador de sistemas

Teste o servidor SFTP.

Tarefa	Descrição	Habilidades necessárias
Atualizar o grupo de segurança	Na seção Grupo de segurança do seu servidor SFTP, adicione o IP da sua máquina de teste para obter acesso ao SFTP.	Desenvolvedor
Use um utilitário de cliente SFTP para testar o servidor.	Teste as transferências de arquivos usando qualquer utilitário de cliente SFTP. Para obter uma lista de clientes e instruções, consulte Transferência de arquivos usando um cliente na AWS Transfer Family documentação.	Desenvolvedor

Recursos relacionados

- AWS Transfer Family Guia do usuário
- Guia do usuário do Amazon S3
- Endereços IP elásticos na EC2 documentação da Amazon

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre uma VM local para a Amazon EC2 usando o AWS Application Migration Service

Criado por Thanh Nguyen (AWS)

Resumo

Quando se trata de migração de aplicativos, as organizações podem adotar abordagens diferentes para redefinir a hospedagem (mover sem alterações (lift-and-shift)) os servidores do aplicativo do ambiente on-premises para a Nuvem da Amazon Web Services (AWS). Uma forma é provisionar novas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e, em seguida, instalar e configurar o aplicativo do zero. Outra abordagem é usar serviços de migração de terceiros ou nativos da AWS para migrar vários servidores ao mesmo tempo.

Esse padrão descreve as etapas para migrar uma máquina virtual (VM) compatível para uma EC2 instância da Amazon na nuvem da AWS usando o AWS Application Migration Service. Você pode usar a abordagem deste padrão para migrar uma ou várias máquinas virtuais manualmente, uma por uma ou automaticamente ao criar scripts de automação apropriados com base nas etapas descritas.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da AWS em uma das regiões da AWS compatíveis com o Serviço de migração de aplicativos
- Conectividade de rede entre o servidor de origem e o EC2 servidor de destino por meio de uma rede privada usando o AWS Direct Connect ou uma rede privada virtual (VPN), ou pela Internet

Limitações

- Para obter a lista mais recente das regiões aceitas, consulte as Regiões da AWS compatíveis.
- Para obter uma lista dos sistemas operacionais compatíveis, consulte a seção Sistemas operacionais compatíveis e a seção Geral da Amazon EC2 FAQs.

Arquitetura

Pilha de tecnologia de origem

- Um servidor físico, virtual ou hospedado na nuvem executando um sistema operacional suportado pela Amazon EC2

Pilha de tecnologias de destino

- Uma EC2 instância da Amazon executando o mesmo sistema operacional da VM de origem
- Amazon Elastic Block Store (Amazon EBS)

Arquitetura de origem e destino

O diagrama a seguir mostra a arquitetura de alto nível e os principais componentes da solução. No datacenter on-premises, há máquinas virtuais com discos on-premises. Na AWS, há uma área de preparação com servidores de replicação e uma área de recursos migrados com EC2 instâncias para teste e transferência. As duas sub-redes contêm volumes do EBS.

1. Inicializar o Serviço de migração de aplicativos da AWS.
2. Configure a configuração e os relatórios do servidor da área de preparação, incluindo os recursos da área de preparação.
3. Instale agentes nos servidores de origem e use a replicação contínua de dados em nível de bloco (compactada e criptografada).
4. Automatize a orquestração e a conversão do sistema para reduzir a janela de substituição.

Arquitetura de rede

O diagrama a seguir mostra a arquitetura de alto nível e os principais componentes da solução do ponto de vista da rede, incluindo protocolos e portas necessários para comunicação entre os componentes principais no datacenter on-premises e na AWS.

Ferramentas

- O Serviço de migração de aplicativos da AWS ajuda você a redefinir a hospedagem (mover sem alterações (lift-and-shift)) aplicativos na nuvem da Nuvem AWS sem alterações e com o mínimo de tempo de inatividade.

Práticas recomendadas

- Não coloque o servidor de origem off-line nem execute uma reinicialização até que a transição para a EC2 instância de destino seja concluída.

- Ofereça ampla oportunidade para que os usuários realizem testes de aceitação do usuário (UAT) no servidor de destino para identificar e resolver quaisquer problemas. Idealmente, esse teste deve começar pelo menos duas semanas antes da transição.
- Monitore com frequência o status de replicação do servidor no console do Serviço de migração de aplicativos para identificar problemas logo no início.
- Use credenciais temporárias do AWS Identity and Access Management (IAM) para instalação do agente, em vez das credenciais permanentes do usuário do IAM.

Épicos

Gerar credenciais de AWS

Tarefa	Descrição	Habilidades necessárias
Crie o perfil do IAM do AWS Replication Agent.	Faça login com permissões administrativas para a Conta AWS. No console do AWS Identity and Access Management (IAM), crie um perfil do IAM: 1. No console do IAM, selecione Perfis. 2. Selecione Criar perfil. 3. Na página Selecionar entidade confiável, na seção Tipo de entidade confiável, selecione Conta da AWS. 4. Na seção Uma conta da AWS, selecione Esta conta (< account-id>). 5. Escolha Próximo. 6. Na página Adicionar permissões, pesquise	Administrador da AWS, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	a política `AWSApplicationMigrationAgentInstallationPolicy` , marque a caixa de seleção ao lado do nome da política. 7. Escolha Próximo. 8. Na página de Detalhes do perfil, insira MGN_Agent_Installation_Role como nome do perfil. 9. Verifique se os campos estão corretos e escolha Criar perfil.	

Tarefa	Descrição	Habilidades necessárias
Gerar credenciais de segurança temporárias	Em uma máquina com AWS Command Line Interface (AWS CLI) instalada, faça login com permissões administrativas. Ou, alternativamente (dentro de uma região da AWS compatível), no Console de Gerenciamento da AWS, faça login com permissões administrativas na conta da AWS e abra a AWS CloudShell. Gere credenciais temporárias com o comando a seguir, substituindo `<account-id>` pelo ID da conta da AWS. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/MGN_Agent_Installation_Role --role-session-name mgn_installation_session_role` Na saída do comando, copie os valores para `AccessKeyId`, `SecretAccessKey`, e `SessionToken`. Armazene-os em um local seguro para uso posterior.	Administrador da AWS, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	Important Essas credenciais temporárias expirarão após uma hora. Se você precisar de credenciais após uma hora, repita as etapas anteriores.	

Inicialize o Serviço de migração de aplicativos e crie o modelo de Configurações de replicação

Tarefa	Descrição	Habilidades necessárias
Inicialize o serviço.	No console, faça login com permissões administrativas para a Conta AWS. Escolha Serviço de migração de aplicativos e, em seguida, escolha Começar.	Administrador da AWS, engenheiro de migração
Crie e configure o modelo de Configurações de replicação.	1. Forneça os seguintes detalhes de configuração: a. Selecione a sub-rede da área de teste. b. Selecione o tipo de instância do servidor de replicação (`t3.small` por padrão). c. Selecione o tipo de volume do EBS (gp3 por padrão).	Administrador da AWS, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	d. Selecione a opção de criptografia do EBS. e. Certifique-se de que a caixa de seleção Sempre usar o grupo de segurança do Serviço de migração de aplicativos esteja marcada. f. Marque a caixa de seleção Usar IP privado para replicação de dados (VPN DirectConnect, emparelhamento de VPC) se você estiver usando conectividade de rede privada entre o ambiente local e a AWS. g. Marque a caixa de seleção Controle de utilização da largura de banda da rede (por servidor - em Mbps) se quiser limitar a largura de banda da rede para o Serviço de migração de aplicativos. 2. Selecione Criar modelo. O Serviço de migração de aplicativos criará automatic amente todos os perfis do IAM necessários para facilitar a replicação de dados e a	

Tarefa	Descrição	Habilidades necessárias
	inicialização de servidores migrados.	

Instale AWS Replication Agents nas máquinas de origem

Tarefa	Descrição	Habilidades necessárias
Tenha as credenciais exigidas da AWS prontas.	Ao executar o arquivo do instalador em um servidor de origem, você precisará inserir as credenciais temporári as geradas anteriormente, incluindo `AccessKeyId` , `SecretAccessKey` , e `SessionToken` .	Engenheiro de migração, administrador da AWS
Para servidores Linux, instale o agente.	Copie o comando do instalado r, faça login nos servidores de origem e execute o instalado r. Para obter instruçõe s detalhadas, consulte a Documentação da AWS.	Administrador da AWS, engenheiro de migração
Para servidores Windows, instale o agente.	Baixe o arquivo do instalado r para cada servidor e, em seguida, execute o comando do instalador. Para obter instruções detalhadas, consulte a Documentação da AWS.	Administrador da AWS, engenheiro de migração
Aguarde até que a replicaçã o inicial dos dados seja concluída.	Quando o agente for instalado , o servidor de origem aparecerá no console do Serviço de migração	Administrador da AWS, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	de aplicativos, na seção Servidores de origem. Aguarde enquanto o servidor passa pela replicação inicial dos dados.	

Define as configurações de inicialização

Tarefa	Descrição	Habilidades necessárias
Especificar os detalhes do servidor.	No console do Serviço de migração de aplicativos, escolha a seção Servidores de origem e, em seguida, escolha um nome de servidor na lista para acessar os detalhes do servidor.	Administrador da AWS, engenheiro de migração
Define as configurações de inicialização.	Escolha a guia Configura ções de inicialização. Você pode definir uma variedade de configurações, incluindo configurações gerais de lançamento e configurações do modelo de EC2 lançament o. Para obter instruçõe s detalhadas, consulte a Documentação da AWS.	Administrador da AWS, engenheiro de migração

Realize um teste

Tarefa	Descrição	Habilidades necessárias
Teste os servidores de origem.	1. No console do Serviço de migração de aplicativos, na seção Servidores de origem, certifique-se que o ciclo de vida de Migração dos servidores de origem esteja pronto para teste e que o status da replicação de dados esteja íntegro. 2. Marque a caixa de seleção à esquerda de cada servidor de origem. 3. Escolha Testar e substitui r e, em seguida, selecione Iniciar instâncias de teste. 4. Quando solicitado, escolha Inicializar. Os servidores serão inicializ ados.	Administrador da AWS, engenheiro de migração
Verifique se o teste teve êxito.	Depois que os servidores de teste forem completamente iniciados, o status de Alertas na página mostrará Iniciado para cada servidor.	Administrador da AWS, engenheiro de migração
Teste o servidor.	Execute testes no servidor de teste para garantir que ele funcione conforme o esperado.	Administrador da AWS, engenheiro de migração

Agende e realize uma substituição

Tarefa	Descrição	Habilidades necessárias
Agende uma janela de substituição.	Agende uma agenda de substituição adequado com as equipes relevantes.	Administrador da AWS, engenheiro de migração
Execute a substituição.	1. No console de migração de aplicativos, na página Servidores de origem, marque a caixa de seleção à esquerda de cada servidor de origem. 2. Escolha Teste e Substituição e selecione Marcar como “Pronto para substituição”. 3. Verifique se o ciclo de vida de migração de cada servidor de origem está pronto para ser substituído. 4. Escolha Teste e Substituição e, em seguida, selecione Inicializar instâncias de substituição. 5. Quando solicitado, escolha Inicializar. Os servidores serão inicializados. O ciclo de vida da migração do servidor de origem mudará para Substituição em andamento.	Administrador da AWS, engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Verifique se a substituição foi concluída com êxito.	Depois que os servidores de substituição forem completamente iniciados, o status de alertas na página Servidores de origem mostrará Inicializado para cada servidor.	Administrador da AWS, engenheiro de migração
Teste o servidor.	Execute testes no servidor de substituição para garantir que ele funcione conforme o esperado.	Administrador da AWS, engenheiro de migração
Finalize a substituição.	Escolha Teste e Substituição e, em seguida, selecione Finalizar substituição para finalizar o processo de migração.	Administrador da AWS, engenheiro de migração

Recursos relacionados

- Serviço de migração de aplicativos da AWS
- Guia do usuário do serviço de migração de aplicativos da AWS

Migre pequenos conjuntos de dados on-premises para o Amazon S3 usando o AWS SFTP

Criado por Charles Gibson (AWS) e Sergiy Shevchenko (AWS)

Resumo

Esse padrão descreve como migrar pequenos conjuntos de dados (5 TB ou menos) de datacenters on-premises para o Amazon Simple Storage Service (Amazon S3) usando o AWS Transfer for SFTP (AWS SFTP). Os dados podem ser despejos de banco de dados ou arquivos simples.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um link do AWS Direct Connect estabelecido entre seu datacenter e a AWS

Limitações

- Os arquivos de dados devem ter menos de 5 TB. Para arquivos acima de 5 TB, você pode realizar um upload de várias partes para o Amazon S3 ou escolher outro método de transferência de dados.

Arquitetura

Pilha de tecnologia de origem

- Arquivos simples on-premises ou despejos de banco de dados

Pilha de tecnologias de destino

- Amazon S3

Arquitetura de origem e destino

Ferramentas

- AWS SFTP: permite a transferência de arquivos diretamente para dentro e para fora do Amazon S3 usando o Secure File Transfer Protocol (SFTP).
- AWS Direct Connect: estabelece uma conexão de rede dedicada entre seus datacenters on-premises e a AWS.
- VPC endpoints — permitem que você conecte de forma privada uma VPC a serviços compatíveis da AWS e serviços de endpoint de VPC fornecidos pela AWS PrivateLink sem um gateway de internet, dispositivo de tradução de endereços de rede (NAT), conexão VPN ou conexão AWS Direct Connect. As instâncias na VPC não exigem que endereços IP públicos se comuniquem com recursos no serviço.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Documente os requisitos atuais do SFTP.		Proprietário do aplicativo e SA
Identifique os requisitos de autenticação.	Os requisitos podem incluir autenticação baseada em chave, nome de usuário ou senha ou provedor de identidades (IdP).	Proprietário do aplicativo e SA
Identifique os requisitos de integração do aplicativo.		Proprietário do aplicativo
Identifique os usuários que precisam do serviço.		Proprietário do aplicativo
Determine o nome DNS do endpoint do servidor SFTP.		Redes
Determine a estratégia de backup.		SA, DBA (se os dados forem transferidos)

Tarefa	Descrição	Habilidades necessárias
Identifique a migração do aplicativo ou a estratégia de substituição.		Proprietário do aplicativo, SA e DBA

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Crie uma ou mais nuvens privadas virtuais (VPCs) e sub-redes na sua conta da AWS.		Proprietário do aplicativo e AMS
Criar grupos de segurança e lista de controle de acesso (ACL) de rede.		Segurança, redes e AMS
Criar o bucket do S3.		Proprietário do aplicativo e AMS
Crie o perfil do IAM (identity and access management).	Crie uma política do IAM que inclua as permissões para habilitar o AWS SFTP de modo a acessar seu bucket do S3. Essa política do IAM determina o nível de acesso que você fornece aos usuários do SFTP. Crie outra política do IAM para estabelecer uma relação de confiança com o AWS SFTP.	Segurança e AMS
Associe um domínio registrado (opcional).	Se você tiver seu próprio domínio registrado, poderá associá-lo ao servidor SFTP.	Redes e AMS

Tarefa	Descrição	Habilidades necessárias
	Você pode rotear o tráfego do SFTP para o seu endpoint de servidor SFTP de um domínio ou de um subdomínio.	
Crie um servidor SFTP.	Especifique o tipo de provedor de identidade usado pelo serviço para autenticar seus usuários.	Proprietário do aplicativo e AMS
Abra um cliente SFTP.	Abra um cliente SFTP e configure a conexão para usar o host do endpoint SFTP. O AWS SFTP oferece suporte a todos os clientes SFTP padrão. Os clientes SFTP comumente usados incluem OpenSSH, WinSCP, Cyberduck e. FileZilla Você pode obter o nome do host do servidor SFTP no console do AWS SFTP.	Proprietário do aplicativo e AMS

Planejar e testar

Tarefa	Descrição	Habilidades necessárias
Planeje a migração do aplicativo.	Planeje todas as alterações necessárias na configuração do aplicativo, defina a data da migração e determine o cronograma de testes.	Proprietário do aplicativo e AMS
Teste a infraestrutura.	Teste em um ambiente que não seja de produção.	Proprietário do aplicativo e AMS

Recursos relacionados

Referências

- Guia do usuário do AWS Transfer for SFTP
- Recursos do AWS Direct Connect
- VPC Endpoints

Tutoriais e vídeos

- AWS Transfer for SFTP (vídeo)
- Guia do usuário do AWS Transfer for SFTP
- AWS SA Whiteboarding - Direct Connect (vídeo)

Migre da Oracle GlassFish para o AWS Elastic Beanstalk

Criado por Sandeep Bondugula (AWS)

Resumo

Esse padrão descreve como migrar um aplicativo Java executado em um GlassFish servidor Oracle local para o AWS Elastic Beanstalk na nuvem da AWS.

Na AWS, o aplicativo Java é implantado em um GlassFish servidor Docker com o AWS Elastic Beanstalk, que é executado em um grupo de Auto Scaling da Amazon Elastic Compute Cloud (EC2Amazon).

Atributos adicionais:

- o Amazon Elastic Beanstalk atua como um invólucro para vários recursos subjacentes. Ele configura o Elastic Load Balancing (que gerencia o tráfego de entrada do Amazon Route 53), dispersa o tráfego para uma ou mais EC2 instâncias e também serve como uma ferramenta de implantação.
- Para migrar um banco de dados on-premises para o Amazon Relational Database Service (Amazon RDS), atualize os detalhes da conexão do banco de dados. No banco de dados de backend, você pode configurar as implantações Multi-AZ do Amazon RDS e escolher o tipo de mecanismo de banco de dados.
- Você pode usar a implantação Multi-AZ para obter alta disponibilidade junto com o grupo do Auto Scaling e a política de escalabilidade para melhorar a resiliência.
- Você pode configurar uma política de escalabilidade com base nas CloudWatch métricas da Amazon.
- No AWS Elastic Beanstalk, você pode definir as configurações subjacentes do Elastic Load Balancing e o Amazon Auto Scaling. EC2

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo Java local em execução em GlassFish
- Um arquivo Java Web Application Resource (WAR)

Versões do produto

- Oracle Glassfish 4.1.2 e 5.0
- Java 7 GlassFish 4.0
- Java 8 GlassFish 4.1 ou posterior

Arquitetura

Pilha de tecnologia de origem

- Aplicativos desenvolvidos em GlassFish

Pilha de tecnologias de destino

- Elastic Beanstalk

Arquitetura de destino

Fluxo de trabalho de implantação

Ferramentas

- Amazon Elastic Beanstalk: é um serviço para implantação e escalabilidade de aplicativos web e serviços desenvolvidos com Java, .NET, PHP, Node.js, Python, Ruby, Go e Docker em servidores familiares, como Apache, Nginx, Passenger e IIS.
- Amazon CloudWatch — fornece dados e insights acionáveis para monitorar aplicativos, responde às mudanças de desempenho em todo o sistema, otimiza a utilização de recursos e fornece uma visão unificada da integridade operacional.
- Docker: uma plataforma que empacota software em unidades padronizadas para criar, testar e implantar aplicativos rapidamente.
- Java: uma linguagem de programação de uso geral. O Java é baseado em classes, orientado a objetos e projetado para ter menos dependências de implementação.

Épicos

Configurar uma VPC

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de nuvem privada virtual (VPC) com as informações necessárias.		SysAdmin
Crie pelo menos duas sub-redes na VPC.		SysAdmin
Crie uma tabela de rotas segundo com os requisitos.		SysAdmin

Configure o Amazon S3

Tarefa	Descrição	Habilidades necessárias
Crie um bucket do Amazon Simple Storage Service (Amazon S3).		SysAdmin
Copie o arquivo WAR para o bucket do S3 e faça upload do código do aplicativo.		SysAdmin

Criar um perfil do IAM

Tarefa	Descrição	Habilidades necessárias
Crie um perfil do IAM do AWS Identity and Access Management (IAM).	Você pode usar o perfil padrão de “aws-elasticbeanstalk-ec2 funções” ou deixar que o Elastic Beanstalk o crie automaticamente.	SysAdmin

Configurar Elastic Beanstalk

Tarefa	Descrição	Habilidades necessárias
Abra o painel do Elastic Beanstalk.		SysAdmin
Crie um novo aplicativo e escolha o ambiente do servidor web.		SysAdmin
Escolha o GlassFish Docker como plataforma pré-confi gurada.		SysAdmin
Fazer upload do código.	Forneça o URL do arquivo de bucket do S3 ou o arquivo ZIP dos arquivos do sistema local.	SysAdmin
Escolha o tipo de ambiente.	Nas Configurações de capacidade de configuração, escolha Instância única ou Balanceador de carga.	SysAdmin
Configurar o balanceador de carga	Se você escolheu Balancead or de carga na etapa anterior, configure implantação multi-AZ.	SysAdmin
Nas Configurações de segurança, escolha o perfil do IAM criado anteriormente.		SysAdmin
Nas configurações de segurança da configuração, se você tiver um par de chaves existente, use-o ou crie um		SysAdmin

Tarefa	Descrição	Habilidades necessárias
novo par de EC2 chaves da Amazon.		
Nas configurações de monitoramento de configuração, configure a Amazon CloudWatch.		SysAdmin
Nas Configurações de segurança, escolha a VPC criada anteriormente.		SysAdmin
Selecione Criar ambiente		SysAdmin

Teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Teste o aplicativo usando o URL fornecido no ambiente criado.		
Aplique as alterações do Serviço de nomes de domínio (DNS) no Amazon Route 53.		

Recursos relacionados

- GlassFish Documentação da Oracle
- GlassFish Implementação de referência Java EE de código aberto
- Documentação do AWS Elastic Beanstalk
- Usando o Elastic Beanstalk com a Amazon CloudWatch
- Definição de preço do AWS Elastic Beanstalk
- EC2 Grupo de Auto Scaling

- Escalabilidade do tamanho de seu grupo do Auto Scaling
- Implantações multi-AZ do Amazon RDS

Migre um banco de dados Oracle local para o Oracle na Amazon EC2

Criado por Baji Shaik (AWS) e Pankaj Choudhary (AWS)

Resumo

Esse padrão orienta você pelas etapas de migração de um banco de dados Oracle local para a Oracle em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Ele descreve duas opções de migração: usar o AWS Data Migration Service (AWS DMS) ou usar ferramentas nativas da Oracle, como RMAN, importação/exportação do Data Pump, espaços de tabela transportáveis e Oracle. GoldenGate

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle de origem em um datacenter on-premises

Limitações

- O sistema operacional (SO) de destino deve ser suportado pela Amazon EC2. Para obter uma lista completa dos sistemas compatíveis, consulte Amazon EC2 FAQs.

Versões do produto

- Oracle versões 10.2 e posterior (para versões 10.x), 11g e até 12.2 e 18c para as edições Enterprise, Standard, Standard One e Standard Two. Para obter a lista mais recente de versões suportadas pelo AWS DMS, consulte “Bancos de dados de EC2 instâncias locais e da Amazon” em Fontes para migração de dados na documentação do AWS DMS.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Oracle on-premises

Pilha de tecnologias de destino

- Uma instância de banco de dados Oracle na Amazon EC2

Arquitetura de destino

Arquitetura de migração de dados

Uso do AWS DMS:

Uso de ferramentas nativas da Oracle:

Ferramentas

- AWS DMS: o AWS Database Migration Services (AWS DMS) oferece suporte a vários bancos de dados de origem e destino. Para obter informações sobre as versões e edições do banco de dados compatíveis, consulte Uso de um banco de dados Oracle como origem para o AWS DMS. Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos.
- Ferramentas nativas da Oracle - RMAN, importação/exportação de Data Pump, espaços de tabela transportáveis, Oracle GoldenGate

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões dos bancos de dados de origem e de destino.		DBA
Identifique a versão do sistema operacional de destino.		DBA, SysAdmin
Identificar os requisitos de hardware para a instância do		DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
servidor de destino com base na lista de compatibilidade da Oracle e nos requisitos de capacidade.		
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, SysAdmin
Identifique os requisitos de rede (latência e largura de banda).		DBA, SysAdmin
Escolher o tipo de instância adequado com base na capacidade, nos atributos de armazenamento e nos atributos de rede.		DBA, SysAdmin
Identificar os requisitos de segurança de acesso à rede/ host para bancos de dados de origem e destino.		DBA, SysAdmin
Identifique uma lista de usuários do sistema operacion al necessários para a instalação do software Oracle.		DBA, SysAdmin
Faça o download da AWS Schema Conversion Tool (AWS SCT) e dos drivers.		DBA
Crie um projeto AWS SCT para o workload e conecte-se ao banco de dados de origem.		DBA

Tarefa	Descrição	Habilidades necessárias
Gere arquivos SQL para a criação de objetos (tabelas, índices, sequências etc.).		DBA
Determine uma estratégia de backup.		DBA, SysAdmin
Determine os requisitos de disponibilidade.		DBA
Identifique a migração de aplicativos / a estratégia de transição.		DBA SysAdmin, proprietário do aplicativo

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Crie uma nuvem privada virtual (VPC) e sub-redes na sua conta da AWS.		SysAdmin
Crie grupos de segurança e listas de controle de acesso à rede (ACLs).		SysAdmin
Configure e inicie a EC2 instância.		SysAdmin

Instalar o software Oracle

Tarefa	Descrição	Habilidades necessárias
Crie os usuários e grupos do sistema operacional necessários para o software Oracle.		DBA, SysAdmin
Baixe a versão necessária do software Oracle.		
Instale o software Oracle na EC2 instância.		DBA, SysAdmin
Crie objetos como tabelas, chaves primárias, visualizações e sequências usando os scripts gerados pelo AWS SCT.		DBA

Migrar dados - opção 1

Tarefa	Descrição	Habilidades necessárias
Use ferramentas nativas da Oracle ou ferramentas de terceiros para migrar dados e objetos do banco de ados.	As ferramentas da Oracle incluem importação/exportação do Data Pump, RMAN, espaços de tabela transportáveis e. GoldenGate	DBA

Migrar dados - opção 2

Tarefa	Descrição	Habilidades necessárias
Determine o método de migração.		DBA

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de replicação no console do AWS DMS.		DBA
Crie endpoints de origem e de destino.		DBA
Criar uma tarefa de replicaçã o.		DBA
Habilite a captura de dados de alteração (CDC) para capturar alterações para uma replicaçã o contínua.		DBA
Execute a tarefa de replicação e monitore os logs.		DBA
Crie objetos secundários, como índices e chaves estrangeiras, quando o carregamento completo estiver concluído.		DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Substituir

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de substituição/transição de aplicativo.		DBA SysAdmin, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários do AWS Secrets Manager.		DBA, SysAdmin
Revise e valide os documentos do projeto.		DBA SysAdmin, proprietário do aplicativo
Reúna métricas sobre o tempo de migração, % de manual x ferramenta, economia de custos etc.		DBA SysAdmin, proprietário do aplicativo
Feche o projeto e forneça feedback.		

Recursos relacionados

Referências

- Estratégias para migrar bancos de dados Oracle para a AWS
- Migrar bancos de dados Oracle para a Nuvem AWS
- EC2 Site da Amazon
- Site do AWS DMS
- Publicações no blog do AWS DMS
- EC2 Preços da Amazon
- Licenciamento do software Oracle no ambiente de computação em nuvem

Tutoriais e vídeos

- Começando com a Amazon EC2
- Conceitos básicos do AWS DMS
- Introdução à Amazon EC2 — Elastic Cloud Server e hospedagem com AWS (vídeo)

Migre um banco de dados Oracle local para a Amazon EC2 usando o Oracle Data Pump

Criado por Navakanth Talluri (AWS)

Resumo

Ao migrar bancos de dados, você deve considerar fatores como os mecanismos e as versões do banco de dados de origem e de destino, ferramentas e serviços de migração e períodos de inatividade aceitáveis. Se você estiver migrando um banco de dados Oracle local para o Amazon Elastic Compute Cloud (Amazon EC2), você pode usar ferramentas da Oracle, como o Oracle Data Pump e o Oracle Recovery Manager (RMAN). Para obter mais informações sobre estratégias, consulte Migração de bancos de dados Oracle para a nuvem AWS.

O Oracle Data Pump ajuda você a extrair o backup lógico e consistente do banco de dados e restaurá-lo na EC2 instância de destino. Esse padrão descreve como migrar um banco de dados Oracle local para uma EC2 instância usando o Oracle Data Pump e o `NETWORK_LINK` parâmetro, com o mínimo de tempo de inatividade. O `NETWORK_LINK` parâmetro inicia uma importação por meio de um link de banco de dados. O cliente Oracle Data Pump Import (impdp) na EC2 instância de destino se conecta ao banco de dados de origem, recupera dados dele e grava os dados diretamente no banco de dados na instância de destino. Não há arquivos de backup ou de despejo usados nessa solução.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados da Oracle no on-premises que:
  - Não é um banco de dados Oracle Real Application Clusters (RAC)
  - Não é um banco de dados Oracle Automatic Storage Management (Oracle ASM)
  - Está no modo leitura/gravação.
- Você criou um link do AWS Direct Connect entre o datacenter on-premises e a AWS. Para obter mais informações, consulte Criar uma conexão (documentação do Direct Connect).

Versões do produto

- Oracle Database 10g Versão 1 (10.1) e posteriores

Arquitetura

Pilha de tecnologia de origem

- Um servidor de banco de dados Oracle autônomo (não RAC e não ASM) em um datacenter on-premises

Pilha de tecnologias de destino

- Um banco de dados Oracle em execução na Amazon EC2

Arquitetura de destino

O pilar de confiabilidade do AWS Well-Architected Framework recomenda a criação de backups de dados para ajudar a fornecer alta disponibilidade e resiliência. Para obter mais informações, consulte Arquitetura para alta disponibilidade em Melhores práticas para execução do banco de dados Oracle na AWS. Esse padrão configura bancos de dados primários e standby em EC2 instâncias usando o Oracle Active Data Guard. Para alta disponibilidade, as EC2 instâncias devem estar em zonas de disponibilidade diferentes. No entanto, as zonas de disponibilidade podem estar na mesma região da AWS ou em regiões da AWS diferentes.

O Active Data Guard fornece acesso somente de leitura a um banco de dados físico em espera e aplica alterações de redo continuamente a partir do banco de dados principal. Com base no objetivo de ponto de recuperação (RPO) e no objetivo de tempo de recuperação (RTO) da, você pode escolher entre as opções de transporte de redo síncrono e assíncrono.

A imagem a seguir mostra a arquitetura de destino se as EC2 instâncias primária e em espera estiverem em diferentes regiões da AWS.

Arquitetura de migração de dados

Depois de concluir a configuração da arquitetura de destino, você usa o Oracle Data Pump para migrar os dados e esquemas locais para a instância primária. EC2 Durante a substituição, os aplicativos não podem acessar o banco de dados on-premises ou o banco de dados de destino. Você desliga esses aplicativos até que eles possam ser conectados ao novo banco de dados de destino na EC2 instância primária.

A imagem a seguir mostra a arquitetura durante a migração de dados. Neste exemplo de arquitetura, as EC2 instâncias primária e em espera estão em diferentes regiões da AWS.

Ferramentas

Serviços da AWS

- O AWS Direct Connect conecta sua rede interna a um local do Direct Connect por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para serviços públicos da AWS, ignorando provedores de serviço da internet no caminho da sua rede.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.

Outras ferramentas e serviços

- O Oracle Active Data Guard ajuda você a criar, manter, gerenciar e monitorar bancos de dados em espera.
- O Oracle Data Pump ajuda você a mover dados e metadados de um banco de dados para outro em alta velocidade.

Práticas recomendadas

- Melhores práticas para execução do Oracle Database na AWS
- Importação de dados usando NETWORK_LINK

Épicos

Configure as EC2 instâncias na AWS

Tarefa	Descrição	Habilidades necessárias
Identifique a configuração do hardware de origem para o host on-premises e os parâmetros do kernel.	Valide a configuração on-premises, incluindo tamanho de armazenam ento, operações de entrada e saída por segundo (IOPS) e	DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
	CPU. Isso é importante para o licenciamento da Oracle, que é baseado em núcleos de CPU.	
Crie a infraestrutura na AWS.	Crie nuvens privadas virtuais (VPCs), sub-redes privadas, grupos de segurança, listas de controle de acesso à rede (ACLs), tabelas de rotas e gateway de internet. Para obter mais informações, consulte: • VPCs e sub-redes • Tutorial: criar uma VPC para uso com uma instância de banco de dados	DBA, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Configure as EC2 instâncias usando o Active Data Guard.	Configure EC2 instâncias da AWS usando uma configuração do Active Data Guard, conforme descrito no AWS Well-Architected Framework. A versão do Oracle Database na EC2 instância pode ser diferente da versão local porque esse padrão usa backups lógicos. Observe o seguinte: • Coloque o banco de dados de destino no modo de leitura e gravação. • No banco de dados de destino, forneça os detalhes do Transparent Network Substrate (TNS) do banco de dados de origem. Para obter mais informações, consulte: • Inicializando um banco de dados (documentação da Oracle) • Criando e configurando um banco de dados Oracle (documentação da Oracle)	DBA, administrador de sistemas da AWS

Migre o banco de dados para a Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Crie um dblink para o banco de dados local a partir da instância. EC2	Crie um link de banco de dados (dblink) entre o banco de dados Oracle na EC2 instância e o banco de dados Oracle local. Para obter mais informações, consulte Usando a importação de link de rede para mover dados (document ação da Oracle).	DBA
Verifique a conexão entre a EC2 instância e o host local.	Use o dblink para confirmar se a conexão entre a EC2 instância e o banco de dados local está funcionando. Para obter instruções, consulte CREATE DATABASE LINK (documentação da Oracle).	DBA
Pare todos os aplicativos conectados ao banco de dados on-premises.	Depois que o tempo de inatividade do banco de dados for aprovado, encerre todos os aplicativos e trabalhos dependentes conectados ao seu banco de dados on-premises. Você pode fazer isso diretamente do aplicativ o ou do banco de dados usando o cron. Para obter mais informações, consulte Usar o utilitário Crontab para agendar tarefas no Oracle Linux.	DBA, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Agende o trabalho de migração de dados.	No host de destino, use o comando `impdb` para agendar a importação do Data Pump. Isso conecta o banco de dados de destino ao host on-premises e inicia a migração de dados. Para obter mais informações, consulte Data Pump Import e NETWORK_LINK (documentação da Oracle).	DBA
Valide a migração de dados.	A validação de dados é uma etapa crucial. Para validação de dados, você pode usar ferramentas personalizadas ou ferramentas Oracle, como uma combinação de consultas dblink e SQL.	DBA

Substituir

Tarefa	Descrição	Habilidades necessárias
Colocar o banco de dados de origem em um modo somente leitura.	Confirme se o aplicativo foi encerrado e se nenhuma alteração está sendo feita no banco de dados de origem. Abra o banco de dados de origem no modo somente leitura. Isso ajuda você a evitar transaçõe s abertas. Para ter mais informações, consulte `ALTER`	DBA, DevOps engenheiro, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`DATABASE`Em SQL Statements (documentação da Oracle).	
Valide a contagem de objetos e os dados.	Para validar os dados e o objeto, use ferramentas personalizadas ou ferramentas Oracle, como uma combinação de consultas dblink e SQL.	DBA, desenvolvedor de aplicativos
Conecte os aplicativos ao banco de dados na EC2 instância primária.	Altere o atributo de conexão do aplicativo para apontar para o novo banco de dados que você criou na EC2 instância primária.	DBA, desenvolvedor de aplicativos
Valide o desempenho do aplicativo.	Iniciar o aplicativo Valide a funcionalidade e o desempenho do aplicativo usando o Automated Workload Repository (documentação da Oracle).	Desenvolvedor de aplicativos, DevOps engenheiro, DBA

Recursos relacionados

Referências da AWS

- Migrar bancos de dados Oracle para a Nuvem AWS
- Amazon EC2 para Oracle
- Migração de bancos de dados Oracle volumosos para a AWS para ambientes multiplataforma
- VPCs e sub-redes
- Tutorial: criar uma VPC para uso com uma instância de banco de dados

Referências da Oracle

- Configurações do Oracle Data Guard
- Importação da bomba de dados

Migre sistemas RHEL BYOL para instâncias com licença incluída da AWS usando o AWS MGN

Criado por Mike Kuznetsov (AWS)

Resumo

Ao migrar suas workloads para a AWS usando o AWS Application Migration Service (AWS MGN), talvez você precise mover sem alterações (lift-and-shift) (redefinir a hospedagem) as suas instâncias do Red Hat Enterprise Linux (RHEL) e alterar a licença do modelo padrão traga a sua própria licença (BYOL) para um modelo AWS License Included (LI) durante a migração. O AWS MGN oferece suporte a uma abordagem escalável que usa Amazon Machine Image (AMI). IDs Esse padrão descreve como realizar a alteração da licença nos servidores RHEL durante a migração de redefinição de hospedagem em grande escala. Também explica como alterar a licença de um sistema RHEL que já está em execução no Amazon Elastic Compute Cloud (Amazon EC2).

Pré-requisitos e limitações

Pré-requisitos

- Acesso à conta de destino da AWS
- O AWS MGN foi inicializado na conta e região da AWS de destino para a migração (não é necessário se você já tiver migrado do seu sistema on-premises para a AWS)
- Um servidor RHEL de origem com uma licença RHEL válida

Arquitetura

Esse padrão abrange dois cenários:

- Migração de um sistema on-premises diretamente para uma instância do AWS LI usando o AWS MGN. Para esse cenário, siga as instruções no primeiro épico (Migrar para a instância de LI - opção 1) e no terceiro épico.
- Alteração do modelo de licenciamento de BYOL para LI para um sistema RHEL migrado anteriormente que já está em execução na Amazon. EC2 Para esse cenário, siga as instruções no segundo épico (Migrar para a instância de LI - opção 2) e no terceiro épico.

> **Note**
>
> O terceiro épico envolve a reconfiguração da nova instância do RHEL para usar os servidores Red Hat Update Infrastructure (RHUI) fornecidos pela AWS. Esse processo é o mesmo para os dois cenários.

Ferramentas

Serviços da AWS

- O AWS Application Migration Service (AWS MGN) ajuda você a redefinir a hospedagem aplicativos (mover sem alterações (lift-and-shift)) na nuvem AWS sem alterações e com o mínimo de tempo de inatividade.

Épicos

Migrar para a instância LI - opção 1 (para um sistema RHEL on-premises)

Tarefa	Descrição	Habilidades necessárias
Encontre o ID da AMI da instância RHEL AWS LI na região de destino.	Visite o AWS Marketplace ou use o EC2 console da Amazon para encontrar a ID da AMI RHEL que corresponda à versão do sistema de origem da RHEL (por exemplo, RHEL-7.7) e anote a ID da AMI. No EC2 console da Amazon, você pode filtrar o AMIs usando um dos seguintes termos de pesquisa: • Descrição = Fornecida pela Red Hat, Inc. • Nome da AMI = RHEL-7.7	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Defina as configurações de lançamento do AWS MGN.	1. No console do AWS MGN, adicione o sistema RHEL de origem: instale o AWS Replication Agent e adicione o servidor de origem seguindo as instruções na documentação do AWS MGN. 2. Na página Servidores de origem, escolha o sistema RHEL de origem e, em seguida, escolha a guia Configurações de inicialização. 3. Na seção Settings (Configurações), escolha Edit (Editar). Para desativar a seleção automática e especificar manualmente o tipo de instância de destino, altere o Tamanho correto do tipo de instância para Nenhum e escolha Salvar configurações. Isso permite que você use o tipo de instância que você configura no seu modelo de EC2 lançamento da Amazon. Para obter mais informações, consulte a documentação do AWS MGN. 4. Na seção EC2 Launch Template, escolha Modificar	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	. Na caixa de diálogo Sobre a modificação de modelos de EC2 lançamento, escolha Modificar novamente. Isso abre o EC2 console da Amazon para que você possa alterar o modelo dessa instância. 5. Analise as principais considerações na documentação do AWS MGN. **Note** Você pode ignorar o aviso de não escolher sua própria AMI. 6. No EC2 console da Amazon, no novo modelo de lançamento, modifique o seguinte: • Para AMI, especifique o ID da AMI que você identificou anteriormente ou pesquise por RHEL-x e especifique a versão necessária (por exemplo, RHEL-7.7). • Em Tipo de instância, defina o tipo de instância de destino desejado.	

Tarefa	Descrição	Habilidades necessárias
	• Deixe as seguintes seções inalteradas: Par de chaves (login), Configurações de rede (a menos que você queira especificar uma sub-rede de destino e grupos de segurança), Armazenamento, Tags de recursos (a menos que você queira adicionar ou modificar alguma tag). • (Opcional) Na seção Detalhes avançados, especifique a função do perfil de instância do IAM, se necessário, para gerenciamento futuro pelo AWS Systems Manager. 7. Escolha Criar versão do modelo e, em seguida, escolha o link na mensagem de sucesso para visualizar o modelo de lançamento. 8. Escolha Ações, Definir versão padrão. Em Versão do modelo, selecione a versão mais recente (versão 2 para um novo sistema) e escolha Definir como versão padrão.	

Tarefa	Descrição	Habilidades necessárias
	Agora, o AWS MGN usará essa versão do modelo de lançamento para iniciar instâncias de teste ou de substituição. Para obter mais informações, consulte a documentação do AWS MGN.	

Tarefa	Descrição	Habilidades necessárias
Valide as configurações.	1. No console do AWS MGN, na página Servidores de origem, escolha seu servidor de origem e, em seguida, escolha a guia Configurações de inicializ ação. 2. Na seção EC2 Launch Template, verifique se os parâmetros Tipo de instância, sub-rede e grupos de segurança estão definidos corretamente. **Note** Essa seção não exibe a ID da AMI que você seleciono u. Para ver o ID, você pode abrir o EC2 console da Amazon, exibir Launch Templates e pesquisar o ID do modelo mostrado nesta seção.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Inicie a nova instância de LI.	1. Quando a sincronização inicial é concluída, a coluna do Ciclo de vida da migração para o servidor na página de Servidores de origem do console AWS MGN muda para Pronto para teste. Para iniciar a nova instância de teste, escolha seu servidor de origem, abra o menu Teste e substituição e, em seguida, escolha Iniciar instâncias de teste. Escolha Exibir detalhes do trabalho para monitorar o status do trabalho de inicialização. Para obter mais informações, consulte a documentação do AWS MGN. 2. Aguarde a conclusão do trabalho de inicialização e, em seguida, abra a página de detalhes da EC2 instância executada. Escolha a guia Detalhes e verifique se a seção Detalhes da instância contém o seguinte: • Detalhes da plataforma: “Red Hat Enterprise Linux” • Nome da AMI: o nome da AMI que você especific	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	ou no modelo de EC2 lançamento 3. Vá para a nova instância de LI seguindo as instruções na documentação do AWS MGN. 4. Reconfigure a nova instância para usar os servidores RHUI fornecidos pela AWS seguindo as etapas do último épico.	

Migrar para a instância LI - opção 2 (para uma instância RHEL EC2 BYOL)

Tarefa	Descrição	Habilidades necessárias
Migre sua instância RHEL BYOL para uma EC2 instância AWS LI.	Você pode alternar os sistemas RHEL que você migrou anteriormente para a AWS como BYOL para instâncias do AWS LI movendo seus discos (volumes do Amazon Elastic Block Store) e anexando-os a uma nova instância de LI. Para fazer essa troca, siga estas etapas: 1. Execute uma nova instância RHEL de destino a partir de uma AMI RHEL LI. Certifique-se de que a AMI que você selecionou:	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	• Usa a mesma versão do RHEL da sua instância atual do RHEL. • Tem o mesmo processo de inicialização (BIOS ou UEFI) da sua instância RHEL atual. Por exemplo, se o servidor de origem for baseado em BIOS, use a AMI RHEL do AWS Marketplace que também é baseada em BIOS; para sistemas baseados em UEFI, escolha a AMI baseada em UEFI. 2. Pare as duas instâncias: a nova instância de LI e a instância de origem original. 3. Separe todos os volumes do EBS (incluindo o disco raiz) da nova instância de LI e exclua-os. 4. Separe todos os volumes do EBS (incluindo o disco raiz) da instância de origem antiga e anexe-os à nova instância de LI. Mantenha o mesmo mapeamento de volumes para dispositivos. (Por exemplo, o volume do EBS que estava anteriormente conectado à unidade `/dev/sda` deve	

Tarefa	Descrição	Habilidades necessárias
	ser conectado como `/dev/sda` à nova instância.) 5. Exclua a instância de origem (agora sem disco). 6. Inicie a nova instância de LI. Faça login na instância e reconfigure-a para usar os servidores RHUI fornecidos pela AWS seguindo as etapas do próximo épico.	

Reconfigure o sistema operacional RHEL para usar o RHUI fornecido pela AWS – ambas as opções

Tarefa	Descrição	Habilidades necessárias
Cancele o registro do sistema operacional da assinatura e da licença da Red Hat.	Após a migração e a substituição bem-sucedida, o sistema RHEL precisa ser removido da assinatura da Red Hat para parar de consumir a licença da Red Hat e evitar a cobrança dupla. Para remover o RHEL OS da assinatura Red Hat, siga o processo descrito na documentação do Red Hat Subscription Management (RHSM). Use o comando de CLI de : `subscription-manager unregister`	Administrador do Linux ou do sistema

Tarefa	Descrição	Habilidades necessárias
	Você também pode desativar o plug-in do gerenciador de assinaturas para parar de verificar o status da assinatura em cada chamada do yum. Para fazer isso, edite o arquivo de configuração `/etc/yum/pluginconf.d/subscription-manager.conf` e altere o parâmetro `enabled=1` para `enabled=0` .	

Tarefa	Descrição	Habilidades necessárias
Substitua a configuração de atualização antiga (RHUI, rede Red Hat Satellite, repositórios yum) pela RHUI fornecida pela AWS.	Você deve reconfigurar o sistema RHEL migrado para usar os servidores RHUI fornecidos pela AWS. Isso lhe dá acesso aos servidores RHUI nas regiões da AWS sem exigir a infraestrutura de atualização externa. O processo inclui as seguintes etapas: 1. Faça backup da configuração do yum existente. 2. Remova a configuração e os pacotes antigos do RHUI (repositórios yum). 3. Adicione a nova configuração RHUI e os pacotes de certificados fornecidos pela AWS. Você precisa recuperá-los de outra instância do RHEL na AWS porque esses pacotes de configuração estão disponíveis somente nos servidores RHUI fornecidos pela AWS. Aqui estão as etapas e comandos detalhados: 1. Faça backup da configuração e dos certificados existentes do yum copiando	Administrador do Linux ou do sistema

Tarefa	Descrição	Habilidades necessárias

	todas as pastas `/etc/yum*` e `/etc/pki/*` em um local de backup. Por exemplo:
	`mkdir yum-backup`
	`cp -ra /etc/yum* /etc/pki ./yum-backup`
	`tar czf yum-backup.tgz ./yum-backup`
	2. Remova a configuração e os pacotes antigos do RHUI:
	a. Encontre todos os pacotes RHUI instalados:
	`sudo rpm -qa | grep rhui`
	b. Exclua esses pacotes:
	`sudo yum remove $(rpm -qa | grep rhui)`
	c. Remova o arquivo `/etc/yum/vars/releasever`, se ele existir.
	3. Adicione os novos pacotes de certificados e RHUI fornecidos pela AWS. Você deve recuperá-los de outra instância do RHEL na AWS. Há várias maneiras de fazer isso. Por exemplo, você pode seguir as instruções	

Tarefa	Descrição	Habilidades necessárias

	fornecidas no artigo do Red Hat Knowledgebase:
	a. Execute outra instância do RHEL (RHEL-EC2) no AWS Marketplace.
	b. Faça o download de dois pacotes dessa instância : o pacote de configura ção do cliente RHUI mais recente e os certificados de autoridade de certifica ção (CA). Por exemplo, execute este comando na sua área de trabalho:
	`ssh RHEL-EC2 "sudo yumdownloader ca-certificates rh-amazon-rhui-client"`
	c. Copie os pacotes da EC2 instância RHEL- para o novo sistema migrado. Por exemplo:
	`scp RHEL-EC2:rh-amazon-rhui-client\* RHEL-EC2:ca-certificates\* .`
	`ssh <migrated-instance> "mkdir /tmp/amazon"`
	`scp rh-amazon-rhui-client* ca-certificates* <migrated`	

Tarefa	Descrição	Habilidades necessárias

	`-instance>:/tmp/am azon`
	d. Instale os novos pacotes de configuração RHUI e CA na instância migrada:
	`ssh <migrated- instance> "sudo rpm -Uhv /tmp/amazon/ *"`	

Valide a configuração.	Na instância migrada de destino, verifique se a nova configuração está correta:
	`sudo yum clean all`
	`sudo yum repolist`
		Administrador do Linux ou do sistema

Recursos relacionados

- Guia do usuário do AWS Application Migration Service (AWS MGN)
- Obtenha suporte para um pacote de cliente AWS RHUI IMDSv2 (artigo da Red Hat Knowledgebase)
- Modelos de EC2 lançamento da Amazon (EC2 documentação da Amazon)

Migre um banco de dados SAP ASE local para a Amazon EC2

Criado por Sergey Dmitriev (AWS) e Gergely Cserdi (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados SAP Adaptive Server Enterprise (ASE) de um host local para uma instância do Amazon Elastic Compute Cloud (Amazon). EC2 O padrão abrange o uso de ferramentas nativas do AWS Database Migration Service (AWS DMS) ou do SAP ASE, como ASE Cockpit, Sybase Central para ASE e DBA Cockpit para migração.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados SAP ASE de origem em um datacenter on-premises

Limitações

- O banco de dados de origem deve ter menos de 64 TB.

Versões do produto

- SAP ASE versão 15.x e 16.x ou superior

Arquitetura

Pilha de tecnologia de origem

- Banco de dados SAP ASE on-premises

Pilha de tecnologias de destino

- Banco de dados SAP ASE em uma EC2 instância

Arquitetura de migração de banco de dados

Usando o AWS DMS:

Usando ferramentas nativas do SAP ASE:

Ferramentas

- AWS DMS - AWS Data Migration Service (AWS DMS) oferece suporte a vários bancos de dados de origem e destino diferentes. Para obter mais informações, consulte Origens para migração de dados e Destinos para migração de dados Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos.
- SAP ASE — As ferramentas nativas incluem ASE Cockpit, Sybase Central para ASE e DBA Cockpit.

Épicos

Analise a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões dos bancos de dados de origem e de destino.		DBA
Identifique a versão do sistema operacional de destino.		DBA, SysAdmin
Identifique os requisitos de hardware para as instância s do servidor de origem e de destino com base na lista de compatibilidade do SAP ASE e nos requisitos de capacidad e da Oracle.		DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
Identifique os requisitos para o tipo e capacidade de armazenamento.		DBA, SysAdmin
Identifique os requisitos de rede, incluindo latência e largura de banda.		DBA, SysAdmin
Escolha o tipo de instância, a capacidade, os atributos de armazenamento e os atributos de rede adequados.		DBA, SysAdmin
Identifique os requisitos de segurança de acesso à rede e host para os bancos de dados de origem e de destino.		DBA, SysAdmin
Identifique uma lista de usuários do sistema operacional necessários para a instalação do software SAP ASE.		DBA, SysAdmin
Determine a estratégia de backup.		DBA
Determine os requisitos de disponibilidade.		DBA
Identifique a estratégia de transição e alternância de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC) e sub-redes.		SysAdmin
Criar grupos de segurança e lista de controle de acesso (ACL) de rede.		SysAdmin
Configure e inicie a EC2 instância.		SysAdmin

Instale o software

Tarefa	Descrição	Habilidades necessárias
Crie os usuários e grupos do sistema operacional necessários para que o software SAP ASE funcione.		DBA, SysAdmin
Baixe a versão necessária do software SAP ASE.		DBA, SysAdmin
Instale o banco de dados SAP ASE, o software do servidor de backup e o software do servidor de replicação na EC2 instância e, em seguida, configure o servidor.		DBA, SysAdmin

Migrar os dados - opção 1

Tarefa	Descrição	Habilidades necessárias
Use ferramentas nativas do SAP ASE ou terceirizadas para migrar objetos e dados do banco de dados.	Consulte a documentação do SAP ASE ou de ferramentas de terceiros. Elas incluem ASE Cockpit, Sybase Central para ASE e DBA Cockpit.	DBA

Migrar os dados - opção 2

Tarefa	Descrição	Habilidades necessárias
Migre os dados usando o AWS DMS.		DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Substituir

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de substituição ou transição de aplicativos.		DBA SysAdmin, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, SysAdmin
Valide e revise os documentos do projeto.		DBA SysAdmin, proprietário do aplicativo
Reúna métricas sobre o tempo de migração, porcentagem de manual versus economia de custos de ferramentas. etc.		DBA SysAdmin, proprietário do aplicativo
Feche o projeto e forneça feedback, se houver.		DBA SysAdmin, proprietário do aplicativo

Recursos relacionados

Referências

- Amazon EC2
- AWS DMS
- EC2 Preços da Amazon

Tutoriais e vídeos

- Começando com a Amazon EC2
- Introdução ao AWS Database Migration Service
- AWS Database Migration Service (vídeo)
- Introdução à Amazon EC2 — Elastic Cloud Server e hospedagem com AWS (vídeo)

Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2

Criado por Senthil Ramasamy (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados local do Microsoft SQL Server para o Microsoft SQL Server em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Ele abrange duas opções de migração: usar AWS Database Migration Service (AWS DMS) ou usar ferramentas nativas do Microsoft SQL Server, como backup e restauração, Copy Database Wizard ou copiar e anexar banco de dados.

Pré-requisitos e limitações

Pré-requisitos

- Uma AWS conta ativa
- Um sistema operacional suportado pela Amazon EC2 (para obter uma lista completa das versões suportadas do sistema operacional, consulte Amazon EC2 FAQs)
- Um banco de dados de origem do Microsoft SQL Server em um datacenter on-premises

Versões do produto

- Para bancos de dados locais e de EC2 instâncias da Amazon, AWS DMS oferece suporte a:
  - SQL Server versões 2005, 2008, 2008R2, 2012, 2014, 2016, 2017 e 2019
  - Edições Enterprise, Standard, Workgroup, Developer e Web
- Para obter a lista mais recente das versões suportadas, consulte Usando um banco de dados Microsoft SQL Server como destino para AWS DMS.

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Microsoft SQL Server on-premises

Pilha de tecnologias de destino

- Banco de dados Microsoft SQL Server em uma EC2 instância

Arquitetura de destino

Arquitetura de migração de dados

- Usando AWS DMS

- Usando ferramentas nativas do SQL Server

Ferramentas

- AWS Database Migration Service (AWS DMS) ajuda você a migrar seus dados de e para bancos de dados comerciais e de código aberto amplamente usados, incluindo Oracle, SQL Server, MySQL e PostgreSQL. Você pode usar AWS DMS para migrar seus dados para o Nuvem AWS, entre instâncias locais (por meio de uma Nuvem AWS configuração) ou entre combinações de configurações na nuvem e no local.
- AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de banco de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.
- As ferramentas nativas do Microsoft SQL Server incluem backup e restauração, Copy Database Wizard e cópia e anexação de banco de dados.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões dos bancos de dados de origem e de destino.		DBA

Tarefa	Descrição	Habilidades necessárias
Identifique a versão do sistema operacional de destino.		DBA, administrador de sistemas
Identifique os requisitos de hardware para a instância do servidor de destino com base na lista de compatibilidade e nos requisitos de capacidade do Microsoft SQL Server.		DBA, administrador de sistemas
Identifique os requisitos de armazenamento para tipo e capacidade.		DBA, administrador de sistemas
Identifique os requisitos de rede, incluindo latência e largura de banda.		DBA, administrador de sistemas
Escolha o tipo de EC2 instância com base na capacidade, nos recursos de armazenamento e nos recursos de rede.		DBA, administrador de sistemas
Identifique os requisitos de segurança de acesso à rede e host para os bancos de dados de origem e de destino.		DBA, administrador de sistemas
Identifique uma lista de usuários necessários para a instalação do software Microsoft SQL Server.		DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Determine a estratégia de backup.		DBA
Determine os requisitos de disponibilidade.		DBA
Identifique a estratégia de migração e substituição de aplicativos.		DBA, administrador de sistemas

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC) e sub-redes.		Administrador de sistemas
Criar grupos de segurança e lista de controle de acesso (ACL) de rede.		Administrador de sistemas
Configure e inicie uma EC2 instância.		Administrador de sistemas

Instale o software

Tarefa	Descrição	Habilidades necessárias
Crie os usuários e grupos necessários para o software Microsoft SQL Server.		DBA, administrador de sistemas
Faça o download do software Microsoft SQL Server.		DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Instale o software Microsoft SQL Server na EC2 instância e configure o servidor.		DBA, administrador de sistemas

Migrar os dados - opção 1

Tarefa	Descrição	Habilidades necessárias
Use ferramentas nativas do Microsoft SQL Server ou ferramentas de terceiros para migrar os objetos e dados do banco de dados.	As ferramentas incluem backup e restauração, Copy Database Wizard e cópia e anexação de banco de dados. Para obter mais informaçõ es, consulte o guia Migrando bancos de dados do Microsoft SQL Server para o. Nuvem AWS	DBA

Migrar os dados - opção 2

Tarefa	Descrição	Habilidades necessárias
Migre os dados usando o AWS DMS.	Para obter mais informaçõ es sobre o uso AWS DMS, consulte os links na seção Recursos relacionados.	DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos.	Use AWS Schema Conversion Tool (AWS SCT) para analisar	DBA, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	e modificar o código SQL incorporado ao código-fonte do aplicativo.	

Substituir

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de troca de aplicativos.		DBA, proprietário do aplicativo, administrador de sistemas

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Desligue todos os AWS recursos temporários.	Os recursos temporários incluem a instância AWS DMS de replicação e a EC2 instância para AWS SCT.	DBA, administrador de sistemas
Revise e valide os documentos do projeto.		DBA, proprietário do aplicativo, administrador de sistemas
Reúna métricas sobre a hora de migrar, porcentagem de economia de custos manuais versus ferramentas e assim por diante.		DBA, proprietário do aplicativo, administrador de sistemas
Feche o projeto e forneça feedback.		DBA, proprietário do aplicativo, administrador de sistemas

Recursos relacionados

Referências

- Migrando bancos de dados Microsoft SQL Server para o Nuvem AWS
- Amazon EC2
- Amazon EC2 FAQs
- EC2 Preços da Amazon
- AWS Database Migration Service
- Produtos Microsoft em AWS
- Licenciamento da Microsoft em AWS
- Microsoft SQL Server em AWS

Tutoriais e vídeos

- Começando com a Amazon EC2
- Conceitos básicos do AWS Database Migration Service
- Associe uma EC2 instância da Amazon ao seu Simple AD Active Directory
- Associe uma EC2 instância da Amazon ao seu AWS Managed Microsoft AD Active Directory
- AWS Database Migration Service(vídeo)
- Introdução à Amazon EC2 — Elastic Cloud Server e hospedagem com AWS (vídeo)

Migre um banco de dados MySQL local para a Amazon EC2

Criado por Lorenzo Mota (AWS)

Resumo

Esse padrão fornece orientação para migrar um banco de dados MySQL local para um banco de dados MySQL em uma instância do Amazon Elastic Compute Cloud (Amazon). EC2 O padrão discute o uso de AWS Database Migration Service (AWS DMS) ou ferramentas nativas do MySQL, como mysqldump, para a migração. Ele se concentra na migração completa do banco de dados para uma instância de banco de dados MySQL.

O padrão é principalmente para DBAs arquitetos de soluções. Ele pode ser usado em projetos pequenos ou grandes, em uma fase de teste ou migração final. Recomendamos que você execute pelo menos um ciclo de teste antes de usar esse padrão em um ambiente de produção.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem do MySQL em um datacenter on-premises

Versões do produto

- MySQL versão 5.5 e posterior
- Um sistema operacional de destino suportado pela Amazon EC2; veja Amazon EC2 FAQs

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados MySQL on-premises.

Pilha de tecnologias de destino

- Uma instância de banco de dados MySQL na Amazon EC2

Métodos de migração de dados da AWS

- AWS DMS
- Ferramentas nativas do MySQL, como mysqldump, ou ferramentas de terceiros, como Percona XtraBackup

Arquitetura de destino

O diagrama a seguir ilustra a EC2 implementação alvo da Amazon após a transição.

Arquitetura de migração de dados AWS

Usando o AWS DMS:

O diagrama a seguir ilustra o fluxo de trabalho de migração de dados com base no envio AWS DMS de alterações completas e incrementais ao banco de dados MySQL de destino até a transição. A conexão de rede local para AWS depende dos requisitos do cliente SQL e está fora do escopo desse padrão.

Usando outras ferramentas do MySQL:

O diagrama a seguir ilustra o fluxo de trabalho de migração de dados com base no uso de ferramentas MySQL para gerar arquivos de despejo de exportação do banco de dados local. Esses arquivos são movidos para o Amazon Simple Storage Service (Amazon S3) e importados para o banco de dados MySQL de destino antes da transferência. A conexão de rede local para AWS depende dos requisitos do cliente SQL e está fora do escopo desse padrão.

Observações:

- Dependendo das considerações sobre o tempo de inatividade e do tamanho do banco de dados para a transição final, você pode usar AWS DMS ou outra ferramenta de captura de dados de alteração (CDC) para minimizar o tempo de transição. Ao usar uma ferramenta do CDC AWS DMS, como a, você pode migrar para o banco de dados de destino em minutos.
- Uma estratégia off-line com mysqldump pode ser suficiente se o tamanho do banco de dados e a latência da rede permitirem uma janela curta de migração por transferência. (Recomendamos que você realize testes para obter um tempo aproximado.)
- Normalmente, uma estratégia de CDC AWS DMS requer mais monitoramento e complexidade do que uma opção off-line.

Ferramentas

AWS serviços

- AWS Database Migration Service (AWS DMS) suporta vários bancos de dados de origem e destino. Para obter informações sobre bancos de dados de origem e destino do MySQL suportados pelo AWS DMS, consulte Usando um banco de dados compatível com MySQL como fonte para AWS DMS e Usando um banco de dados compatível com MySQL como destino para. AWS DMS Se seu banco de dados de origem não for compatível com AWS DMS, você deverá escolher outro método para migrar seus dados.

Outras ferramentas

- mysqldump é um utilitário MySQL que cria um arquivo de despejo de um banco de dados MySQL para fins de backup ou migração.
- O Percona XtraBackup é um utilitário de código aberto para realizar backups sem bloqueio em bancos de dados MySQL.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões do banco de dados.	Valide as versões dos bancos de dados de origem e de destino. Para obter informaçõ es sobre as versões do MySQL suportadas pelo AWS DMS, consulte Sources for AWS DMS and Targets for AWS DMS na AWS DMS documentação.	DBA
Identifique o sistema operacional de destino.	Determine a versão do sistema operacional de destino. Para obter uma lista dos sistemas operacion	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	ais de destino suportados pela Amazon EC2, consulte Amazon EC2 FAQs.	
Identificar os requisitos de hardware.	Determine os requisitos de hardware para a instância do servidor de destino com base na lista de compatibilidade do MySQL e nos requisitos de capacidade.	DBA, administrador de sistemas
Identifique os requisitos de armazenamento.	Determine o tipo de armazenamento e a capacidade do banco de dados de destino.	DBA, administrador de sistemas
Identificar os requisitos de rede.	Determine os requisitos de rede, como latência e largura de banda.	DBA, administrador de sistemas
Escolha o tipo de instância de destino.	Escolha o tipo de instância de destino com base na capacidade, nos recursos de armazenamento e nos recursos de rede.	DBA, administrador de sistemas
Identificar os requisitos de segurança.	Determine os requisitos de segurança de acesso à rede ou ao host para os bancos de dados de origem e de destino.	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Identifique os usuários.	Determine a lista de usuários do sistema operacional para a instalação do software MySQL. Para ter mais informações, consulte a documentação do MySQL.	DBA, administrador de sistemas
Determine uma estratégia de backup.		DBA
Determine os requisitos de disponibilidade.		DBA
Identifique a migração de aplicativos e a estratégia de transição.		DBA, administrador de sistemas

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC) e sub-redes.	Configure tabelas de rotas, gateway da internet, gateways NAT e sub-redes. Para obter mais informações, consulte as opções de configuração da VPC na documentação da Amazon VPC.	Administrador de sistemas
Crie grupos de segurança e listas de controle de acesso à rede (ACLs).	Configure portas (o padrão para MySQL é 3306) e intervalos CIDR ou específicos IPs , dependendo de seus requisitos.	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Configure e inicie uma EC2 instância.	Para obter instruções, consulte Iniciar uma EC2 instância na EC2 documentação da Amazon.	Administrador de sistemas

Instalar o software MySQL

Tarefa	Descrição	Habilidades necessárias
Crie usuários e grupos.	Crie os usuários e grupos do sistema operacional que precisam acessar o servidor e o banco de dados. Para obter mais informações, consulte Access Control and Account Management na documentação do MySQL.	DBA, administrador de sistemas
Baixe o MySQL.	Baixe o software MySQL. Para obter instruções e binários, consulte Instalando o MySQL na documentação do MySQL.	DBA, administrador de sistemas
Instale o MySQL na EC2 instância e configure o servidor.	Conecte-se à sua EC2 instância e instale o software MySQL. Para obter mais informações, consulte Connect to your EC2 instance na EC2 documentação da Amazon.	DBA, administrador de sistemas

Migrar dados — opção 1

Tarefa	Descrição	Habilidades necessárias
Migre dados com o MySQL nativo ou ferramentas de terceiros.	Essa opção usa ferrament as nativas do MySQL ou ferramentas de terceiros para migrar objetos e dados do banco de dados. Para obter instruções, consulte a documentação do mysqldump ou do Percona XtraBackup (para migração física). Para obter mais informações sobre o uso dessas ferramentas, consulte a postagem do AWS blog Opções de migração do MySQL para o Amazon RDS for MySQL ou Amazon Aurora MySQL.	DBA

Migrar dados — opção 2

Tarefa	Descrição	Habilidades necessárias
Migre dados com AWS DMS.	Para obter mais informaçõ es, consulte Visão de alto nível AWS DMS da AWS DMS documentação.	DBA

Prepare-se para a transição

Tarefa	Descrição	Habilidades necessárias
Reúna a contagem de objetos.	Colete contagens de objetos do banco de dados de origem	DBA

Tarefa	Descrição	Habilidades necessárias
	e dos novos bancos de dados de destino. Corrija quaisquer discrepâncias no banco de dados de destino.	
Verifique dependências.	Confirme se as dependênc ias (links) de e para outros bancos de dados ainda são válidas e funcionam corretame nte.	DBA
Teste.	Se esse for um ciclo de testes, realize testes de consulta, colete métricas e corrija quaisquer problemas.	DBA

Substituir

Tarefa	Descrição	Habilidades necessárias
Mova clientes.	Mude os clientes do aplicativo para a nova infraestrutura.	DBA, proprietário do aplicativ o, administrador de sistemas
Forneça suporte.	Forneça suporte durante o teste funcional do aplicativo.	DBA

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Desligar recursos.	Encerre a instância AWS DMS de replicação e outros AWS recursos temporários.	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Documentos de revisão e projeto.	Revise e valide os documentos do projeto.	DBA, proprietário do aplicativo, administrador de sistemas
Colete métricas.	Colete métricas como tempo de migração, porcentagem de alterações manuais em comparação com alterações auxiliadas por ferramentas e economia de custos.	DBA, proprietário do aplicativo, administrador de sistemas
Encerrar o projeto.	Encerre o projeto de migração e forneça feedback.	DBA, proprietário do aplicativo, administrador de sistemas
Desative o banco de dados de origem.	Desative o banco de dados MySQL local.	DBA, administrador de sistemas

Recursos relacionados

Referências

- EC2 Documentação da Amazon
- AWS DMS documentação
- EC2 Preços da Amazon
- AWS DMS Step-by-Step Demonstrações
- mysqldump
- Percona XtraBackup

Tutoriais e vídeos

- Começando com AWS DMS
- Introdução à Amazon EC2 — Elastic Cloud Server e hospedagem com AWS (vídeo)

Reduza o tempo de substituição homogêneo da migração do SAP usando o Application Migration Service

Criado por Pavel Rubin (AWS), Diego Valverde (AWS) e Sunil Yadav (AWS)

Resumo

Esse padrão descreve as etapas para migrar workloads do SAP usando o AWS Application Migration Service. O Application Migration Service facilita as substituições usando a replicação em nível de bloco para manter os volumes de replicação sincronizados continuamente a partir de suas fontes.

As workloads da SAP incluem os aplicativos SAP Customer Relationship Management (SAP CRM), SAP Enterprise Resource Planning (ERP) e SAP Business Warehouse (SAP BW).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa AWS com conectividade de rede estável entre os servidores SAP de origem e a nuvem privada virtual (VPC) de destino na AWS
- Um banco de dados de origem do SAP Adaptive Server Enterprise (ASE) para Linux ou Windows em um datacenter on-premises

Limitações

- O sistema operacional de destino deve ser suportado pelo Amazon Elastic Compute Cloud (Amazon EC2). Para obter mais informações, consulte Amazon EC2 FAQs.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados SAP ASE

Pilha de tecnologias de destino

- Amazon EC2
- Amazon Elastic Block Store (Amazon EBS)

Arquitetura de origem e destino

O diagrama a seguir mostra a migração dos servidores on-premises por meio do Agente de Replicação para o endpoint do Serviço de Migração de Aplicativos. Um endpoint do Amazon Simple Storage Service (Amazon S3) é usado para acessar arquivos de instalação e configuração. As sub-redes da área de armazenamento e os recursos migrados contêm EC2 instâncias, com armazenamento de dados em volumes do EBS. A porta TCP 443 é usada para conectar a rede da máquina de origem ao Application Migration Service e para conectar as sub-redes da área de armazenamento aos endpoints regionais do Application Migration Service, Amazon e EC2 Amazon S3. A porta TCP 1500 é usada para replicação de dados entre a rede local e a área de armazenamento.

Ferramentas

- O AWS Application Migration Service ajuda você a rehospedar (lift-and-shift) aplicativos na nuvem da AWS sem alterações e com o mínimo de tempo de inatividade.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (Amazon). EC2
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Security Token Service (AWS STS) ajuda você a solicitar credenciais temporárias com privilégios limitados para os usuários.

Épicos

Inicializar o Application Migration Service

Tarefa	Descrição	Habilidades necessárias
Inicializar o Application Migration Service	Inicializar o Application Migration Service na região da AWS onde você deseja	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	implementar a base de dados SAP ASE. A AWS fornece uma configuração automatizada na primeira vez que você acessa a página do Application Migration Service em cada região.	
Crie manualmente perfis de serviço.	(Opcional) Se você quiser usar a automação (por exemplo, o AWS Control Tower) para configurar a conta, você pode criar manualmente as seis perfis do IAM do AWS Identity and Access Management necessárias para instalação, replicação e lançamentos. Para obter instruções, consulte a Documentação do AWS.	Administrador da AWS
Crie um modelo de configurações de replicação.	O modelo de configurações de replicação define a sub-rede, o tipo de instância, a criptografia do Amazon EBS e como os dados são roteados. Para obter informações detalhadas sobre configurações, consulte a documentação da AWS.	AWS geral

Gere credenciais para a instalação do Agente

Tarefa	Descrição	Habilidades necessárias
Criar um novo perfil do IAM.	No console do IAM navegue até Roles (Perfis) e, em seguida, escolha Create Role (Criar perfil). Para o tipo de entidade confiável, escolha a conta da AWS e, em seguida, escolha Avançar.	Administrador de sistemas AWS
Anexe AWSApplication MigrationAgentPolicy à função do IAM.	A `AWSApplicationMigrationAgentPolicy` política gerenciada pela AWS contém as permissões necessárias para realizar a instalação do Application Migration Service Agent. Após anexar a política, selecione Next.	Administrador de sistemas AWS
Conclua a criação do perfil.	Atribua um nome amigável e escolha Criar perfil.	Administrador de sistemas AWS
Gere credenciais temporárias.	Para gerar o ID da chave de acesso, a chave de acesso secreta e o token de sessão, siga as instruções na documentação do AWS STS. Essas credenciais são usadas durante a instalação do Agente.	Administrador de sistemas AWS

Instale o Application Migration Service Agent na máquina de origem SAP

Tarefa	Descrição	Habilidades necessárias
Baixe o instalador do agente na máquina de origem do SAP.	Baixe o instalador do Agente apropriado para seu sistema operacional de origem: Windows ou Linux.	Proprietário do App
Instale o AWS Replication Agent.	Quando você executa o arquivo do instalador do Agente em uma máquina de origem, primeiro é solicitado que você insira sua chave de acesso, chave de acesso secreta, token de sessão e a região para a qual replicar. Use as credenciais temporárias do perfil do IAM que você criou anteriormente e da mesma região que você configurou durante a inicialização.	Proprietário do App
Aguarde a replicação inicial dos dados.	Depois que o Agente é instalado, a máquina de origem aparece na guia Máquinas no console do Application Migration Service.	Proprietário do App

Configurar o modelo de lançamento da máquina de destino

Tarefa	Descrição	Habilidades necessárias
Atualize o modelo Launch para o servidor de origem.	Cada servidor de origem usa um modelo exclusivo EC2 do Launch que informa	AWS geral

Tarefa	Descrição	Habilidades necessárias
	a configuração do EC2 servidor de destino. Você pode editar esse modelo se quiser personalizar a EC2 configuração da Amazon do seu servidor migrado.	
Definir a versão do modelo de execução padrão	Depois de fazer as alteraçõe s necessárias no modelo do Launch, especifique o uso dessa versão atualizada como o modelo padrão do Launch. Para obter mais informações, consulte a documentação da AWS.	AWS geral
Desative o dimensionamento correto do tipo de instância.	(Opcional) O dimension amento correto do tipo de instância fornece recomenda ções automáticas de tipo de instância com base na configuração do servidor SAP de origem. Recomendamos desativar essa configuração para que você possa especific ar tipos de instância personali zados no modelo do Launch.	AWS geral

Realize um teste

Tarefa	Descrição	Habilidades necessárias
Inicie um lançamento de teste.	No console do Application Migration Service, selecione um ou mais servidores e, em	AWS geral, engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	seguida, selecione Iniciar instâncias de teste em Teste e substituição.	
Aguarde até que o processo de conversão e lançamento seja concluído.	Você pode revisar o processo de lançamento na guia Histórico de lançamento. Depois que a máquina for iniciada com sucesso como uma EC2 instância, a guia Alertas será atualizada para Iniciado.	
Verifique se o teste teve êxito.	Conecte-se à instância iniciada por meio do Remote Desktop Protocol (RDP) ou SSH (Secure Shell) e execute as verificações apropriadas do aplicativo. Por exemplo, faça login na interface SAP e valide a funcionalidade.	Engenheiro de migração, proprietário do App
Atualizar o ciclo de vida da fonte.	Se o teste tiver sido bem-sucedido, atualize o ciclo de vida da máquina de origem para Marcar como “Pronto para transferência” na guia Teste e substituição.	Engenheiro de migração, líder de migração

Agende e realize uma transição para a meta da Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Agende uma janela de substituição.		Líder de substituição, líder de migração, proprietário do App

Tarefa	Descrição	Habilidades necessárias
Inicie um lançamento de substituição.	Selecione um ou mais servidores. Na guia Teste e substituição, selecione Iniciar instâncias de substituição em Teste e substituição no console do Application Migration Service.	Engenheiro de migração
Aguarde até que o processo de conversão e lançamento seja concluído.	Você pode revisar o processo de lançamento na guia Histórico de lançamento. Depois que a máquina for iniciada com sucesso como uma EC2 instância, a guia Alertas será atualizada para Iniciado.	
Verifique se a substituição foi concluída com êxito.	Conecte-se à instância iniciada por meio de RDP ou SSH e execute as verificações apropriadas do aplicativo.	Proprietário do App, engenheiro de migração
Atualizar o ciclo de vida da fonte.	Se a substituição for bem-sucedida, atualize o ciclo de vida da máquina de origem selecionando Finalizar substituição na guia Teste e substituição.	Engenheiro de migração

Recursos relacionados

Referências

- Serviço de migração de aplicações da AWS
- AWS Application Migration FAQ

Vídeo

- AWS Application Migration Service Architecture

Redefinir a hospedagem de workloads on-premises na Nuvem AWS: lista de verificação de migração

Criado por Srikanth Rangavajhala (AWS)

Resumo

A redefinição da hospedagem de workloads on-premises na Nuvem da Amazon Web Services (AWS) envolve as seguintes fases de migração: planejamento, pré-descoberta, descoberta, compilação, teste e substituição. Esse padrão descreve as fases e as tarefas relacionadas. As tarefas são descritas em alto nível e são compatíveis com cerca de 75% de todas as workloads de aplicativos. Você pode implementar essas tarefas em duas a três semanas em um ciclo de sprint ágil.

Você deve analisar e examinar essas tarefas com sua equipe de migração e consultores. Após a análise, você pode coletar as informações, eliminar ou reavaliar tarefas conforme necessário para atender aos seus requisitos e modificar outras tarefas para serem compatíveis com pelo menos 75% das workloads de aplicativos em seu portfólio. Em seguida, você pode usar uma ferramenta de gerenciamento de projetos ágil, como Atlassian Jira ou Rally Software, para importar as tarefas, atribuí-las aos recursos e rastrear suas atividades de migração.

O padrão pressupõe que você esteja usando o AWS Cloud Migration Factory para redefinir a hospedagem de suas workloads, mas é possível usar a ferramenta de migração de sua escolha.

O Amazon Macie pode ajudar a identificar dados confidenciais em suas bases de conhecimento, armazenados como fontes de dados, registros de invocação de modelos e registros de solicitações em buckets do Amazon Simple Storage Service (Amazon S3). Para obter mais informações, consulte a documentação do Macie.

Pré-requisitos e limitações

Pré-requisitos

- Ferramenta de gerenciamento de projetos para rastrear tarefas de migração (por exemplo, Atlassian Jira ou Rally Software)
- Ferramenta de migração para redefinir a hospedagem suas workloads na AWS (por exemplo, Cloud Migration Factory)

Arquitetura

Plataforma de origem

- Pilha de origem on-premises (incluindo tecnologias, aplicativos, bancos de dados e infraestrutura)

Plataforma de destino

- Pilha de destinos da Nuvem AWS (incluindo tecnologias, aplicativos, bancos de dados e infraestrutura)

Arquitetura

O diagrama a seguir ilustra a redefinição da hospedagem (descobrindo e migrando servidores de um ambiente de origem on-premises para a AWS) usando o Cloud Migration Factory e o AWS Application Migration Service.

Ferramentas

- Você pode usar uma ferramenta de migração e gerenciamento de projetos de sua escolha.

Épicos

Fase de planejamento

Tarefa	Descrição	Habilidades necessárias
Limpe a pendência de pré-descoberta.	Conduza a sessão de trabalho de limpeza da pendência de pré-descoberta com líderes de departamento e proprietários de aplicativos.	Gerente de projetos, líder de scrum ágil
Conduza a sessão de trabalho de planejamento do sprint.	Como exercício de definição de escopo, distribua os aplicativos que você deseja migrar entre sprints e ondas.	Gerente de projetos, líder de scrum ágil

Fase pré-descoberta

Tarefa	Descrição	Habilidades necessárias
Confirme o conhecimento do aplicativo.	Confirme e documente o proprietário do aplicativo e conhecimento dele sobre o aplicativo. Determine se há outra pessoa responsável para questões técnicas.	Especialista em migração (entrevistador)
Determine os requisitos de conformidade do aplicativo.	Confirme com o proprietário do aplicativo que o aplicativo não precisa estar em conformidade com os requisitos do Padrão de segurança de dados do Setor de cartões de pagamento (PCI DSS), da Lei Sarbanes-Oxley (SOX), das informações de identificação pessoal (PII) ou de outros padrões. Se existirem requisitos de conformidade, as equipes devem concluir as verificações de conformidade nos servidores que serão migrados.	Especialista em migração (entrevistador)
Confirme os requisitos da versão de produção.	Confirme os requisitos para liberar o aplicativo migrado para produção (como data de lançamento e duração do tempo de inatividade) com o proprietário do aplicativo ou com o contato técnico.	Especialista em migração (entrevistador)

Tarefa	Descrição	Habilidades necessárias
Obtenha a lista de servidores.	Obtenha a lista de servidores associados ao aplicativo de destino.	Especialista em migração (entrevistador)
Obtenha o diagrama lógico que mostra o estado atual.	Obtenha o diagrama do estado atual do aplicativo a partir do arquiteto corporativo ou do proprietário do aplicativo.	Especialista em migração (entrevistador)
Crie um diagrama lógico que mostre o estado de destino.	Crie um diagrama lógico do aplicativo que mostre a arquitetura de destino na AWS. Esse diagrama deve ilustrar os servidores, a conectividade e os fatores de mapeamento.	Arquiteto corporativo, Proprietário da empresa
Obtenha informações sobre o servidor.	Colete informações sobre os servidores associados ao aplicativo, incluindo detalhes de configuração.	Especialista em migração (entrevistador)
Adicione informações do servidor ao modelo de descoberta.	Adicione informações detalhadas do servidor ao modelo de descoberta de aplicativos (consulte `mobilize-application-questionnaire.xlsx` no anexo para esse padrão). Esse modelo inclui todos os detalhes de segurança, infraestrutura, sistema operacional e rede relacionados ao aplicativo.	Especialista em migração (entrevistador)

Tarefa	Descrição	Habilidades necessárias
Publique o modelo de descoberta de aplicativos.	Compartilhe o modelo de descoberta do aplicativo com o proprietário do aplicativo e a equipe de migração para acesso e uso comuns.	Especialista em migração (entrevistador)

Fase de descoberta

Tarefa	Descrição	Habilidades necessárias
Confirme a lista de servidores.	Confirme a lista de servidores e a finalidade de cada servidor com o proprietário do aplicativo ou o líder técnico.	Especialista em migração
Identifique e adicione grupos de servidores.	Identifique grupos de servidores, como servidores web ou servidores de aplicativos, e adicione essas informações ao modelo de descoberta de aplicativos. Selecione a camada do aplicativo (web, aplicativo, banco de dados) à qual cada servidor deve pertencer.	Especialista em migração
Preencha o modelo de descoberta do aplicativo.	Preencha os detalhes do modelo de descoberta de aplicativos com a ajuda da equipe de migração, da equipe de aplicativos e da AWS.	Especialista em migração

Tarefa	Descrição	Habilidades necessárias
Adicione detalhes ausentes do servidor (equipes de middleware e SO).	Peça às equipes de middlewar e e sistema operacional (SO) que analisem o modelo de descoberta de aplicativ os e adicionem todos os detalhes ausentes do servidor, incluindo informações do banco de dados.	Especialista em migração
Obtenha regras de tráfego de entrada/saída (equipe de rede).	Peça à equipe de rede que obtenha as regras de tráfego de entrada/saída para os servidores de origem e destino. A equipe de rede também deve adicionar regras de firewall existentes, exportá-las para um formato de grupo de segurança e adicionar balanceadores de carga existentes ao modelo de descoberta de aplicativos.	Especialista em migração
Identifique a marcação necessária.	Determine os requisitos de marcação para o aplicativo.	Especialista em migração
Crie detalhes de solicitação de firewall.	Capture e filtre as regras de firewall necessárias para se comunicar com o aplicativo.	Especialista em migração, arquiteto de soluções, líder de rede
Atualize o tipo de EC2 instância.	Atualize o tipo de instância do Amazon Elastic Compute Cloud (Amazon EC2) a ser usado no ambiente de destino, com base nos requisitos de infraestrutura e servidor.	Especialista em migração, arquiteto de soluções, líder de rede

Tarefa	Descrição	Habilidades necessárias
Identifique o diagrama do estado atual.	Identifique ou crie o diagrama que mostra o estado atual do aplicativo. Esse diagrama será usado na solicitação de segurança da informação (InfoSec).	Especialista em migração, arquiteto de soluções
Finalize o diagrama de estados futuros.	Finalize o diagrama que mostra o estado futuro (destino) do aplicativo. Esse diagrama também será usado na InfoSec solicitação.	Especialista em migração, arquiteto de soluções
Crie solicitações de serviço de firewall ou grupo de segurança .	Crie solicitações de serviço de firewall ou grupo de segurança (para desenvolv imento/controle de qualidade , pré-produção e produção) . Se você estiver usando o Cloud Migration Factory, inclua portas específicas de replicação, caso elas ainda não estejam abertas.	Especialista em migração, arquiteto de soluções, líder de rede
Analise as solicitações de firewall ou grupo de segurança (InfoSec equipe).	Nessa etapa, a InfoSec equipe analisa e aprova as solicitaç ões do firewall ou do grupo de segurança que foram criadas na etapa anterior.	InfoSec engenheiro, especiali sta em migração

Tarefa	Descrição	Habilidades necessárias
Implemente solicitações do grupo de segurança de firewall (equipe de rede).	Depois que a InfoSec equipe aprova as solicitações de firewall, a equipe de rede implementa as regras de firewall de entrada/saída necessárias.	Especialista em migração, arquiteto de soluções, líder de rede

Fase de compilação (repetição para ambientes de desenvolvimento/QA, pré-produção e produção)

Tarefa	Descrição	Habilidades necessárias
Importe os dados do aplicativo e do servidor.	1. Verifique se você está conectado ao seu servidor de execução de migração como um usuário de domínio com permissões de administrador local nos servidores de origem dentro do escopo. 2. Use o formulário de entrada de migração para importar os atributos dos servidore s de origem dentro do escopo. Para obter mais informações, consulte Guia de implementação do Cloud Migration Factory. Se você não estiver usando o Cloud Migration Factory, siga as instruções para configurar sua ferramenta de migração.	Especialista em migração, administrador em nuvem

Tarefa	Descrição	Habilidades necessárias
Verifique os pré-requisitos dos servidores de origem.	Conecte-se aos servidores de origem dentro do escopo para verificar os pré-requisitos, como porta TCP 1500, porta TCP 443, espaço livre do volume raiz, versão do .NET Framework e outros parâmetros. Eles são necessários para a replicação. Para obter mais informações, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem
Crie uma solicitação de serviço para instalar agentes de replicação.	Crie uma solicitação de serviço para instalar agentes de replicação nos servidores dentro do escopo para desenvolvimento/controle de qualidade, pré-produção ou produção.	Especialista em migração, administrador em nuvem
Instale os agentes de replicação.	Instale os agentes de replicação nos servidores de origem dentro do escopo nas máquinas de desenvolvimento/controle de qualidade, pré-produção ou produção. Para obter mais informações, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem

Tarefa	Descrição	Habilidades necessárias
Envie os scripts de pós-inicialização.	O Application Migration Service oferece suporte a scripts de pós-inicialização para ajudar você a automatizar atividades a nível do sistema operacional, como instalar ou desinstalar software após a inicialização das instâncias de destino. Essa etapa envia os scripts de pós-inicialização para máquinas Windows ou Linux, dependendo dos servidores identificados para migração. Para obter instruções, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem
Verifique o status da replicação	Confirme automaticamente o status da replicação dos servidores de origem dentro do escopo usando o script fornecido. O script se repete a cada cinco minutos até que o status de todos os servidores de origem em determinada onda mude para Integrado. Para obter instruções, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem

Tarefa	Descrição	Habilidades necessárias
Crie o usuário administrador.	Talvez seja necessário um administrador local ou usuário sudo nas máquinas de origem para solucionar quaisquer problemas após a substitui ção da migração, indo dos servidores de origem dentro do escopo para a AWS. A equipe de migração usa esse usuário para fazer login no servidor de destino quando o servidor de autenticação (por exemplo, o servidor DC ou LDAP) não está acessível . Para obter instruções para esta etapa, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem
Valide o modelo de inicializ ação.	Valide os metadados do servidor para garantir que funcionem com êxito e não tenham dados inválidos. Essa etapa valida os metadados de teste e de substituição. Para obter instruções, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem

Fase de teste (repetição para ambientes de desenvolvimento/QA, pré-produção e produção)

Tarefa	Descrição	Habilidades necessárias
Crie uma solicitação de serviço.	Crie uma solicitação de serviço para que a equipe de infraestrutura e outras equipes realizem a substituição de aplicativos para instâncias de desenvolvimento/controle de qualidade, pré-produção ou produção.	Especialista em migração, administrador em nuvem
Defina um balanceador de carga (opcional).	Defina os balanceadores de carga necessários, como um Application Load Balancer ou um balanceador de carga F5 com iRules.	Especialista em migração, administrador em nuvem
Inicialize instâncias para testes.	Inicialize todas as máquinas de destino para uma determinada onda no Application Migration Service no modo de teste. Para obter mais informações, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem
Verifique o status da instância de destino.	Verifique o status da instância de destino verificando o processo de inicialização de todos os servidores de origem dentro do escopo na mesma onda. A inicialização das instâncias de destino pode levar até 30 minutos. Você pode verificar o status manualmente fazendo	Especialista em migração, administrador em nuvem

Tarefa	Descrição	Habilidades necessárias
	login no EC2 console da Amazon, pesquisando o nome do servidor de origem e revisando a coluna Verificação de status. O status verificações 2/2 aprovadas indicam que a instância está íntegra do ponto de vista da infraestrutura.	
Modifique as entradas de DNS.	Modifique as entradas de Sistema de Nomes de Domínio (DNS) (Use `resolv.conf` ou `host.conf` para um ambiente Microsoft Windows.) Configure cada EC2 instância para apontar para o novo endereço IP desse host. **Note** Certifique-se de que não haja conflitos de DNS entre servidores locais e na nuvem da AWS. Essa etapa e as etapas a seguir são opcionais, dependendo do ambiente em que o servidor está hospedado.	Especialista em migração, administrador em nuvem

Tarefa	Descrição	Habilidades necessárias
Teste a conectividade com hosts de back-end a partir de EC2 instâncias.	Verifique os logins usando as credenciais de domínio dos servidores migrados.	Especialista em migração, administrador em nuvem
Atualize o registro DNS A.	Atualize o registro DNS A de cada host para apontar para o novo endereço IP EC2 privado da Amazon.	Especialista em migração, administrador em nuvem
Atualize o registro DNS CNAME.	Atualize o registro DNS CNAME para servidore s virtuais IPs (nomes de balanceadores de carga) para apontar para o cluster para servidores web e de aplicativ os.	Especialista em migração, administrador em nuvem
Teste o aplicativo em ambientes aplicáveis.	Faça login na nova EC2 instância e teste o aplicativo nos ambientes de desenvolv imento/controle de qualidade, pré-produção e produção.	Especialista em migração, administrador em nuvem
Marque como pronto para a substituição.	Quando o teste estiver concluído, altere o status do servidor de origem para indicar que ele está pronto para a substituição, para que os usuários possam inicializ ar uma instância de substitui ção. Para obter instruções, consulte Guia de implement ação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem

Fase de substituição

Tarefa	Descrição	Habilidades necessárias
Crie um plano de implantação de produção.	Crie um plano de implantação de produção (incluindo um plano de retrocesso).	Especialista em migração, administrador em nuvem
Notifique a equipe de operações sobre o tempo de inatividade.	Notifique a equipe de operações sobre a agenda de inatividade dos servidores. Algumas equipes podem exigir um tíquete de solicitação de mudança ou de solicitação de serviço (CR/SR) para essa notificação.	Especialista em migração, administrador em nuvem
Replique as máquinas de produção.	Replique as máquinas de produção usando o Application Migration Service ou outra ferramenta de migração.	Especialista em migração, administrador em nuvem
Desligue os servidores de origem dentro do escopo.	Depois de verificar o status de replicação dos servidores de origem, você pode desligar os servidores de origem para interromper as operações dos aplicativos de clientes para os servidores. Você pode desligar os servidores de origem na janela de substituição. Para obter mais informações, consulte Guia de implementação do Cloud Migration Factory.	Administrador de nuvem
Inicialize instâncias para substituição.	Inicialize todas as máquinas de destino para uma	Especialista em migração, administrador em nuvem

Tarefa	Descrição	Habilidades necessárias
	determinada onda no Application Migration Service no modo de substituição. Para obter mais informações, consulte Guia de implementação do Cloud Migration Factory.	
Recupere a instância IPs de destino.	Recupere as quatro instâncias IPs de destino. Se a atualização do DNS for um processo manual em seu ambiente, você precisará obter os novos endereços IP para todas as instâncias de destino. Para obter mais informações, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem
Verifique as conexões do servidor de destino.	Depois de atualizar os registros DNS, conecte-se às instâncias de destino com o nome do host para verificar as conexões. Para obter mais informações, consulte Guia de implementação do Cloud Migration Factory.	Especialista em migração, administrador em nuvem

Recursos relacionados

- Como migrar
- Guia de implementação do AWS Cloud Migration Factory
- Automatizar migrações de servidores em grande escala com o Cloud Migration Factory
- Guia do usuário do serviço de migração de aplicativos da AWS

- Programa de Aceleração da Migração da AWS

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Configure a infraestrutura Multi-AZ para um SQL Server Always On FCI usando a Amazon FSx

Criado por Manish Garg (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Nishad Mankar (AWS) e RAJNEESH TYAGI (AWS)

Resumo

Se você precisar migrar rapidamente um grande número de instâncias de cluster de failover Always On do Microsoft SQL Server (FCIs), esse padrão pode ajudá-lo a minimizar o tempo de provisionamento. Ao usar a automação e o Amazon FSx for Windows File Server, ele reduz os esforços manuais, os erros cometidos pelo homem e o tempo necessário para implantar um grande número de clusters.

Esse padrão configura a infraestrutura do SQL Server FCIs em uma implantação de Zona de Multidisponibilidade (Multi-AZ) na Amazon Web Services (AWS). O provisionamento dos serviços da AWS necessários para essa infraestrutura é automatizado usando modelos da AWS CloudFormation. A instalação do SQL Server e a criação de nós de cluster em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) são realizadas usando PowerShell comandos.

Essa solução usa um sistema de arquivos Amazon FSx para Windows Multi-AZ altamente disponível como testemunha compartilhada para armazenar os arquivos do banco de dados do SQL Server. O sistema de FSx arquivos da Amazon e as instâncias EC2 do Windows que hospedam o SQL Server são unidos ao mesmo domínio do AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um usuário da AWS com permissões suficientes para provisionar recursos usando CloudFormation modelos da AWS
- AWS Directory Service para Microsoft Active Directory
- Credenciais no AWS Secrets Manager para autenticação no AWS Managed Microsoft AD em um par de valores-chave:
  - `ADDomainName`: <Nome do domínio>
  - `ADDomainJoinUserName`: <Nome de usuário do domínio>

- `ADDomainJoinPassword`: <Senha do usuário do domínio>
- `TargetOU`: <Valor OU Alvo>

> **Note**
>
> Você usará o mesmo nome de chave na automação do AWS Systems Manager para a atividade de junção do AWS Managed Microsoft AD.

- Arquivos de mídia do SQL Server para instalação do SQL Server e contas de serviço ou domínio do Windows criadas, que serão usados durante a criação do cluster
- Uma nuvem privada virtual (VPC), com duas sub-redes públicas em zonas de disponibilidade separadas, duas sub-redes privadas nas zonas de disponibilidade, um gateway da internet, gateways NAT, associações de tabelas de rotas e um servidor de salto

Versões do produto

- Windows Server 2012 R2 e Microsoft SQL Server 2016

Arquitetura

Pilha de tecnologia de origem

- SQL Server local com o FCIs uso de um drive compartilhado

Pilha de tecnologias de destino

- EC2 Instâncias da AWS
- Servidor FSx de arquivos Amazon para Windows
- Runbook do AWS Systems Manager Automation
- Configurações de rede (VPC, sub-redes, gateway da internet, gateways NAT, servidor de salto, grupos de segurança)
- AWS Secrets Manager
- AWS Managed Microsoft AD
- Amazon EventBridge
- AWS Identity and Access Management (IAM)

Arquitetura de destino

O diagrama a seguir mostra uma conta da AWS em uma única região da AWS, com uma VPC que inclui duas zonas de disponibilidade, duas sub-redes públicas com gateways NAT, um servidor de salto na primeira sub-rede pública, duas sub-redes privadas, cada uma com uma EC2 instância para um nó do SQL Server em um grupo de segurança de nós e um sistema de FSx arquivos da Amazon conectado a cada um dos nós do SQL Server. AWS Directory Service, Amazon EventBridge, AWS Secrets Manager e AWS Systems Manager também estão incluídos.

Automação e escala

- Você pode usar o AWS Systems Manager para se juntar ao AWS Managed Microsoft AD e realizar a instalação do SQL Server.

Ferramentas

Serviços da AWS

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- O AWS Directory Service fornece várias maneiras de usar o Microsoft Active Directory (AD) com outros serviços da AWS, como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) para SQL Server e FSx Amazon para Windows File Server.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, funções do Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras contas da AWS.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente.

- O AWS Systems Manager ajuda você a gerenciar seus aplicativos e infraestrutura em execução na nuvem AWS. Isso simplifica o gerenciamento de aplicações e recursos, diminui o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus recursos da AWS de modo seguro e em grande escala.

Outras ferramentas

- PowerShellé um programa de gerenciamento de automação e configuração da Microsoft executado em Windows, Linux e macOS. Esse padrão usa PowerShell scripts.

Repositório de código

O código desse padrão está disponível no repositório GitHub aws-windows-failover-cluster-automation.

Práticas recomendadas

- Os perfis do IAM usados para implantar essa solução devem seguir o princípio do privilégio mínimo. Para ter mais informações, consulte a documentação do IAM.
- Siga as CloudFormation melhores práticas da AWS.

Épicos

Implante a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Implante a CloudFormation pilha do Systems Manager.	1. Faça login em sua conta AWS e abra o Console de Gerenciamento da AWS. 2. Navegue até o CloudFormation console e crie a CloudFormation pilha do Systems Manager fazendo o upload do `ssm.yaml` modelo. Forneça valores	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	para os parâmetros a seguir: • StateUnJoinAssociationLoggingBucketName— Forneça um nome para o bucket do S3 que o modelo criará para fins de registro. • SSMAssociationADUnjoinNome — Forneça um nome para o `AWS::SSM::Association` recurso. • SSMAutomationDocumentName— Forneça um nome para o runbook do Systems Manager Automation. • EventBridgeName— Forneça um nome para o ônibus do EventBridge evento. 3. Implante a CloudFormation pilha do Systems Manager iniciando o `ssm.yaml` CloudFormation modelo. O modelo criará o runboook do Systems Manager Automation que é iniciado quando uma nova EC2 instância com a tag é iniciada. `ADJoined: FSXADD` O runbook Automation	

Tarefa	Descrição	Habilidades necessárias
	(Automação) adicionará a instância ao diretório AWS Managed Microsoft AD.	

Tarefa	Descrição	Habilidades necessárias
Implante a pilha de infraestrutura.	Após a implantação bem-sucedida da pilha do Systems Manager, crie a `infra` pilha, que inclui nós de EC2 instância, grupos de segurança, o sistema de arquivos Amazon FSx for Windows File Server e a função do IAM. 1. Navegue até o CloudFormation console e inicie o `infra-cf.yaml` modelo. Para implantar essa pilha, os seguintes parâmetros são obrigatórios: • `ActiveDirectoryId` : ID do AWS Managed Microsoft AD • `ADDnsIpAddresses1` : endereço IP DNS primário do AWS Managed Microsoft AD • `ADDnsIpAddresses2` : endereço IP DNS secundário do AWS Managed Microsoft AD • `FSxSecurityGroupName` — Nome do grupo de FSx segurança da Amazon • `FSxWindowsFileSystemName` — Nome da FSx unidade Amazon	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• `ImageID`: ID da imagem base do Windows 2012 R2 ou imagem de máquina da Amazon (AMI) usada para criar o nó da instância do SQL Server • `KeyPairName` — Par de valores-chave a ser anexado aos nós da EC2 instância para acesso • `Node1SecurityGroupName` : nome do primeiro grupo de segurança do nó • `Node2SecurityGroupName` : nome do grupo de segurança do segundo nó • `OUSecretName` : nome do segredo que contém as informações do AWS Managed Microsoft AD • `PrivateSubnet1` : ID da primeira sub-rede privada • `PrivateSubnet2` : ID da segunda sub-rede privada • `SqlFSxFCIName` — Nome da tag aplicada aos nós primário e	

Tarefa	Descrição	Habilidades necessárias
	secundário e à Amazon FSx. • `SqlFSxServerNetBIOSName1` — Nome do nó da EC2 instância primária (máximo de 15 caracteres) • `SqlFSxServerNetBIOSName2` — Nome do nó da EC2 instância secundária (máximo de 15 caracteres) • `VPC`: ID da VPC • `WorkloadInstanceType` — Tipo de EC2 instância Implante a pilha `infra`. A pilha criará todos os componentes de infraestrutura necessários para configurar a FCI do Windows SQL Server. 2. Depois que os nós da EC2 instância forem iniciados, o documento Systems Manager Automation será invocado para unir essas instâncias ao AWS Managed Microsoft AD. Você pode acompanhar o progresso na página Automação do console do Systems Manager.	

Configurar o Windows SQL Server Always On FCI

Tarefa	Descrição	Habilidades necessárias

Instale as ferramentas do Windows.	1. Faça login na EC2 instância primária, que é o nó 1. Para instalar os recursos do Windows (Active Directory e FCI Tools), execute o PowerShell script a seguir.
	`Install-WindowsFeature -Name RSAT-AD-Powershell,Failover-Clustering -IncludeManagementTools`
	`Install-WindowsFeature -Name RSAT-Clustering,RSAT-ADDS-Tools,RSAT-AD-Powershell,RSAT-DHCP,RSAT-DNS-Server`
	2. Faça login na EC2 instância secundária, que é o nó 2, e execute o mesmo script para ativar os recursos no nó 2.
		AWS DevOps, DevOps engenheiro, DBA

Pré-configure os objetos do computador do cluster nos serviços de domínio do Active Directory.	Para pré-configurar o objeto de nome de cluster (CNO) nos serviços de domínio do Active Directory (AD DS) e pré-configurar um objeto de computador virtual (VCO) para um perfil em cluster, siga as instruções na documentação do Windows Server.	AWS DevOps, DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
Crie o WSFC.	Para criar o cluster do Windows Server Failover Clustering (WSFC), faça o seguinte: 1. Faça login na EC2 instância primária, que é o nó 1. Para criar o compartilhamento de FSx arquivos da Amazon e conceder acesso total à conta de serviço do AD listada, execute o código a seguir. `Invoke-Command -ComputerName "<FSx Windows Remote PowerShell Endpoint>" -ConfigurationName FSxRemoteAdmin -scriptblock { New-FSxSmbShare -Name "SQLDB" -Path "D:\share" -Description "SQL Databases Share" -ContinuouslyAvailable $true -FolderEnumerationMode AccessBased -EncryptData $true grant-fsxsmbshareaccess -name SQLDB -AccountName "<domain\user>" -accessRight Full }`	AWS DevOps, DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
	Esse comando também criará o compartilhamento de arquivos continuam ente disponível (CA), que é otimizado para uso pelo Microsoft SQL Server. 2. Para criar o cluster de failover na instância primária (nó 1), execute o comando a seguir. `New-Cluster -Name <CNO Name> -Node <Node1 Name>, <Node2 Name> -StaticAddress <Node1 Secondary Private IP>, <Node2 Secondary Private IP>` O comando requer os seguintes parâmetros: • `Name`: o nome do cluster (CNO) • `Node`: os nomes dos nós primários e secundários, respectivamente • `StaticAddress` : os endereços IP secundári os dos nós primário e secundário, respectiv amente	

Tarefa	Descrição	Habilidades necessárias
	Important Um administrador de domínio ou usuário comum deve ter permissão de administrador em ambos os nós para criar o cluster Windows Server Failover Clustering (WSFC). Caso contrário, o comando anterior falhará e retornará a mensagem, `You do not have administrator privilege on servers`. 3. Depois que o cluster for criado, execute o comando a seguir para anexar a testemunha de compartil hamento de arquivos. `Set-ClusterQuorum -FileShareWitness \ \<FSx Windows Remote PowerShell Endpoint> \share\witness`	

Tarefa	Descrição	Habilidades necessárias
Instale o cluster de failover do SQL Server.	Depois que o cluster do WSFC estiver configurado, instale o cluster do SQL Server na instância primária (node1). 1. Na unidade T em ambos os nós, crie pastas `tempdb` e `log` . As pastas são usadas nos PowerShell comandos. 2. Depois de copiar os arquivos de mídia do SQL Server para instalação do SQL Server nos dois nós, execute o PowerShel l comando a seguir no nó 1 para instalar o SQL Server no nó 1. `D:\setup.exe /Q ` `/ACTION=InstallF ailoverCluster ` /IACCEPTSQLSERVE RLICENSETERMS ` /FEATURES="SQL,I S,BC,Conn" ` /INSTALLSHAREDDIR="C: \Program Files\Mic rosoft SQL Server” ` /INSTALLSHAREDWO WDIR="C:\Program Files (x86)\Microsoft SQL Server" ` /RSINSTALLMODE=" FilesOnlyMode" ` /INSTANCEID="MSS QLSERVER" `	AWS DevOps, DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
	`/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node1>;Cluster Network 1;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/INSTANCEDIR="C:\Program Files\Microsoft SQL Server" ` `/ENU="True" ` `/ERRORREPORTING=0 ` `/SQMREPORTING=0 ` `/SAPWD=“<Domain User password>” ` `/SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS" ` `/SQLSYSADMINACCOUNTS="<domain\username>" ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="<domain\username>" /AGTSVCPASSWORD="<Domain User password>" ` `/ISSVCACCOUNT="<domain\username>" /ISSVCPASSWORD="<Domain User password>" `	

Tarefa	Descrição	Habilidades necessárias
	`/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/INSTALLSQLDATADIR="\\<FSX DNS name>\share\Program Files\Microsoft SQL Server" ` `/SQLUSERDBDIR="\\<FSX DNS name>\share\data" ` `/SQLUSERDBLOGDIR="\\<FSX DNS name>\share\log" ` `/SQLTEMPDBDIR="T:\tempdb" ` `/SQLTEMPDBLOGDIR="T:\log" ` `/SQLBACKUPDIR="\\<FSX DNS name>\share\SQLBackup" ` `/SkipRules=Cluster_VerifyForErrors ` `/INDICATEPROGRESS`	

Tarefa	Descrição	Habilidades necessárias
Adicione um nó secundário ao cluster.	Para adicionar o SQL Server ao nó secundário (nó 2), execute o PowerShell comando a seguir. `D:\setup.exe /Q ` `/ACTION=AddNode ` `/IACCEPTSQLSERVERLICENSETERMS ` `/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node2>;Cluster Network 2;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/CONFIRMIPDEPENDENCYCHANGE=1 ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="domain\username>" /AGTSVCPASSWORD="<Domain User password>" ` `/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/SkipRules=Cluster_VerifyForErrors `	AWS DevOps, DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
	`/INDICATEPROGRESS`	
Teste a FCI do SQL Server.	1. Na instância do Windows de um dos nós, em Ferramentas Administrativas, inicie o Gerenciador de cluster de failover. 2. Navegue até Nós e confirme se o status do nó é Status em execução. 3. Selecione Perfis, abra o menu de contexto (clique com o botão direito do mouse) do SQL Server (MSSQLSERVER) e selecione Mover e selecionar nó. 4. Após a seleção do nó, o SQL Server deve estar em execução no outro nó.	DBA, engenheiro DevOps

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Limpar os recursos	Para limpar os recursos, use o processo de exclusão de CloudFormation pilhas da AWS: 1. Abra o CloudFormation console da AWS. 2. Na página Pilhas, selecione a pilha `infra`. A pilha deve	AWS DevOps, DBA, engenheiro DevOps

Tarefa	Descrição	Habilidades necessárias
	estar em execução no momento. 3. No painel de detalhes da pilha, escolha Excluir. 4. Selecione Excluir pilha quando solicitado. 5. Repita as etapas 2 a 4 para a pilha `ssm`. Após a conclusão da exclusão da pilha, as pilhas estarão no estado `DELETE_COMPLETE` . As pilhas no `DELETE_CO MPLETE` estado não são exibidas no CloudFormation console por padrão. Para exibir as pilhas excluídas, você deve alterar o filtro de visualização da pilha conforme descrito em Visualização das pilhas excluídas no console da AWS. CloudFormation Se houver falha na exclusão, uma pilha estará no estado `DELETE_FAILED` . Para obter soluções, consulte Falhas na exclusão da pilha na CloudFormation documenta ção.	

Solução de problemas

Problema	Solução
Falha no CloudFormation modelo da AWS	Se o CloudFormation modelo falhar durante a implantação, faça o seguinte: 1. Abra o CloudFormation console da AWS. 2. Na página Pilhas no CloudFormation console, selecione a pilha. 3. Selecione Eventos e verifique o status da pilha.
Falha na junção do AWS Managed Microsoft AD	Para solucionar os problemas de junção, siga estas etapas: 1. Abra o console do Systems Manager. 2. Selecione a região de implantação. 3. No painel esquerdo, selecione Automação e localize o runbook de automação com falha. 4. Abra o runbook de automação e verifique o status de execução e as etapas de execução. 5. Investigue os detalhes da etapa que falhou para ver o erro ou a falha exatos.

Recursos relacionados

- Simplifique suas implantações de alta disponibilidade do Microsoft SQL Server usando o Amazon FSx para Windows File Server
- Usando FSx o Windows File Server com o Microsoft SQL Server

Use as consultas do BMC Discovery para extrair dados de migração para o planejamento da migração

Criado por Ben Tailor-Hamblin (AWS), Simon Cunningham (AWS), Emma Baldry (AWS) e Shabnam Khan (AWS)

Resumo

Este guia fornece exemplos de consultas e etapas para ajudá-lo a extrair dados de sua infraestrutura e aplicativos on-premises usando o BMC Discovery. O padrão mostra como usar as consultas do BMC Discovery para escanear sua infraestrutura e extrair informações de software, serviços e dependências. Os dados extraídos são necessários para as fases avaliar e mobilizar de uma migração em grande escala para a nuvem da Amazon Web Services (AWS). Você poderá usar esses dados para tomar decisões críticas sobre quais aplicativos migrar juntos como parte do seu plano de migração.

Pré-requisitos e limitações

Pré-requisitos

- Uma licença para o BMC Discovery (antigo BMC ADDM) ou a versão de software como serviço (SaaS) do BMC Helix Discovery
- Versão local ou SaaS do BMC Discovery, instalada

> **Note**
>
> Para versões locais do BMC Discovery, você deve instalar o aplicativo em uma rede cliente com acesso a todos os dispositivos de rede e servidor que estão no escopo de uma migração em vários data centers. O acesso à rede do cliente deve ser fornecido de acordo com as instruções de instalação do aplicativo. Se a verificação das informações do Windows Server for necessária, você deverá configurar um dispositivo gerenciador de proxy do Windows na rede.

- Acesso à rede para permitir que o aplicativo escaneie dispositivos em datacenters, se você estiver usando o BMC Helix Discovery

Versões do produto

- BMC Discovery 22.2 (12.5)

- BMC Discovery 22.1 (12.4)
- BMC Discovery 21.3 (12.3)
- BMC Discovery 21.05 (12.2)
- BMC Discovery 20.08 (12.1)
- BMC Discovery 20.02 (12.0)
- BMC Discovery 11.3
- BMC Discovery 11.2
- BMC Discovery 11.1
- BMC Discovery 11.0
- BMC Atrium Discovery 10.2
- BMC Atrium Discovery 10.1
- BMC Atrium Discovery 10.0

Arquitetura

O diagrama a seguir mostra como os gerentes de ativos poderão usar as consultas do BMC Discovery para escanear aplicativos modelados pelo BMC em ambientes SaaS e on-premises.

O diagrama mostra o seguinte fluxo de trabalho: um gerenciador de ativos usa o BMC Discovery ou o BMC Helix Discovery para verificar instâncias de banco de dados e software em execução em servidores virtuais hospedados em vários servidores físicos. A ferramenta poderá modelar aplicativos com componentes que abrangem vários servidores virtuais e físicos.

Pilha de tecnologia

- BMC Discovery
- BMC Helix Discovery

Ferramentas

- O BMC Discovery é uma ferramenta de descoberta de datacenter que ajuda você a descobrir automaticamente seu datacenter.
- O BMC Helix Discovery é um sistema de modelagem de dependências e descoberta baseado em SaaS que ajuda você a modelar dinamicamente seus ativos de dados e suas dependências.

Práticas recomendadas

É uma prática recomendada para mapear dados de aplicativos, dependências e infraestrutura ao migrar para a nuvem. O mapeamento ajuda a entender a complexidade do ambiente atual e as dependências entre vários componentes.

As informações sobre ativos que essas consultas fornecem são importantes por vários motivos:

1. Planejamento: compreender as dependências entre os componentes ajuda a planejar o processo de migração com mais eficácia. Por exemplo, talvez seja necessário migrar alguns componentes primeiro para garantir que outros possam ser migrados com êxito.
2. Avaliação de riscos: o mapeamento das dependências entre os componentes poderá ajudá-lo a identificar possíveis riscos ou problemas que possam surgir durante o processo de migração. Por exemplo, você poderá descobrir que certos componentes dependem de tecnologias desatualizadas ou sem suporte que poderão causar problemas na nuvem.
3. Arquitetura de nuvem: mapear seus dados de aplicativo e infraestrutura também poderá ajudá-lo a projetar uma arquitetura de nuvem adequada que atenda às suas necessidades organizacionais. Por exemplo, talvez seja necessário projetar uma arquitetura de várias camadas para oferecer suporte aos requisitos de alta disponibilidade ou escalabilidade.

No geral, mapear dados de aplicativos, dependências e infraestrutura é uma etapa crucial no processo de migração para a nuvem. O exercício de mapeamento poderá ajudá-lo a entender melhor seu ambiente atual, identificar possíveis problemas ou riscos e projetar uma arquitetura de nuvem adequada.

Épicos

Identificar e avaliar as ferramentas de descoberta

Tarefa	Descrição	Habilidades necessárias
Identifique os proprietários do ITSM.	Identifique os proprietários do Gerenciamento de Serviços de TI (ITSM) (geralmente, entrando em contato com as equipes de suporte operacional).	Líder de migração

Tarefa	Descrição	Habilidades necessárias
Verificar o CMDB.	Identifique o número de bancos de dados de gerenciamento de configuração (CMDBs) que contêm informações sobre ativos e, em seguida, identifique as fontes dessas informações.	Líder de migração
Identifique as ferramentas de descoberta e verifique o uso do BMC Discovery.	Se sua organização estiver usando o BMC Discovery para enviar dados sobre seu ambiente para a ferramenta CMDB, verifique o escopo e a cobertura de seus escaneamentos. Por exemplo, verifique se o BMC Discovery está examinando todos os data centers e se os servidores de acesso estão localizados em zonas perimetrais.	Líder de migração
Verifique o nível de modelagem do aplicativo.	Verifique se os aplicativos foram modelados no BMC Discovery. Caso contrário, recomende o uso da ferramenta BMC Discovery para modelar quais instâncias de software em execução fornecem um aplicativo e um serviço comercial.	Engenheiro de migração, líder de migração

Extrair dados da infraestrutura

Tarefa	Descrição	Habilidades necessárias
Extraia dados em servidores físicos e virtuais.	Para extrair dados nos servidores físicos e virtuais examinados pelo BMC Discovery, use o Criador de consultas para executar a seguinte consulta: `search Host show key as 'Serverid', virtual, name as 'HOSTNAME', os_type as 'osName', os_version as 'OS Version', num_logical_processors as 'Logical Processor Counts', cores_per_processor as 'Cores per Processor', logical_ram as 'Logical RAM', #Consumer:StorageUse:Provider:DiskDrive.size as 'Size'` **Note** Você pode usar os dados extraídos para determinar os tamanhos de instância apropriados para a migração.	Engenheiro de migração, líder de migração
Extraia dados em aplicativos modelados.	Se seus aplicativos forem modelados no BMC Discovery	Proprietário do aplicativo BMC Discovery

Tarefa	Descrição	Habilidades necessárias
	, você poderá extrair dados sobre os servidores que executam o software do aplicativo. Para obter os nomes dos servidores, use o Criador de consultas para executar a seguinte consulta: `search SoftwareInstance show key as 'ApplicationID', #RunningSoftware:HostedSoftware:Host:Host.key as 'ReferenceID', type, name` **Note** Os aplicativos são modelados no BMC Discovery por meio de uma coleção de instâncias de software em execução. O aplicativo depende de todos os servidores que executam o software do aplicativo.	

Tarefa	Descrição	Habilidades necessárias
Extraia dados em bancos de dados.	Para obter uma lista de todos os bancos de dados escaneados e dos servidores em que esses bancos de dados estão sendo executados, use o Criador de consultas para executar a seguinte consulta: `search Database show key as 'Key', name, type as 'Source Engine Type', #Detail:Detail:ElementWithDetail:SoftwareInstance.name as 'Software Instance', #Detail:Detail:ElementWithDetail:SoftwareInstance.product_version as 'Product Version', #Detail:Detail:ElementWithDetail:SoftwareInstance.edition as 'Edition', #Detail:Detail:ElementWithDetail:SoftwareInstance.#RunningSoftware:HostedSoftware:Host:Host.key as 'ServerID'`	Proprietário do App

Tarefa	Descrição	Habilidades necessárias
Extraia dados na comunicação com o servidor.	Para obter informações sobre todas as comunicaç ões de rede entre servidores coletadas pelo BMC Discovery a partir de registros históricos de comunicações de rede, use o Criador de consultas para executar a seguinte consulta: `search Host TRAVERSE InferredElement:Inference:Associate:DiscoveryAccess TRAVERSE DiscoveryAccess:DiscoveryAccessResult:DiscoveryResult:NetworkConnectionList TRAVERSE List:List:Member:DiscoveredNetworkConnection PROCESS WITH networkConnectionInfo`	Proprietário do aplicativo BMC Discovery

Tarefa	Descrição	Habilidades necessárias
Extraia dados sobre a descoberta de aplicativos.	Para obter informações sobre dependências do aplicativo, use o Criador de consultas para executar a seguinte consulta: `search SoftwareInstance show key as 'SRC App ID', #Dependant:Dependency:DependedUpon:SoftwareInstance.key as 'DEST App ID'`	Proprietário do aplicativo BMC Discovery
Extraia dados sobre serviços comerciais.	Para extrair dados sobre serviços comerciais fornecidos por hosts, use o Criador de consultas para executar a seguinte consulta: `search Host show name, #Host:HostedSoftware:AggregateSoftware:BusinessService.name as 'Name'`	Proprietário do aplicativo BMC Discovery

Solução de problemas

Problema	Solução
A consulta falha ao ser executada ou contém colunas não preenchidas.	Analise os registros de ativos no BMC Discovery e determine quais campos você precisa. Em seguida, substitua esses campos na consulta usando o Criador de consultas.

Problema	Solução
Os detalhes de um ativo dependente não serão preenchidos.	Isso provavelmente se deve às permissões de acesso ou à conectividade de rede. A ferramenta de descoberta poderá não ter as permissões necessárias para acessar determinados ativos, especialmente se eles estiverem em redes ou ambientes diferentes. Recomendamos que você trabalhe em estreita colaboração com especialistas no assunto de descoberta para garantir que todos os ativos pertinentes sejam identificados.

Recursos relacionados

Referências

- Direito ao licenciamento BMC Discovery (Documentação da BMC)
- Recursos e componentes do BMC Discovery (Documentação do BMC)
- Guia do usuário do BMC Discovery (Documentação da BMC)
- Pesquisando dados (no BMC Discovery) (Documentação da BMC)
- Descoberta e análise de portfólio para migração (Recomendações da AWS)

Tutoriais e vídeos

- BMC Discovery: Webinar - Melhores práticas de consulta de relatórios (Parte 1) () YouTube

Realocar

Tópicos

- Migre um banco de dados Amazon RDS for Oracle para Conta da AWS outro Região da AWS e AWS DMS use-o para replicação contínua
- Migre o VMware SDDC para a VMware nuvem na AWS usando o HCX VMware
- Migrar uma instância do banco de dados Amazon RDS para outra VPC ou outra conta
- Migrar uma instância do banco de dados Amazon RDS para Oracle para outra VPC
- Migre um cluster do Amazon Redshift para uma região da AWS na China
- Transporte bancos de dados PostgreSQL entre duas instâncias de banco de dados Amazon RDS usando pg_transport

Migre um banco de dados Amazon RDS for Oracle para Conta da AWS outro Região da AWS e AWS DMS use-o para replicação contínua

Criado por Durga Prasad Cheepuri (AWS) e Eduardo Valentim (AWS)

Resumo

> **Warning**
>
> Os usuários do IAM têm credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

Esse padrão orienta você pelas etapas de migração de um banco de dados de origem do Amazon Relational Database Service (Amazon RDS) para Oracle para um banco de dados de origem diferente e. Conta da AWS Região da AWS O padrão usa um DB snapshot para uma única carga de dados completa e habilita AWS Database Migration Service (AWS DMS) para replicação contínua.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS que contém o banco de dados Amazon RDS for Oracle de origem, que foi criptografado usando uma chave AWS Key Management Service não padrão AWS KMS()
- Um ativo Conta da AWS em um banco de dados Região da AWS diferente do de origem, para usar no banco de dados Amazon RDS for Oracle de destino
- Emparelhamento de nuvem privada virtual (VPC) entre a origem e o destino VPCs
- Familiaridade com o uso de um banco de dados Oracle como fonte para AWS DMS
- Familiaridade com o uso de um banco de dados Oracle como alvo para AWS DMS

Versões do produto

- Oracle para as versões 11g (versões 11.2.0.3.v1 e posteriores) até 12.2 e 18c. Para obter a lista mais recente de versões e edições suportadas, consulte Usando um banco de dados Oracle como fonte para AWS DMS e com o uso de um banco de dados Oracle como destino AWS DMS na

AWS documentação. Para versões do Oracle compatíveis com o Amazon RDS, consulte Oracle no Amazon RDS.

Arquitetura

Pilhas de tecnologia de origem e de destino

- Instância do banco de dados Amazon RDS para Oracle

Arquitetura de replicação contínua

Ferramentas

Ferramentas usadas para carregamento completo de dados de uma só vez

- O Amazon Relational Database Service (Amazon RDS) cria um snapshot do volume de armazenamento da sua instância de banco de dados, fazendo backup de toda a instância de banco de dados e não apenas de bancos de dados individuais. Ao criar um snapshot de banco de dados, você precisa identificar de qual instância de banco de dados deseja fazer backup e, em seguida, dar um nome para a sua instância de banco de dados para que você possa restaurar a partir dela depois. O tempo necessário para criar um snapshot varia com o tamanho dos bancos de dados. Como o snapshot inclui todo o volume de armazenamento, o tamanho de arquivos, como arquivos temporários, também afeta o tempo necessário para criar o snapshot. Para obter mais informações para usar snapshots de banco de dados, consulte Criar um snapshot do banco de dados na documentação do Amazon RDS.
- AWS Key Management Service (AWS KMS) cria uma chave para a criptografia do Amazon RDS. Ao criar uma instância de banco de dados criptografada, você também pode fornecer o AWS KMSidentificador da chave de criptografia. Se você não especificar um identificador de AWS KMSchave, o Amazon RDS usa sua chave de criptografia padrão para sua nova instância de banco de dados. AWS KMScria sua chave de criptografia padrão para seu Conta da AWS. Conta da AWS A sua tem uma chave de criptografia padrão diferente para cada uma Região da AWS. Para esse padrão, a instância de banco de dados Amazon RDS deve ser criptografada usando a chave não padrão AWS KMS. Para obter mais informações sobre o uso de AWS KMSchaves para criptografia do Amazon RDS, consulte Criptografar recursos do Amazon RDS na documentação do Amazon RDS.

Ferramentas usadas para replicação contínua

- AWS Database Migration Service (AWS DMS) é usado para replicar mudanças em andamento e manter os bancos de dados de origem e destino sincronizados. Para obter mais informações sobre o uso AWS DMS para replicação contínua, consulte Como trabalhar com uma instância de AWS DMS replicação na AWS DMS documentação.

Épicos

Configure sua fonte Conta da AWS

Tarefa	Descrição	Habilidades necessárias
Preparar a instância de origem do banco de dados Oracle.	Deixe a instância do banco de dados Amazon RDS para Oracle ser executada no modo ARCHIVELOG e defina o período de retenção. Para obter detalhes, consulte Trabalhando com um banco de dados Oracle AWS gerenciado como fonte para AWS DMS.	DBA
Defina o log complementar para a instância do banco de dados Oracle de origem.	Defina o registro suplement ar em nível de banco de dados e em nível de tabela para a instância de banco de dados Amazon RDS for Oracle. Para obter detalhes, consulte Trabalhando com um banco de dados Oracle AWS gerenciado como fonte para AWS DMS.	DBA
Atualize a política de AWS KMS chaves na conta de origem.	Atualize a política de AWS KMS chaves na origem Conta da AWS para permitir que o	SysAdmin

Tarefa	Descrição	Habilidades necessárias
	destino use Conta da AWS a AWS KMS chave criptografada do Amazon RDS. Para obter detalhes, consulte a AWS KMS documentação.	
Crie um snapshot manual do banco de dados do Amazon RDS da instância do banco de dados de origem.		Usuário do IAM AWS
Compartilhe o snapshot manual e criptografado do Amazon RDS com o destino. Conta da AWS	Para obter detalhes, consulte Compartilhamento de um DB snapshot.	Usuário do IAM AWS

Configure seu alvo Conta da AWS

Tarefa	Descrição	Habilidades necessárias
Associar política.	No destino Conta da AWS, anexe uma política AWS Identity and Access Management (IAM) ao usuário raiz do IAM, para permitir que o usuário do IAM copie um DB snapshot criptografado usando a AWS KMS chave compartilhada.	SysAdmin
Mude para a fonte Região da AWS.		Usuário do IAM AWS
Copie o snapshot compartilhado.	No console do Amazon RDS, no painel Snapshots, escolha	Usuário do IAM AWS

Tarefa	Descrição	Habilidades necessárias
	Shared with Me e selecione o snapshot compartilhado. Copie o snapshot para o Região da AWS mesmo banco de dados de origem usando o Amazon Resource Name (ARN) para AWS KMS a chave usada pelo banco de dados de origem. Para obter detalhes, consulte Cópia de um DB snapshot.	
Mude para o destino Região da AWS e crie uma nova AWS KMS chave.		Usuário do IAM AWS
Copie o snapshot.	Mude para a fonte Região da AWS. No console do Amazon RDS, no painel Snapshots , escolha Owned by Me e selecione o snapshot copiado. Copie o instantâneo para o destino Região da AWS usando a AWS KMS chave do novo destino Região da AWS.	Usuário do IAM AWS

Tarefa	Descrição	Habilidades necessárias
Restaure o snapshot.	Mude para o alvo Região da AWS. No console do Amazon RDS, no painel Snapshots, escolha Owned by Me. Selecione o snapshot copiado e restaure-o para uma instância do banco de dados Amazon RDS para Oracle. Para obter detalhes, consulte Restauração a partir de um DB snapshot.	Usuário do IAM AWS

Prepare seu banco de dados de origem para replicação contínua

Tarefa	Descrição	Habilidades necessárias
Crie um usuário da Oracle com as permissões apropriadas.	Crie um usuário Oracle com os privilégios necessários para o Oracle como fonte para AWS DMS. Para obter detalhes, consulte a AWS DMS documentação.	DBA
Configure o banco de dados de origem para Oracle LogMiner ou Oracle Binary Reader.		DBA

Prepare seu banco de dados de origem para replicação contínua

Tarefa	Descrição	Habilidades necessárias
Crie um usuário da Oracle com as permissões apropriadas.	Crie um usuário Oracle com os privilégios necessários para o Oracle como alvo para AWS DMS. Para obter detalhes, consulte a AWS DMS documentação.	DBA

Crie AWS DMS componentes

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de replicação no destino. Região da AWS	Crie uma instância de replicação na VPC do destino. Região da AWS Para obter detalhes, consulte a AWS DMS documentação.	Usuário do IAM AWS
Crie endpoints de origem e destino com as conexões necessárias de criptografia e teste.	Para obter detalhes, consulte a AWS DMS documentação.	DBA
Criar tarefas de replicação.	1. Para o tipo de migração, escolha replicação contínua. 2. Para o ponto inicial da captura de dados de alteração (CDC), use o número de alteração do sistema Oracle (SCN) quando o snapshot do Amazon RDS foi obtido para carga total ou o	IAM user (Usuário do IAM)

Tarefa	Descrição	Habilidades necessárias
	timestamp quando a carga total foi obtida. 3. Para `TargetTablePrepMode`, escolha DO_NOTHING. Se a tarefa tiver tabelas de dados de objetos binários grandes (LOB), escolha o modo LOB limitado e defina o tamanho máximo de LOB como o tamanho máximo dos dados de LOB na tabela. 4. Ativar o registro em log. 5. Agrupe tabelas relacionadas por meio de chaves em uma única tarefa. Se houver tabelas com uma grande quantidade de dados de LOB e a tabela não tiver relação com outras tabelas, crie uma tarefa separada para ela com as configurações de LOB descritas anteriormente. Para obter detalhes, consulte a AWS DMS documentação.	
Inicie e monitore as tarefas.	Para obter detalhes, consulte a AWS DMS documentação.	Usuário do IAM AWS

Tarefa	Descrição	Habilidades necessárias
Habilite a validação da tarefa, se necessário.	Observe que habilitar a validação tem um impacto no desempenho da replicação. Para obter detalhes, consulte a AWS DMS documentação.	Usuário do IAM AWS

Recursos relacionados

- Alterando uma política fundamental
- Criação de um snapshot manual de banco de dados do Amazon RDS
- Criação de um snapshot manual de banco de dados do Amazon RDS
- Copiar um snapshot
- Restaurar um snapshot de banco de dados do Amazon RDS
- Começando com AWS DMS
- Usando um banco de dados Oracle como fonte para AWS DMS
- Usando um banco de dados Oracle como alvo para AWS DMS
- AWS DMS configuração usando emparelhamento de VPC
- Como faço para compartilhar snapshots manuais de banco de dados ou snapshots de cluster de banco de dados do Amazon RDS com outra pessoa? Conta da AWS (Artigo do Centro de Conhecimentos da AWS)

Migre o VMware SDDC para a VMware nuvem na AWS usando o HCX VMware

Criado por Deepak Kumar (AWS)

Resumo

Aviso: a partir de 30 de abril de 2024, o VMware Cloud on não AWS é mais revendido AWS nem por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu AWS representante para obter detalhes.

Esse padrão descreve o uso da VMware Hybrid Cloud Extension (HCX) para migrar suas máquinas virtuais (VMs) e aplicativos locais para a VMware nuvem na Amazon Web Services (AWS). A migração usa software de data center definido por software (SDDC) de VMware classe empresarial na nuvem da AWS para fornecer acesso otimizado aos serviços da AWS.

VMware O Cloud on AWS integra produtos de computação, armazenamento e virtualização de rede (vSphere, vSAN e NSX VMware) com o gerenciamento de servidores VMware vCenter, que é otimizado para ser executado em uma infraestrutura AWS dedicada, elástica e bare-metal. A infraestrutura resultante é de baixa manutenção, simplificada e hiperconvergente.

Com esse serviço, as equipes de TI podem gerenciar seus recursos baseados em nuvem com ferramentas familiares VMware . Para obter mais informações, consulte VMware Cloud on AWS no VMware site.

VMware O HCX oferece suporte a três tipos de migrações para a nuvem:

- Hibridez (extensão do data center): estender um VMware SDDC local existente para a AWS para fornecer expansão de espaço, capacidade sob demanda, um ambiente de teste/desenvolvimento e desktops virtuais.
- Evacuação da nuvem (atualização da infraestrutura de todo o datacenter): consolidando datacenters e migrando completamente para a Nuvem AWS (incluindo lidar com compartilhamento de local de datacenters ou de fim de locação).
- Migração específica de aplicativo: movendo aplicativos individuais para a Nuvem AWS para atender a necessidades comerciais específicas.

Pré-requisitos e limitações

Pré-requisitos

- Inscreva-se em uma conta da AWS (necessária para a criação do VMware Cloud SDDC).
- Inscreva-se em Minha VMware conta. Registre-se em https://my.vmware.com/web/vmware/ e preencha todos os campos.
- Verifique a versão do vCenter e dos hosts e colete o número de. VMs Se possível, solicite uma RVToolsexportação para exibir informações sobre seus ambientes virtuais. Recomendamos a versão 6.0 ou superior do vCenter.
- Você deve implantar switches virtuais distribuídos se quiser estender as redes de datacenter (L2), testar o VMotion usando o HCX ou analisar a dependência do aplicativo usando o vRealize Network Insight.
- Escolha uma rede de sub-rede de gerenciamento atual local não conflitante para criar o SDDC na nuvem na AWS. VMware
- Valide os requisitos do HCX revisando os pré-requisitos fornecidos no Guia do usuário do HCX. VMware
- Identifique e agrupe VMs as ondas de migração. Verifique VMs se você pode usar para testar.
- Colete todos os dados sobre consumo relativo de largura de banda, compressão de WAN e velocidade de transferência de dados.

Observações

- Não há necessidade de VMware NSX-V ou NSX-T no local.
- Sem custos adicionais para o HCX (ele está incluído no VMware Cloud on AWS).

Arquitetura

O diagrama a seguir mostra a solução HCX baseada em serviços de vários componentes. Cada componente suporta uma função específica na solução HCX. Para obter mais informações sobre cada componente do HCX, consulte a postagem do blog Migração de cargas de trabalho para a nuvem VMware na AWS com a extensão de nuvem híbrida (HCX).

Pilha de tecnologia de origem

- Aplicativos locais VMs e gerenciados pelo VMware vSphere

Pilha de tecnologias de destino

- VMware Nuvem na AWS

Ferramentas

- VMware HCX — O VMware HCX é uma ferramenta que você pode usar para migrar seus aplicativos e cargas de trabalho entre data centers e ambientes de nuvem. Ele está incluído no VMware Cloud on AWS.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Escolher uma estratégia de migração.	Decida se você deseja ampliar seu datacenter (hibridez), mover todos os seus datacenters (evacuação da nuvem) ou mover aplicativos específicos para a AWS.	SysAdmin, Proprietário do aplicativo
Validar os requisitos de HCX.	Para obter informações sobre migração, consulte o Guia do usuário do VMware HCX.	SysAdmin, Proprietário do aplicativo

Migre para a VMware nuvem na AWS

Tarefa	Descrição	Habilidades necessárias
Migre seus aplicativos VMs ou aplicativos.	Para obter mais informaçõ es, consulte Migração híbrida com VMware HCX na VMware documentação.	SysAdmin, Proprietário do aplicativo

Recursos relacionados

- VMware Nuvem na AWS: conceitos básicos
- Migração híbrida com VMware HCX
- VMware Guia do usuário do HCX
- VMware Preços da nuvem na AWS
- VMware Roteiro da nuvem na AWS

Migrar uma instância do banco de dados Amazon RDS para outra VPC ou outra conta

Criado por Dhrubajyoti Mukherjee (AWS)

Resumo

Este padrão fornece orientação sobre como migrar uma instância do banco de dados Amazon Relational Database Service (Amazon RDS) de uma nuvem privada virtual (VPC) para outra na mesma conta da AWS ou de uma conta da AWS para outra conta da AWS.

Esse padrão é útil se você quiser migrar suas instâncias de banco de dados do Amazon RDS para outra VPC ou conta por motivos de separação ou segurança (por exemplo, quando quiser colocar a pilha de aplicativos e o banco de dados em lugares diferentes). VPCs

A migração de uma instância de banco de dados para outra conta da AWS envolve etapas como obter um snapshot manual, compartilhá-lo e restaurá-lo na conta de destino. Esse processo pode ser demorado, dependendo das alterações do banco de dados e das taxas de transação. Também acarreta tempo de inatividade do banco de dados, portanto, planeje a migração com antecedência. Considere uma estratégia de implantação azul/verde para minimizar o tempo de inatividade. Como alternativa, você pode avaliar o AWS Data Migration Service (AWS DMS) para minimizar o tempo de inatividade devido à alteração. No entanto, esse padrão não cobre essa opção. Para saber mais, consulte a documentação do AWS DMS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões do AWS Identity and Access Management (IAM) necessárias para VPC, sub-redes e console do Amazon RDS

Limitações

- Alterações em uma VPC acarretam a reinicialização do banco de dados, resultando em interrupções no aplicativo. Recomendamos migrar em horários fora de pico.
- Limitações ao migrar o Amazon RDS para outra VPC:
  - A instância de banco de dados que você está migrando deve ser uma única instância sem espera. Ela não deve ser membro de um cluster.
  - O Amazon RDS não deve estar em diversas zonas de disponibilidade.

  - O Amazon RDS não deve ter nenhuma réplica de leitura.
  - O grupo de sub-redes criado na VPC de destino deve ter sub-redes da zona de disponibilidade em que o banco de dados de origem está sendo executado.
- Limitações ao migrar o Amazon RDS para outra conta da AWS:
  - Atualmente, não há compatibilidade para o compartilhamento de snapshots criptografados com a chave de serviço padrão do Amazon RDS.

Arquitetura

Migração para uma VPC na mesma conta da AWS

O diagrama a seguir mostra o fluxo de trabalho para migrar uma instância do banco de dados Amazon RDS para uma VPC diferente na mesma conta da AWS.

Consiste das etapas a seguir. Para obter instruções detalhadas, consulte a seção Tópicos.

1. Crie um grupo de sub-redes de banco de dados na VPC de destino. Um grupo de sub-redes de banco de dados é uma coleção de sub-redes que você pode usar para especificar uma VPC específica ao criar instâncias de banco de dados.
2. Configure a instância do banco de dados Amazon RDS na VPC de origem para usar o novo grupo de sub-redes de banco de dados.
3. Aplique as alterações para migrar o banco de dados do Amazon RDS para a VPC de destino.

Migrar para uma conta da AWS diferente

O diagrama a seguir mostra o fluxo de trabalho para migrar uma instância do banco de dados Amazon RDS para uma conta diferente da AWS.

Consiste das etapas a seguir. Para obter instruções detalhadas, consulte a seção Tópicos.

1. Acesse a instância do banco de dados Amazon RDS na conta de origem da AWS.
2. Crie um snapshot do Amazon RDS na conta de origem da AWS.
3. Compartilhe o snapshot do Amazon RDS com a conta de destino da AWS.
4. Acesse o snapshot do Amazon RDS n conta de destino da AWS.

5. Crie uma instância do banco de dados do Amazon RDS na conta de destino da AWS.

Ferramentas

Serviços da AWS

- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Práticas recomendadas

- Se o tempo de inatividade do banco de dados for uma preocupação ao migrar uma instância do banco de dados Amazon RDS para outra conta, recomendamos que você use o AWS DMS. Esse serviço fornece replicação de dados, o que acarreta menos de cinco minutos de interrupção.

Épicos

Migrar para uma VPC diferente na mesma conta da AWS

Tarefa	Descrição	Habilidades necessárias
Crie uma nova VPC.	No console da Amazon VPC, crie uma nova VPC e sub-redes com as propriedades e os intervalos de endereços IP desejados. Para obter instruções detalhadas, consulte a Documentação do Amazon VPC.	Administrador
Criar um grupo de sub-redes de banco de dados.	No console do Amazon RDS: 1. Escolha Grupos de sub-redes) e Criar grupo de	Administrador

Tarefa	Descrição	Habilidades necessárias
	sub-redes de banco de dados. 2. Insira o nome, a descrição e o ID da VPC do grupo de sub-redes. 3. Adicione as sub-redes que pertencem ao grupo de sub-redes. Adicione sub-redes para abranger pelo menos duas zonas de disponibilidade. 4. Escolha Criar. Para obter mais informações, consulte a documentação do Amazon RDS.	

Tarefa	Descrição	Habilidades necessárias
Modifique a instância do banco de dados Amazon RDS para usar o novo grupo de sub-redes.	No console do Amazon RDS: 1. No painel de navegação, escolha Bancos de dados e em seguida escolha a instância de banco de dados Amazon RDS a ser migrado. 2. Na seção Conectividade, escolha o grupo de sub-redes associado à VPC de destino. 3. Na seção Programar modificações, selecione Aplicar imediatamente. Quando a migração para a VPC de destino é concluída, o grupo de segurança padrão da VPC de destino é atribuído à instância do banco de dados Amazon RDS. Você pode configurar um novo grupo de segurança para essa VPC com as regras de entrada e de saída necessárias para a instância do seu banco de dados. Como alternativa, use a AWS Command Line Interface (AWS CLI) para realizar a migração para a VPC de destino fornecendo explicita	Administrador

Tarefa	Descrição	Habilidades necessárias
	mente o novo ID do grupo de segurança da VPC. Por exemplo: `aws rds modify-db-instance \ --db-instance-identifier testrds \ --db-subnet-group-name new-vpc-subnet-group \ --vpc-security-group-ids sg-idxxxx \ --apply-immediately`	

Migrar para uma conta diferente da AWS

Tarefa	Descrição	Habilidades necessárias
Crie uma nova VPC e um novo grupo de sub-redes na conta de destino da AWS.	1. No console da Amazon VPC, crie uma nova VPC com as propriedades e os intervalos de endereços IP desejados. Para obter instruções detalhadas, consulte a Documentação do Amazon VPC. 2. Crie sub-redes para a nova VPC seguindo as instruções fornecidas na documentação da Amazon VPC. 3. No console do Amazon RDS, crie grupos de sub-redes de banco de dados.	Administrador

Tarefa	Descrição	Habilidades necessárias
	Para obter instruções, consulte a Documentação do Amazon RDS.	
Compartilhe um snapshot manual do banco de dados com a conta de destino.	1. Obtenha um snapshot manual do banco de dados de origem seguindo as instruções fornecidas na documentação do Amazon RDS. 2. Compartilhe o snapshot com a conta de destino da AWS fornecendo o ID da conta de destino. Para obter instruções, consulte o artigo do ref:Post sobre o compartilhamento de snapshots de bancos de dados com outras contas.	Administrador
Iniciar uma instância nova de banco de dados do Amazon RDS.	Iniciar uma instância nova do banco de dados do Amazon RDS a partir do snapshot na conta de destino da AWS. Para obter instruções, consulte a Documentação do Amazon RDS.	Administrador

Recursos relacionados

- Documentação da Amazon VPC
- Documentação do Amazon RDS
- Como altero a VPC para uma instância de banco de dados do Amazon RDS? (Artigo do AWS ref:Post)

- Como faço para transferir a propriedade dos recursos do Amazon RDS para uma conta diferente da AWS? (Artigo do AWS ref:Post)
- Como faço para compartilhar snapshots manuais de banco de dados do Amazon RDS ou snapshots de cluster de banco de dados do Aurora? (Artigo do AWS ref:Post)
- Documentação do AWS DMS

Migrar uma instância do banco de dados Amazon RDS para Oracle para outra VPC

Criado por Pinesh Singal (AWS)

Resumo

Esse padrão de migração fornece step-by-step orientação para migrar uma instância do Amazon Relational Database Service (Amazon RDS) para banco de dados (DB) Oracle de uma nuvem privada virtual (VPC) para outra VPC na mesma conta da Amazon Web Services (AWS). Por exemplo, você pode usar esse padrão se sua empresa exigir que o banco de dados e o servidor de aplicativos Amazon Elastic Compute Cloud (Amazon EC2) estejam na mesma VPC.

O padrão descreve uma estratégia de migração on-line com pouco ou nenhum tempo de inatividade para um banco de dados de origem Oracle de vários terabytes com um grande número de transações.

Para mover uma instância do banco de dados Amazon RDS para Oracle para outra VPC, você deve alterar o grupo de sub-redes do Amazon RDS. Esse grupo de sub-redes precisa ser pré-configurado com a nova VPC e as sub-redes necessárias. Durante a mudança da VPC de uma rede para outra, a instância do Amazon RDS é reinicializada, então o banco de dados não estará acessível enquanto a movimentação estiver em andamento.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Dois VPCs com sub-redes privadas
- Uma instância do banco de dados Amazon RDS para Oracle (em execução), configurada com grupos de segurança de entrada e saída

Limitações

- Uma instância do banco de dados que abrange várias zonas de disponibilidade (Multi-AZ) não é compatível. Esse padrão fornece uma maneira de contornar essa limitação.
- A instância do banco de dados não pode ser migrada enquanto uma réplica de leitura está ativada.
- O grupo de sub-redes na nova VPC deve estar na mesma zona de disponibilidade que o banco de dados.

- A migração deve ocorrer durante o período de manutenção programada ou em períodos de baixo tráfego, pois mover o banco de dados para outra VPC acarreta a reinicialização do banco de dados, resultando em paralisações do aplicativo por alguns minutos.

Versões do produto

- Instância do banco de dados Amazon RDS para Oracle, 12.1.0.2 e posterior

Arquitetura

Pilha de tecnologia de origem

- Uma instância do banco de dados Amazon RDS para Oracle 12.1.0.2.v22 em uma VPC
- Uma VPC configurada em uma tabela de rotas separada
- Grupos de sub-redes do Amazon RDS configurados em uma VPC
- Grupo de opções do Amazon RDS (se necessário)

Pilha de tecnologias de destino

- Uma instância do banco de dados Amazon RDS para Oracle com a versão 12.1.0.2.v22 em uma outra VPC
- Uma VPC Amazon configurada em uma rota separada
- Grupos de sub-redes do Amazon RDS configurados em uma nova VPC
- Grupo de opções do Amazon RDS (se necessário)

Arquitetura de origem e destino

O diagrama a seguir mostra o uso do console para mover o banco de dados Amazon RDS para Oracle de uma sub-rede privada em uma VPC para uma sub-rede privada em outra VPC.

1. Use o console para modificar a instância do banco de dados Amazon RDS para Oracle.
2. Na VPC de destino, modifique o grupo de sub-redes e o grupo de opções, se usado.

Ferramentas

- Amazon RDS - o Amazon Relational Database Service (Amazon RDS) é um serviço Web que facilita a configuração, a operação e escalabilidade de um banco de dados relacional na Nuvem AWS. Ele fornece capacidade econômica e redimensionável para um banco de dados relacional e gerencia tarefas comuns de administração de banco de dados. Esse padrão usa o Amazon RDS para Oracle.

Épicos

Alterar a configuração do banco de dados Amazon RDS para Oracle na VPC existente

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de sub-redes.	Configure um grupo de sub-redes no Amazon RDS.	AWS geral
Crie um grupo de opções.	(Opcional) Configure um grupo de opções no Amazon RDS.	AWS geral
Modifique a instância do banco de dados para o Amazon RDS para Oracle.	Modifique o banco de dados com o grupo de sub-redes e o grupo de opções.	AWS geral, DBA
Atualize o banco de dados Oracle, se necessário.	Para migrar o banco de dados Amazon RDS para Oracle de origem, faça as seguintes alterações: • Remova as réplicas de leitura, se houver. • Desative o atributo Multi-AZ, se estiver ativado.	AWS geral

Configurar o banco de dados do Amazon RDS para Oracle na VPC de destino

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de sub-redes.	No Amazon RDS, configure um grupo de sub-redes usando a sub-rede da nova VPC e a zona de disponibi lidade do banco de dados.	AWS geral
Crie um grupo de opções.	(Opcional) Configure um grupo de opções no Amazon RDS.	AWS geral
Modifique o banco de dados Amazon RDS para Oracle.	Modifique o banco de dados com o novo grupo de sub-redes e o grupo de opções da nova VPC. Você pode aplicar essas alterações imediatam ente ou em uma janela de manutenção. A modificação pode demorar vários minutos para ser concluído. Durante a modificação, você verá as seguintes alterações de status: • moving-to-vpc • C onfiguring-enhanced-monitoring • Modificar • Available (Disponível) A modificação anexará o grupo de segurança padrão	AWS geral, DBA

Tarefa	Descrição	Habilidades necessárias
	da nova VPC. Anexe um novo grupo de segurança conforme exigido pelo Amazon RDS para Oracle.	
Atualize o banco de dados Amazon RDS para Oracle, se necessário.	Depois de migrar para o banco de dados Amazon RDS para Oracle de destino na nova VPC, faça as seguintes modificações, se necessário: • Ative as réplicas de leitura, se existirem no banco de dados de origem. • Ative o atributo Multi-AZ, se estiver ativado no banco de dados de origem.	AWS geral
Teste a conectividade do aplicativo.	Execute um teste de conectividade do banco de dados a partir de qualquer aplicativo. Confirme se o banco de dados Amazon RDS para Oracle modificado na nova VPC está conectado e pode ser acessado pelo aplicativo.	Proprietário do App

Recursos relacionados

- Documentação da Amazon VPC
- VPCs e sub-redes
- Trabalhar com uma instância de banco de dados em uma VPC
- Documentação do Amazon RDS
- Oracle no Amazon RDS

- Console do Amazon RDS
- Como altero a VPC para uma instância de banco de dados do Amazon RDS?

Migre um cluster do Amazon Redshift para uma região da AWS na China

Criado por Jing Yan (AWS)

Resumo

Esse padrão fornece uma step-by-step abordagem para migrar um cluster do Amazon Redshift de outra região da AWS para uma região da AWS na China.

Este padrão usa comandos SQL para recriar todos os objetos do banco de dados, além do comando UNLOAD para mover esses dados do Amazon Redshift para um bucket do Amazon Simple Storage Service (Amazon S3) na região de origem. Em seguida, os dados são migrados para um bucket do S3 na região da AWS na China. O comando COPY é usado para carregar dados do bucket do S3 e transferi-los para o cluster de destino do Amazon Redshift.

Atualmente, o Amazon Redshift não é compatível com os recursos entre regiões, como cópia de snapshots para regiões da AWS na China. Este padrão fornece uma maneira de contornar essa limitação. Você também pode reverter as etapas deste padrão para migrar dados de uma região da AWS na China para outra região da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Contas ativas da AWS em uma região da China e em uma região da AWS fora da China
- Clusters existentes do Amazon Redshift em uma região da China e em uma região da AWS fora da China

Limitações

- Essa é uma migração off-line, o que significa que o cluster de origem do Amazon Redshift não pode realizar operações de gravação durante a migração.

Arquitetura

Pilha de tecnologia de origem

- Migre um cluster do Amazon Redshift para uma região da AWS na China

Pilha de tecnologias de destino

- Migre um cluster do Amazon Redshift para uma região da AWS na China

Arquitetura de destino

Ferramentas

Ferramentas

- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade líder do setor, disponibilidade de dados, segurança e performance. Você pode usar o Amazon S3 para armazenar dados do Amazon Redshift e copiar dados de um bucket do S3 para o Amazon Redshift.
- Amazon Redshift: o Amazon Redshift é um serviço de data warehouse em escala de petabytes totalmente gerenciado na nuvem.
- psql: o psql é um frontend baseado em terminal para o PostgreSQL.

Épicos

Prepare-se para a migração na região de origem

Tarefa	Descrição	Habilidades necessárias
Inicie e configure uma EC2 instância na região de origem.	Faça login no AWS Management Console e abra o console Amazon Elastic Compute Cloud (Amazon EC2). Na barra de navegação na parte superior da tela, a região atual é exibida. Essa região não pode ser uma região da AWS na China. No painel do EC2 console da Amazon, escolha “Launch instance” e crie e configure uma EC2 instância. Important e: garanta que seus grupos de	DBA, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	EC2 segurança para regras de entrada permitam acesso irrestrito à porta TCP 22 de sua máquina de origem. Para obter instruções sobre como iniciar e configurar uma EC2 instância, consulte a seção “Recursos relacionados”.	
Instale a ferramenta psql.	Baixe e instale o PostgreSQL. O Amazon Redshift não fornece a ferramenta psql; ele é instalado com PostgreSQL. Para obter mais informações sobre como usar psql e instalar as ferramentas do PostgreSQL, consulte a seção “Recursos relacionados”.	DBA

Tarefa	Descrição	Habilidades necessárias
Registre os detalhes do cluster do Amazon Redshift.	No console do Amazon Redshift, no painel de navegação, selecione “Clusters”. Em seguida, escolha o nome do cluster do Amazon Redshift na lista. Na guia “Propriedades”, na seção “Configurações do banco de dados”, registre o “Nome do banco de dados” e a “Porta”. Abra a seção “Detalhes da conexão” e registre o “Endpoint”, que está no formato “endpoint :<port>/<databasename>”. Importante: garanta que seus grupos de segurança do Amazon Redshift para regras de entrada permitam acesso irrestrito à porta TCP 5439 de sua instância. EC2	DBA
Conecte o psql ao cluster do Amazon Redshift.	Em um prompt de comando, especifique as informações de conexão executando o comando “psql -h <endpoint > -U <userid> -d <database name> -p <port>”. No prompt da senha do psql, digite a senha do usuário “<userid>”. Assim você está conectado ao cluster do Amazon Redshift e pode inserir os comandos interativamente.	DBA

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Abra o console do Amazon S3 e crie um bucket do S3 para armazenar os arquivos exportados do Amazon Redshift. Para obter instruções sobre como criar um bucket do S3, consulte a seção “Recursos relacionados”.	DBA, AWS geral
Crie uma política do IAM que forneça suporte ao descarregamento de dados.	Abra o console do AWS Identity and Access Management (IAM) e escolha “Políticas”. Escolha “Criar política” e escolha a guia “JSON”. Copie e cole a política do IAM para descarregar dados da seção “Informações adicionais”. Importante: substitua “s3_bucket_name” pelo seu nome do bucket do S3. Escolha “Revisar política” e Insira um nome e uma descrição para a política. Escolha “Criar política”.	DBA

Tarefa	Descrição	Habilidades necessárias
Crie um perfil do IAM para permitir a operação UNLOAD no Amazon Redshift.	Abra o console do IAM e escolha “Perfis”. Escolha “Criar perfil” e “Serviço da AWS” em “Selecionar tipo de entidade confiável”. Escolha “Redshift” para o serviço, “Redshift – Personalizável” e, em seguida, “Avançar”. Escolha a política “Descarregar” que você criou anteriormente e, em seguida, “Avançar”. Digite um “nome de função” e escolha “Criar função”.	DBA
Associe um perfil do IAM ao cluster do Amazon Redshift.	Abra o console do Amazon Redshift e escolha “Gerenciar perfis do IAM”. Escolha “Perfis disponíveis” no menu suspenso e selecione o perfil que você criou anteriormente. Selecione “Aplicar alterações.” Quando o “Status” do perfil do IAM em “Gerenciar perfis do IAM” for exibido como “Em sincronização”, você poderá executar o comando UNLOAD.	DBA
Pare as operações de gravação no cluster do Amazon Redshift.	Você deve se lembrar de interromper todas as operações de gravação no cluster de origem do Amazon Redshift até que a migração seja concluída.	DBA

Prepare para a migração na região de destino

Tarefa	Descrição	Habilidades necessárias
Inicie e configure uma EC2 instância na região de destino.	Faça login no Console de Gerenciamento da AWS de uma região na China, seja Pequim ou Ningxia. No EC2 console da Amazon, escolha “Launch instance” e crie e configure uma EC2 instância . Importante: certifique-se de que seus grupos EC2 de segurança da Amazon para regras de entrada permitam acesso irrestrito à porta TCP 22 de sua máquina de origem. Para obter mais instruções sobre como iniciar e configura r uma EC2 instância, consulte a seção “Recursos relaciona dos”.	DBA
Registre os detalhes do cluster do Amazon Redshift.	No console do Amazon Redshift, no painel de navegação, selecione “Clusters”. Em seguida, escolha o nome do cluster do Amazon Redshift na lista. Na guia “Propriedades”, na seção “Configurações do banco de dados”, registre o “Nome do banco de dados” e a “Porta”. Abra a seção “Detalhes da conexão” e registre o “Endpoint”, que está no formato “endpoint:<port>/	DBA

Tarefa	Descrição	Habilidades necessárias
	<databasename>”. Important e: certifique-se de que seus grupos de segurança do Amazon Redshift para regras de entrada permitam acesso irrestrito à porta TCP 5439 da sua instância. EC2	
Conecte o psql ao cluster do Amazon Redshift.	Em um prompt de comando, especifique as informações de conexão executando o comando “psql -h <endpoint > -U <userid> -d <database name> -p <port>”. No prompt da senha do psql, digite a senha do usuário “<userid>”. Assim você está conectado ao cluster do Amazon Redshift e pode inserir os comandos interativamente.	DBA
Criar um bucket do S3.	Abra o console do Amazon S3 e crie um bucket do S3 para armazenar os arquivos exportados do Amazon Redshift. Para obter ajuda com esse e outros artigos, consulte a seção “Recursos relacionados”.	DBA

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM que seja compatível com cópia de dados.	Abra o console do IAM e escolha “Políticas”. Escolha “Criar política” e escolha a guia “JSON”. Copie e cole a política do IAM para descarregar dados da seção “Informações adicionais”. Importante: substitua “s3_bucket_name” pelo seu nome do bucket do S3. Selecione “Revisar política”, insira um nome e uma descrição para a política. Escolha “Criar política”.	DBA
Crie um perfil do IAM para permitir a operação COPY no Amazon Redshift.	Abra o console do IAM e escolha “Perfis”. Escolha “Criar perfil” e “Serviço da AWS” em “Selecionar tipo de entidade confiável”. Escolha “Redshift” para o serviço, “Redshift – Personalizável” e, em seguida, “Avançar” . Escolha a política “Copy” que você criou anteriormente e, em seguida, “Próximo”. Digite um “nome de função” e escolha “Criar função”.	DBA

Tarefa	Descrição	Habilidades necessárias
Associe um perfil do IAM ao cluster do Amazon Redshift.	Abra o console do Amazon Redshift e escolha “Gerencia r perfis do IAM”. Escolha “Perfis disponíveis” no menu suspenso e selecione o perfil que você criou anteriormente. Selecione “Aplicar alteraçõe s.” Quando o “Status” do perfil do IAM em “Gerenciar perfis do IAM” for exibido como “Em sincronização”, você poderá executar o comando COPY.	DBA

Verifique os dados de origem e as informações do objeto antes de iniciar a migração

Tarefa	Descrição	Habilidades necessárias
Verifique as linhas nas tabelas de origem do Amazon Redshift.	Use os scripts na seção “Informações adicionais” para verificar e registrar o número de linhas nas tabelas de origem do Amazon Redshift. Lembre-se de dividir os dados uniformemente para os scripts UNLOAD e COPY. Isso melhorará a eficiênci a do descarregamento e carregamento dos dados, pois a quantidade de dados abrangida por cada script será equilibrada.	DBA
Verifique o número de objetos de banco de dados no	Use os scripts na seção “Informações adicionais” para	DBA

Tarefa	Descrição	Habilidades necessárias
cluster de origem do Amazon Redshift.	verificar e registrar o número de bancos de dados, usuários, esquemas, tabelas, visualizações e funções definidas pelo usuário (UDFs) em seu cluster de origem do Amazon Redshift.	
Verifique os resultados da instrução SQL antes da migração.	Algumas instruções SQL para validação de dados devem ser classificadas de acordo com as situações reais de negócios e dados. Isso serve para verificar os dados importados a fim de garantir que sejam consistentes e exibidos corretamente.	DBA

Migrar dados e objetos para a região de destino

Tarefa	Descrição	Habilidades necessárias
Gere scripts DDL do Amazon Redshift.	Gere scripts do tipo linguagem de definição de dados (DDL) usando os links da seção “Instruções SQL para consultar o Amazon Redshift” na seção “Informações adicionais”. Esses scripts DDL devem incluir as consultas “criar usuário”, “criar esquema”, “privilégios sobre o esquema para o usuário”, “criar tabela/visualização”,	DBA

Tarefa	Descrição	Habilidades necessárias
	“privilégios sobre objetos para o usuário” e “criar função”.	
Crie objetos no cluster do Amazon Redshift para a região de destino.	Execute os scripts DDL usando a AWS Command Line Interface (AWS CLI) na região da AWS na China. Crie objetos no cluster do Amazon Redshift para a região de destino.	DBA
Descarregue os dados de origem do cluster do Amazon Redshift no bucket do S3.	Execute o comando UNLOAD para descarregar dados do cluster do Amazon Redshift na região de origem para o bucket do S3.	DBA, Desenvolvedor
Transfira os dados do bucket do S3 da região de origem para o bucket do S3 da região de destino.	Transfira os dados de origem do bucket da região S3 para o bucket da região S3 de destino. Como o comando “$ aws s3 sync” não pode ser usado, certifique-se de seguir o processo descrito no artigo “Transferência de dados do Amazon S3 de regiões da AWS para regiões da AWS na China” na seção “Recursos relacionados”.	Desenvolvedor
Carregue dados no cluster de destino do Amazon Redshift.	Na ferramenta psql da sua região de destino, execute o comando COPY para carregar dados do bucket do S3 para o cluster de destino do Amazon Redshift.	DBA

Verifique os dados nas regiões de origem e de destino após a migração

Tarefa	Descrição	Habilidades necessárias
Verifique e compare o número de linhas nas tabelas de origem e de destino.	Verifique e compare o número de linhas nas tabelas de origem e de destino.	DBA
Verifique e compare o número de linhas nas tabelas de origem e de destino.	Verifique e compare o número de linhas nas tabelas de origem e de destino.	DBA
Verifique e compare os resultados do script SQL nas regiões de origem e de destino.	Execute os scripts SQL preparados antes da migração. Verifique e compare os dados para garantir que os resultados do SQL estejam corretos.	DBA
Redefina as senhas de todos os usuários no cluster de destino do Amazon Redshift.	Depois que a migração for concluída e todos os dados forem verificados, você deverá redefinir todas as senhas de usuário do cluster do Amazon Redshift na região da AWS na China.	DBA

Recursos relacionados

- Transferência de dados do Amazon S3 de regiões da AWS para regiões da AWS na China
- Criar um bucket do S3
- Redefinição de uma senha de usuário do Amazon Redshift
- Documentação do JDBC

Mais informações

Política do IAM para descarregar dados

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

Política do IAM para copiar dados

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

Instruções SQL para consultar o Amazon Redshift

```
##Database

select * from pg_database where datdba>1;

##User
```

```
select * from pg_user where usesysid>1;

##Schema

SELECT n.nspname AS "Name",

  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"

FROM pg_catalog.pg_namespace n

WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'

ORDER BY 1;

##Table

select count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema');

select schemaname,count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema') group by schemaname order by 1;

##View

SELECT

    n.nspname AS schemaname,c.relname AS
 viewname,pg_catalog.pg_get_userbyid(c.relowner) as "Owner"

FROM

    pg_catalog.pg_class AS c

INNER JOIN

    pg_catalog.pg_namespace AS n

    ON c.relnamespace = n.oid

WHERE relkind = 'v' and n.nspname not in ('information_schema','pg_catalog');

##UDF

SELECT
```

```
   n.nspname AS schemaname,
   p.proname AS proname,
   pg_catalog.pg_get_userbyid(p.proowner) as "Owner"
FROM pg_proc p
LEFT JOIN pg_namespace n on n.oid = p.pronamespace
WHERE p.proowner != 1;
```

Scripts SQL para gerar instruções DDL

- Script Get_schema_priv_by_user
- Script Generate_tbl_ddl
- Generate_view_ddl
- Generate_user_grant_revoke_ddl
- Generate_udf_ddl

Transporte bancos de dados PostgreSQL entre duas instâncias de banco de dados Amazon RDS usando pg_transport

Criado por Raunak Rishabh (AWS) e Jitender Kumar (AWS)

Resumo

Esse padrão descreve as etapas para migrar bancos de dados extremamente grandes entre duas instâncias de banco de dados Amazon Relational Database Service (Amazon RDS) para PostgreSQL usando a extensão pg_transport. Esta extensão fornece um mecanismo de transporte físico para mover cada banco de dados. Ao fazer streaming dos arquivos do banco de dados com o mínimo de processamento, ele fornece um método extremamente rápido para migrar grandes bancos de dados entre instâncias de banco de dados com o mínimo de tempo de inatividade. Essa extensão usa um modelo pull, em que a instância do banco de dados de destino importa o banco de dados da instância de banco de dados de origem.

Pré-requisitos e limitações

Pré-requisitos

- Ambas as instâncias de banco de dados devem executar a mesma versão principal do PostgreSQL.
- O banco de dados não deve existir no destino. Caso contrário, ocorrerá uma falha no transporte.
- Nenhuma extensão diferente de pg_transport deve ser habilitada no banco de dados de origem.
- Todos os objetos do banco de dados de origem devem estar no espaço de tabela padrão pg_default.
- O grupo de segurança da instância de banco de dados de origem deveria permitir tráfego da instância de banco de dados de destino.
- Instale um cliente PostgreSQL, como o psql, PgAdminou para trabalhar com a instância de banco de dados PostgreSQL do Amazon RDS. Você pode instalar o cliente em seu sistema local ou usar uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Nesse padrão, usamos psql em uma EC2 instância.

Limitações

- Você não pode transportar bancos de dados entre diferentes versões principais do Amazon RDS para PostgreSQL.

- Os privilégios de acesso e a propriedade do banco de dados de origem não são transferidos para o banco de dados de destino.
- Não é possível transportar bancos de dados em réplicas de leitura nem em instâncias pai de réplicas de leitura.
- Não é possível usar os tipos de dados reg em nenhuma tabela de banco de dados que você planeja transportar com esse método.
- É possível executar até 32 transportes totais ao mesmo tempo (inclusive importações e exportações) em uma instância de banco de dados.
- Você não pode renomear ou incluir/excluir tabelas. Tudo é migrado como está.

Cuidado

- Faça backups antes de remover a extensão, pois a remoção da extensão também remove objetos dependentes e alguns dados essenciais para a operação do banco de dados.
- Considere a classe da instância e os processos em execução em outros bancos de dados na instância de origem ao determinar o número de operadores e os valores `work_mem` para pg_transport.
- Quando o transporte é iniciado, todas as conexões no banco de dados de origem são encerradas e o banco de dados é colocado no modo somente leitura.

> **Note**
>
> Quando o transporte está sendo executado em um banco de dados, ele não afeta outros bancos de dados no mesmo servidor.

Versões do produto

- Amazon RDS para PostgreSQL 10.10 e posterior e Amazon RDS para PostgreSQL 11.5 e posterior. Para obter as informações sobre a versão mais recente, consulte Transporte de bancos de dados PostgreSQL entre instâncias de banco de dados na documentação do Amazon RDS.

Arquitetura

Ferramentas

- pg_transport fornece um mecanismo de transporte físico para mover cada banco de dados. Ao fazer streaming dos arquivos do banco de dados com o mínimo de processamento, o transporte físico move os dados muito mais rapidamente que os processos tradicionais de despejo e carregamento e leva um tempo de inatividade mínimo. Os bancos de dados PostgreSQL transportáveis usam um modelo pull, em que a instância do banco de dados de destino importa o banco de dados da instância de banco de dados de origem. Você instala essa extensão em suas instâncias de banco de dados ao preparar os ambientes de origem e de destino, conforme explicado nesse padrão.
- O psql permite que você se conecte e trabalhe com suas instâncias de banco de dados PostgreSQL. Para instalar o psql em seu sistema, consulte a página de downloads do PostgreSQL.

Épicos

Crie o grupo de parâmetros de destino

Tarefa	Descrição	Habilidades necessárias
Crie um grupo de parâmetros para o sistema de destino.	Especifique um nome de grupo que o identifique como um grupo de parâmetros de destino; por exemplo, `pgtarget-param-group` . Para obter instruções, consulte a documentação do Amazon RDS.	DBA
Modificar os parâmetros no grupo de parâmetros.	Defina os seguintes parâmetros: 1. Adicione `pg_transport` ao parâmetro `shared_preload_libraries` . `shared_preload_libraries = pg_stat_s`	DBA

Tarefa	Descrição	Habilidades necessárias
	`tatements, pg_transp ort` 2. Defina o parâmetro `pg_transport.num_w orkers` . Escolha o número de operadores com os quais você deseja executar o transporte. O valor definido determina o número de operadores `transport.send_fil e` que serão criados na origem. 3. Aumente o valor de `max_worker_process es` para mais de três vezes o valor de `pg_transport.num_w orkers` . Por exemplo, se você definir o valor de `pg_transport.num_w orkers` como 4, o valor de `max_worke r_processes` deverá ser pelo menos 13. Se isso falhar, o pg_transp ort recomenda um valor mínimo. 4. Defina `pg_transp ort.timing` como 1. Essa configuração permite relatar informações de tempo durante o transporte.	

Tarefa	Descrição	Habilidades necessárias
	5. Defina o parâmetro `pg_transport.work_mem`. Esse parâmetro especifica a memória máxima a ser alocada para cada operador. O valor padrão é 128 MB. Para obter mais informações sobre estes parâmetros, consulte a documentação do Amazon RDS.	

Criar o grupo de parâmetros de origem

Tarefa	Descrição	Habilidades necessárias
Crie um grupo de parâmetros para o sistema de origem.	Especifique um nome de grupo que o identifique como um grupo de parâmetros de origem; por exemplo, `pgsource-param-group`. Para obter instruções, consulte a documentação do Amazon RDS.	DBA
Modificar os parâmetros no grupo de parâmetros.	Defina os seguintes parâmetros: 1. Adicione `pg_transport` ao parâmetro `shared_preload_libraries`. `shared_preload_libraries = pg_stat_s`	DBA

Tarefa	Descrição	Habilidades necessárias
	`tatements, pg_transp ort` 2. Defina o parâmetro `pg_transport.num_w orkers` . O valor desse parâmetro definido na meta determina o número de operadores `transport .send_file` a serem usados. Se você tiver uma importação em execução nessa instância, aumente esse valor, mas considere o número de operadores que já estão em execução. 3. Aumente o valor de `max_worker_process es` para mais de três vezes o valor de `pg_transport.num_w orkers` do destino. Por exemplo, se você definir o valor de `pg_transp ort.num_workers` como 4 no destino, o valor de `max_worke r_processes` na origem deverá ser pelo menos 13. Se isso falhar, o pg_transport recomenda um valor mínimo. 4. Defina o parâmetro `pg_transport.work_ mem` . Esse parâmetro	

Tarefa	Descrição	Habilidades necessárias
	especifica a memória máxima a ser alocada para cada operador. O valor padrão é 128 MB. Para obter mais informaçõ es sobre estes parâmetros, consulte a documentação do Amazon RDS.	

Prepare o ambiente de destino

Tarefa	Descrição	Habilidades necessárias
Crie uma nova instância de banco de dados Amazon RDS para PostgreSQL para a qual transportar seu banco de dados de origem.	Determine a classe da instância e a versão do PostgreSQL com base nos requisitos da sua empresa.	DBA, administrador de sistemas, arquiteto de banco de dados
Modifique o grupo de segurança do destino para permitir conexões na porta da instância de banco de dados a partir da EC2 instância.	A porta padrão para a instância PostgreSQL é 5432. Se você estiver usando outra porta, as conexões com essa porta devem estar abertas para a EC2 instância.	DBA, administrador de sistemas
Modifique a instância e atribua o novo grupo de parâmetros de destino.	Por exemplo, `.pgtarget-param-group`	DBA
Reiniciar a instância de banco de dados do Amazon RDS.	Os parâmetros `shared_preload_libraries` e `max_worker_processes` são parâmetros estáticos e	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	exigem a reinicialização da instância.	
Conecte-se ao banco de dados a partir da EC2 instância usando psql.	Use o comando: `psql -h <rds_end_point> -p PORT -U username -d database -W`	DBA
Crie a extensão pg_transport.	Execute a consulta a seguir como usuário com a função `rds_superuser` : `create extension pg_transport;`	DBA

Prepare o ambiente de destino

Tarefa	Descrição	Habilidades necessárias
Modifique o grupo de segurança da origem para permitir conexões na porta da instância de banco de dados da instância Amazon e da EC2 instância de banco de dados de destino	A porta padrão para a instância PostgreSQL é 5432. Se você estiver usando outra porta, as conexões com essa porta devem estar abertas para a EC2 instância.	DBA, administrador de sistemas
Modifique a instância e atribua o novo grupo de parâmetros de origem.	Por exemplo, .`pgsource-param-group`	DBA
Reinicie a origem de banco de dados do Amazon RDS.	Os parâmetros `shared_preload_libraries` e `max_worker_processes`	DBA

Tarefa	Descrição	Habilidades necessárias
	são parâmetros estáticos e exigem a reinicialização da instância.	
Conecte-se ao banco de dados a partir da EC2 instância usando psql.	Use o comando: `psql -h <rds_end_point> -p PORT -U username -d database -W`	DBA
Crie a extensão pg_transport e remova todas as outras extensões dos bancos de dados a serem transportados.	O transporte falhará se houver alguma extensão diferente de pg_transport instalada no banco de dados de origem. Esse comando deve ser executado por um usuário com a função `rds_superuser` .	DBA

Execute o transporte

Tarefa	Descrição	Habilidades necessárias
Execute uma simulação.	Use a função `transport.import_from_server` para executar uma simulação primeiro: `SELECT transport.import_from_server( 'source-db-instance-endpoint', source-db-instance-port, 'source-db-instance-user', 'source-user-password', 'source-`	DBA

Tarefa	Descrição	Habilidades necessárias
	`database-name', 'destination-user-password', 'true');` O último parâmetro dessa função (determinado como `true`) define a operação a seco. Essa função exibe todos os erros que você veria ao executar o transporte principal. Resolva os erros antes de executar o transporte principal.	

Tarefa	Descrição	Habilidades necessárias
Se a execução a seco for bem-sucedida, inicie o transporte do banco de dados.	Execute a função `transport.import_from_server` para realizar o transporte. Ele se conecta à fonte e importa os dados. `SELECT transport .import_from_serve r( 'source-db-instanc e-endpoint', source- db-instance-port, 'source-db-instance- user', 'source-user- password', 'source- database-name', 'destination-user- password', false);` O último parâmetro dessa função (definido como `false`) indica que isso não é um ensaio.	DBA

Tarefa	Descrição	Habilidades necessárias
Execute as etapas pós-transporte.	Depois que o transporte do banco de dados estiver concluído: • Valide os dados no ambiente de destino. • Adicione todas as funções e permissões ao destino. • Ative todas as extensões necessárias no destino e na origem, se necessário. • Reverta o valor do parâmetro `max_worker_processes` .	DBA

Recursos relacionados

- Documentação do Amazon RDS
- documentação pg_transport
- Migração de bancos de dados usando bancos de dados transportáveis PostgreSQL do RDS (postagem do blog)
- Downloads do PostgreSQL
- utilitário psql
- Criação de um parameter group de banco de dados
- Modificar parâmetros em um grupo de parâmetros de banco de dados
- Downloads do PostgreSQL

Redefinir a plataforma

Tópicos

- Exportar um banco de dados do Microsoft SQL Server para o Amazon S3 usando o AWS DMS
- Migre o ML Crie, treine e implante cargas de trabalho para a Amazon SageMaker usando as ferramentas do desenvolvedor da AWS
- Migre OpenText TeamSite cargas de trabalho para a nuvem da AWS
- Migrar valores do Oracle CLOB para linhas individuais no PostgreSQL na AWS
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump Import direto em um link de banco de dados
- Migre o Oracle E-Business Suite para o Amazon RDS Custom
- Migre o Oracle PeopleSoft para o Amazon RDS Custom
- Migre a funcionalidade Oracle ROWID para o PostgreSQL na AWS
- Migre códigos de erro do banco de dados Oracle para um banco de dados compatível com Amazon Aurora PostgreSQL
- Migre cargas de trabalho do Redis para o Redis Enterprise Cloud na AWS
- Migre o SAP ASE na Amazon EC2 para o Amazon Aurora compatível com PostgreSQL usando o AWS SCT e o AWS DMS
- Migrar certificados SSL do Windows para um Application Load Balancer usando o ACM
- Migrar uma fila de mensagens do Microsoft Azure Service Bus para o Amazon SQS
- Migre um banco de dados relacional para o MongoDB Atlas em AWS
- Migre um ambiente MongoDB auto-hospedado para o MongoDB Atlas em AWS
- Migre um banco de dados Oracle JD Edwards EnterpriseOne para a AWS usando o Oracle Data Pump e o AWS DMS
- Migre um PeopleSoft banco de dados Oracle para a AWS usando o AWS DMS
- Migrar um banco de dados MySQL on-premises para o Amazon RDS para MySQL
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server
- Migre dados do Microsoft Azure Blob para o Amazon S3 usando o Rclone
- Migre do Couchbase Server para o Couchbase Capella na AWS
- Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2

- Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2 com o Auto Scaling
- Migre uma aplicação .NET do Microsoft Azure App Service para o AWS Elastic Beanstalk
- Migre do Oracle WebLogic para o Apache Tomcat (TomEE) no Amazon ECS
- Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for Oracle usando o AWS DMS
- Migre um banco de dados Oracle local para o Amazon OpenSearch Service usando o Logstash
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump
- Migre do PostgreSQL na Amazon para o EC2 Amazon RDS for PostgreSQL usando pglogical
- Migrar um banco de dados PostgreSQL on-premises para o Aurora PostgreSQL
- Migre um banco de dados local do Microsoft SQL Server para o Microsoft SQL Server na Amazon executando Linux EC2
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando servidores vinculados
- Saiba como migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando backup e restauração nativos.
- Migre um banco de dados Microsoft SQL Server para o Aurora MySQL usando o AWS DMS e o AWS SCT
- Migre um banco de dados MariaDB on-premises para o Amazon RDS para MariaDB usando ferramentas nativas
- Migrar um banco de dados MySQL on-premises para o Aurora MySQL
- Migre bancos de dados MySQL locais para o Aurora MySQL usando XtraBackup Percona, Amazon EFS e Amazon S3
- Migrar aplicações Java on-premises para a AWS usando o App2Container da AWS
- Migrar sistemas de arquivos compartilhados em uma grande migração da AWS
- Migre um banco de dados Oracle para o Amazon RDS for Oracle usando adaptadores de arquivo simples GoldenGate Oracle
- Altere os aplicativos Python e Perl para oferecer suporte à migração do banco de dados do Microsoft SQL Server para o Amazon Aurora Edição Compatível com PostgreSQL

- Transmita dados do IBM Db2, SAP, Sybase e outros bancos de dados para o MongoDB Atlas em AWS

Exportar um banco de dados do Microsoft SQL Server para o Amazon S3 usando o AWS DMS

Criado por Sweta Krishna (AWS)

Resumo

Muitas vezes, as organizações precisam copiar bancos de dados para o Amazon Simple Storage Service (Amazon S3) para migração de banco de dados, backup e restauração, arquivamento de dados e análise de dados. Esse padrão descreve como você pode exportar um banco de dados Microsoft SQL Server para o Amazon S3. O banco de dados de origem pode ser hospedado localmente ou no Amazon Elastic Compute Cloud (Amazon EC2) ou no Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server na Amazon Web Services (AWS) Cloud.

Os dados são exportados usando o AWS Database Migration Service (AWS DMS). Por padrão, o AWS DMS grava dados completos de captura de dados de alteração e carga (CDC) no formato de valores separados por vírgula (.csv). Para um armazenamento mais compacto e opções de consulta mais rápidas, esse padrão usa a opção de formato Apache Parquet (.parquet).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um perfil do AWS Identity and Access Management (IAM) para a conta com acesso de gravação, exclusão e tag ao bucket do S3 de destino, e o AWS DMS (`dms.amazonaws.com`) adicionado como uma entidade confiável a esse perfil do IAM
- Um banco de dados Microsoft SQL Server local (ou Microsoft SQL Server em uma EC2 instância ou um banco de dados Amazon RDS for SQL Server)
- Conectividade de rede entre a nuvem privada virtual (VPC) na AWS e a rede on-premises fornecida pelo AWS Direct Connect ou uma rede privada virtual (VPN)

Limitações

- Atualmente, um bucket do S3 habilitado para VPC (gateway VPC) não é compatível com as versões do AWS DMS anteriores à 3.4.7.
- As alterações na estrutura da tabela de origem durante a carga máxima não são compatíveis.

- O modo completo do Large Binary Object (LOB) do AWS DMS não é compatível.

Versões do produto

- Versões do Microsoft SQL Server 2005 ou superior para as edições Enterprise, Standard, Workgroup e Developer.
- O suporte para o Microsoft SQL Server versão 2019 como origem está disponível no AWS DMS versões 3.3.2 e posterior.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Microsoft SQL Server local (ou Microsoft SQL Server em uma EC2 instância ou um banco de dados Amazon RDS for SQL Server)

Pilha de tecnologias de destino

- AWS Direct Connect
- AWS DMS
- Amazon S3

Arquitetura de destino

Ferramentas

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O AWS Direct Connect vincula a rede interna a um local do Direct Connect por meio de um cabo de fibra ótica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para serviços públicos da AWS, ignorando provedores de serviço da internet no caminho da sua rede.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Validar a versão do banco de dados.	Valide a versão do banco de dados de origem e certifique-se de que ela seja compatível com o AWS DMS. Para obter informações sobre as versões compatíveis do banco de dados do SQL Server, consulte Usar um banco de dados do Microsoft SQL Server como fonte para o AWS DMS.	DBA
Criar um grupo de segurança e de VPC.	Na sua conta da AWS, crie uma VPC e um grupo de segurança. Para obter mais informações, consulte a documentação da Amazon VPC.	Administrador de sistema
Criar um usuário para a tarefa do AWS DMS.	Crie um usuário do AWS DMS no banco de dados de origem e conceda a ele permissões READ. Esse usuário será usado pelo AWS DMS.	DBA
Testar a conectividade do banco de dados.	Teste a conectividade do usuário do AWS DMS com a instância de banco de dados do SQL Server.	DBA

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Crie o bucket do S3 de destino. Esse bucket conterá os dados da tabela migrada.	Administrador de sistemas
Criar uma política e um perfil do IAM.	1. Para criar uma política do IAM com permissões de bucket, use o código na seção Informações adicionais. 2. Crie uma função para o AWS DMS e anexe a política a ele.	Administrador de sistemas

Migrar dados usando o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Criar uma instância de replicação do AWS DMS.	Faça login no console de gerenciamento da AWS e abra o console do AWS DMS. No painel de navegação, escolha Instâncias de replicação, Criar instância de replicação. Para obter instruções, consulte a etapa 1 na documentação do AWS DMS.	DBA
Criar endpoints de origem e de destino.	Criar endpoints de origem e de destino. Teste a conexão da instância de replicação aos endpoints de origem e de destino. Para obter instruções, consulte a etapa 2 na documentação do AWS DMS.	DBA

Tarefa	Descrição	Habilidades necessárias
Criar uma tarefa de replicaçã o.	Crie uma tarefa de replicaçã o e selecione carga total ou carga total com captura de dados de alteração (CDC) para migrar dados do SQL Server para o bucket do S3. Para obter instruçõe s, consulte a etapa 3 na documentação do AWS DMS.	DBA
Iniciar a replicação dos dados.	Inicie a tarefa de replicação e monitore os logs em busca de erros.	DBA

Validar os dados

Tarefa	Descrição	Habilidades necessárias
Validar os dados migrados.	No console, navegue até o seu bucket do S3 de destino. Abra a subpasta com nome idêntico ao do banco de dados de origem. Confirme se a pasta contém todas as tabelas que foram migradas do banco de dados de origem.	DBA

Limpar recursos

Tarefa	Descrição	Habilidades necessárias
Encerrar e excluir os recursos temporários da AWS.	Encerre os recursos temporári os da AWS que você criou para a migração de dados,	DBA

Tarefa	Descrição	Habilidades necessárias
	como a instância de replicação do AWS DMS, e exclua-os depois de validar a exportação.	

Recursos relacionados

- Guia do usuário do AWS Database Migration Service
- Usar um banco de dados do Microsoft SQL Server como origem para o DMS
- Usar o Amazon S3 como destino para o AWS Database Migration Service
- Usar um bucket do S3 como destino do AWS DMS (AWS ref: Post)

Mais informações

Use o código a seguir para adicionar uma política do IAM com permissões de bucket do S3 para a função do AWS DMS. Substitua `bucketname` pelo nome do seu bucket.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "s3:PutObject",
                 "s3:DeleteObject"
             ],
             "Resource": [
                 "arn:aws:s3:::bucketname*"
             ]
         },
         {
             "Effect": "Allow",
             "Action": [
                 "s3:ListBucket"
             ],
             "Resource": [
                 "arn:aws:s3:::bucketname*"
             ]
```

```
        }
    ]
}
```

Migre o ML Crie, treine e implante cargas de trabalho para a Amazon SageMaker usando as ferramentas do desenvolvedor da AWS

Criado por Mustafa Waheed (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão fornece orientação para migrar um aplicativo de aprendizado de máquina (ML) local executado em servidores Unix ou Linux para ser treinado e implantado na AWS usando a Amazon. SageMaker Esta implantação usa um pipeline de integração contínua e implantação contínua (Pipeline de CI/CD). O padrão de migração é implantado usando uma CloudFormation pilha da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa que usa a Zona de Pouso da AWS
- AWS Command Line Interface (AWS CLI), instalado e configurado em seu servidor Unix ou Linux
- Um repositório de código-fonte de ML provisionado na AWS CodeCommit

Limitações

- Somente 300 pipelines individuais podem ser implantados em uma região da AWS.
- Esse padrão é destinado a cargas de trabalho de ML supervisionadas com train-and-deploy código em Python.

Versões do produto

- Docker versão 19.03.5, criação 633a0ea, usando Python 3.6x

Arquitetura

Pilha de tecnologia de origem

- Instância de computação Linux on-premises com dados no sistema de arquivos local ou em um banco de dados relacional

Arquitetura de origem

Pilha de tecnologias de destino

- A AWS foi CodePipeline implantada com o Amazon S3 para armazenamento de dados e o Amazon DynamoDB como armazenamento de metadados para rastrear ou registrar execuções de pipelines

Arquitetura de destino

Arquitetura de migração de aplicativos

- Pacote Python nativo e CodeCommit repositório AWS (e um cliente SQL, para conjuntos de dados locais na instância do banco de dados)

Ferramentas

- Python3
- Git
- AWS CLI — A AWS CLI implanta a CloudFormation pilha da AWS e move os dados para o bucket do S3. O bucket do S3, por sua vez, leva ao destino.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Validar o código-fonte e os conjuntos de dados.		Cientista de dados
Identificar os tamanhos e tipos de instâncias de criação, treinamento e implantação de destino.		Engenheiro de dados, cientista de dados
Criar uma lista de capacidade e requisitos de capacidade.		
Identificar os requisitos de rede.		DBA, administrador de sistemas
Identificar os requisitos de segurança do acesso à rede ou host para os aplicativos de origem e de destino.		Engenheiro de dados, engenheiro de ML, administrador de sistemas
Determine a estratégia de backup.		Engenheiro de ML, administrador de sistemas
Determinar os requisitos de disponibilidade.		Engenheiro de ML, administrador de sistemas
Identificar a estratégia de transição ou migração de aplicativos.		Cientista de dados, engenheiro de ML

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).		Engenheiro de ML, administrador de sistemas
Criar grupos de segurança.		Engenheiro de ML, administrador de sistemas
Configure um bucket do Amazon S3 e ramificações de CodeCommit repositório da AWS para código de ML.		Engenheiro de ML

Faça o upload dos dados e do código

Tarefa	Descrição	Habilidades necessárias
Use ferramentas nativas do MySQL ou ferramentas de terceiros para migrar, treinar, validar e testar conjuntos de dados para o bucket do S3 provisionado.	Isso é necessário para a implantação do AWS CloudFormation Stack.	Engenheiro de dados, engenheiro de ML
Empacote o treinamento de ML e o código de hospedagem como pacotes Python e envie para o repositório provisionado na AWS ou. CodeCommit GitHub	Você precisa do nome da filial do repositório para implantar o CloudFormation modelo da AWS para migração.	Cientista de dados, engenheiro de ML

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Seguir a estratégia de migração da workload de ML.		Proprietário do aplicativo, engenheiro de ML
Implante a CloudFormation pilha da AWS.	Usar a AWS CLI para criar a pilha declarada no modelo YAML fornecido com essa solução.	Cientista de dados, engenheiro de ML

Substituir

Tarefa	Descrição	Habilidades necessárias
Mudar os clientes do aplicativo para a nova infraestrutura.		Proprietário do aplicativo, cientista de dados, engenheiro de ML

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.	Encerre todos os recursos personalizados do CloudFormation modelo da AWS (por exemplo, qualquer função do AWS Lambda que não esteja sendo usada).	Cientista de dados, engenheiro de ML
Revise e valide os documentos do projeto.		Proprietário do aplicativo, cientista de dados
Validar os resultados e as métricas de avaliação	Certifique-se de que a performance do modelo	Proprietário do aplicativo, cientista de dados

Tarefa	Descrição	Habilidades necessárias
do modelo de ML com os operadores.	corresponda às expectativas dos usuários do aplicativo e seja comparável ao estado on-premises.	
Feche o projeto e forneça feedback.		Proprietário do aplicativo, engenheiro de ML

Recursos relacionados

- AWSCodePipeline
- AWS CodeCommit
- AWSCodeBuild
- AmazonSageMaker
- Amazon S3
- Amazon DynamoDB
- AWS Lambda

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre OpenText TeamSite cargas de trabalho para a nuvem da AWS

Criado por Battulga Purevragchaa (AWS), Michael Stewart e Carlos Marruenda Molina

Resumo

> **Warning**
>
> Este cenário precisa de usuários do IAM com acesso programático e credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessári as para realizar a tarefa e que você os remova quando não forem mais necessários. As chaves de acesso podem ser atualizadas, se necessário. Para obter mais informações, consulte Atualização de chaves de acesso no guia do usuário do IAM.

Muitas instâncias da OpenText Experience Platform são hospedadas localmente ou em soluções de hospedagem tradicionais com capacidade fixa e modelos de custo legados. A migração das cargas de trabalho da OpenText Experience Platform para a nuvem da Amazon Web Services (AWS) fornece recursos e valor adicionais ao aumentar a agilidade comercial e as oportunidades de integração, além de reduzir o custo geral de propriedade.

Esse padrão fornece etapas e um modelo para migrar OpenText TeamSitecargas de trabalho para a nuvem da AWS. O padrão ajuda você a entender como definir o escopo e o orçamento de seus projetos de migração, fornecendo uma seção detalhada de Epics que orienta você em um processo de OpenText TeamSite migração.

Esse padrão foi desenvolvido pela AWS e pela TBSCG, uma parceira da AWS, e acompanha o guia de cargas de trabalho de migração OpenText TeamSite e gerenciamento de mídia para a nuvem da AWS no site AWS Prescriptive Guidance.

Pré-requisitos e limitações

Pré-requisitos

- Pelo menos uma conta da AWS
- Uma OpenText carga de trabalho hospedada em um data center local ou em outro provedor de nuvem

- OpenText Licenças ativas

O processo de migração também exige as funções e a responsabilidades descritas na tabela a seguir.

Função	Responsabilidades
Patrocinador	Patrocínio interno
Gerente de entrega	Entrega de migração
Arquiteto da solução	Definir a arquitetura atual e a nova
DevOps engenheiro	DevOps atividades
Testador de controle de qualidade	Testar em nível de sistema
Proprietário do produto	Priorizar tarefas com base nos requisitos de negócios
TeamSite autores	Teste de aceitação do usuário (UAT) da migração
TeamSite administrador	UAT da migração
OpenText liderar	OpenText especialista em produtos
OpenText desenvolvedor	OpenText especialista em produtos
Especialista em preços	AWS e OpenText licenciamento
Segurança de TI	Linha de base de segurança de TI
Desenvolvedor de integração de terceiros	Reformular as integrações existentes
Desenvolvedor de frontend	Fazer alterações no código de frontend migrado
Administrador de banco de dados	Configurar o banco de dados:

Limitações

- Garanta a compatibilidade com seus sistemas operacionais de destino (OSs). Você pode usar a matriz de compatibilidade das notas de lançamento do produto da versão do OpenText produto que você está migrando.

Arquitetura

Pilha de tecnologia de origem

- OpenText soluções de experiência do cliente hospedadas localmente ou em outro provedor de nuvem:
  - OpenText TeamSite
  - OpenText LiveSite
  - OpenText Gerenciamento de mídia
  - OpenText MediaBin

Pilha de tecnologias de destino

- Uma plataforma de experiência OpenText do cliente hospedada na nuvem da AWS e que usa os seguintes serviços da AWS:
  - Nuvem de computação elástica da Amazon (Amazon EC2)
  - Amazon Elastic Container Service (Amazon ECS)
  - OpenSearch Serviço Amazon
  - Elastic Load Balancing
  - AWS Lambda
  - Amazon API Gateway
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon Elastic Block Store (Amazon EBS)
  - Amazon Simple Storage Service (Amazon S3)

Arquitetura de destino

Ferramentas

- O AWS Database Migration Service (AWS DMS) é um serviço em nuvem que facilita a migração de bancos de dados relacionais, data warehouses, bancos de dados NoSQL e outros tipos de armazenamentos de dados.
- O AWS Application Migration Service automatiza a conversão de seus servidores de origem para execução nativa na AWS. Também simplifica a modernização de aplicativos com opções de otimização incorporadas e personalizadas.

Épicos

Descoberta e avaliação

Tarefa	Descrição	Habilidades necessárias
Realizar workshops sobre os requisitos de descoberta.	Realize workshops com equipes técnicas e comerciais para descobrir o cenário atual, reunir requisitos e validar a estratégia de migração. Dependendo da complexidade e do escopo da sua migração, sua organização pode precisar de vários workshops. Duração: duas semanas	Patrocinador (opcional), gerente de entrega, arquiteto de soluções, OpenText líder, proprietário do produto
Analisar os requisitos de solução e migração.	Analise e documente os requisitos comerciais, funcionais e técnicos que influenciam o projeto da solução planejada e o processo de migração. Duração: uma semana	Arquiteto de soluções, OpenText líder, proprietário do produto

Tarefa	Descrição	Habilidades necessárias
Documente sua OpenText arquitetura existente.	Documente sua OpenText arquitetura existente, incluindo os principais componentes e todos os aplicativos e serviços relacionados. Duração: uma semana	Arquiteto de soluções, OpenText líder, proprietário do produto
Definir a arquitetura planejada da AWS.	Defina sua arquitetura planejada da AWS com base nos componentes e requisitos identificados e usando a matriz de OpenText compatibilidade. Você pode encontrar a matriz de OpenText compatibilidade nas notas de lançamento da sua OpenText TeamSite versão. Duração: uma semana	Arquiteto de soluções, OpenText líder, proprietário do produto, segurança de TI
Avaliar o tamanho da arquitetura planejada da AWS.	Os requisitos de tamanho variam para diferentes componentes arquitetônicos, dependendo da workload e de outros requisitos não funcionais. Duração: dois dias	Arquiteto de soluções, OpenText líder
Calcular o TCO.	Calcule o custo total de propriedade (TCO) da solução proposta. Duração: dois dias	Arquiteto de soluções, especialista em preços

Tarefa	Descrição	Habilidades necessárias
Definir a estratégia de migração para cada componente.	Defina e documente quais das sete estratégias comuns de migração (7 Rs) usar para cada componente principal ou adicional que deve ser migrado para a Nuvem AWS. Duração: uma semana	Arquiteto de soluções, OpenText líder, proprietário do produto
Definir o processo de migração dos componentes.	Defina o processo detalhado de migração para cada um dos componentes da sua workload. Duração: uma semana	Arquiteto de soluções, OpenText líder, proprietário do produto, segurança de TI
Definir o processo de migração global e as dependências.	Crie um processo de migração global e um calendário que inclua os detalhes da migração para componentes, dependências e continuidade dos negócios. Duração: três dias	Arquiteto de soluções, OpenText líder, proprietário do produto, segurança de TI

Atividades de segurança e compatibilidade

Tarefa	Descrição	Habilidades necessárias
Criar políticas de segurança.	Configure as políticas de segurança gerenciadas pelo cliente em suas contas da AWS. Isso deve incluir complexidade e rotação de senhas, além de desabilitar	Arquiteto da solução

Tarefa	Descrição	Habilidades necessárias
	automaticamente contas não utilizadas. Para obter mais informaçõ es sobre políticas gerenciad as pelo cliente, consulte Políticas gerenciadas pelo cliente na documentação do AWS Identity and Access Management (IAM).	
Criar usuários do IAM.	Crie os usuários do IAM que precisam de acesso ao Console de Gerenciamento da AWS, à AWS Command Line Interface (AWS CLI) e ao AWS SDKs. Para obter mais informaçõ es sobre como criar usuários do IAM, consulte Criar um usuário do IAM na sua conta da AWS na documentação do IAM.	Arquiteto da solução

Tarefa	Descrição	Habilidades necessárias
Criar grupo do IAM.	Crie os grupos de usuários do IAM necessários (por exemplo, grupos de administradores ou desenvolvedores) e adicione usuários do IAM a esses grupos. Para obter mais informações sobre grupo de usuários do IAM, consulte Grupos de usuários do IAM na documentação do IAM.	Arquiteto da solução
Anexar políticas de segurança.	Anexe políticas de segurança aos grupos ou perfis do IAM. Para obter mais informações, consulte Anexar uma política a um grupo de usuários do IAM na documentação do IAM.	Arquiteto da solução
Habilitar o faturamento detalhado.	Para obter mais informações sobre o faturamento, consulte Monitoramento de seu uso e custos na documentação do Gerenciamento de Faturamento e Custos da AWS.	Arquiteto da solução

Tarefa	Descrição	Habilidades necessárias
Verificar os detalhes de contato de suas contas.	Certifique-se de que os detalhes de contato de suas contas estejam atualizados e mapeados para mais de uma pessoa em sua organização. Para obter mais informações, consulte Gerenciar uma conta da AWS na documentação do Gerenciamento de Faturamento e Custos da AWS.	Arquiteto de soluções, proprietário do produto
Adicionar informações de contato de segurança.	Configure suas informações de contato com suas informações de contato de segurança. Para obter mais informações, consulte Gerenciar uma conta da AWS na documentação do Gerenciamento de Faturamento e Custos da AWS.	Arquiteto de soluções, segurança de TI
Configure funções do IAM para EC2 instâncias.	Configure as funções do IAM para as EC2 instâncias. Para obter mais informações sobre isso, consulte Funções do IAM para a Amazon EC2 na EC2 documentação da Amazon.	Arquiteto da solução

Tarefa	Descrição	Habilidades necessárias
Configurar o acesso ao AWS Support.	Anexe uma política do IAM aos usuários do IAM que precisam acessar o AWS Support no Support Center e criar casos de suporte. Para obter mais informaçõ es, consulte Permissões de acesso para o AWS Support na documentação do AWS Support.	Arquiteto da solução
Habilitar CloudTrail.	Habilite automaticamente a AWS CloudTrail em todas as suas regiões da AWS. Para obter mais informações sobre isso, consulte Como usar `create-trail` na CloudTrail documentação da AWS.	Arquiteto da solução
Ative a validação do arquivo de CloudTrail log.	Ative a validação dos arquivos de CloudTrail log. Para obter mais informações sobre isso, consulte Habilitar a validação da integridade do arquivo de log CloudTrail na CloudTrail documentação da AWS.	Arquiteto da solução

Tarefa	Descrição	Habilidades necessárias
Restrinja o acesso a qualquer bucket do S3 que contenha CloudTrail registros.	Aplique uma política de bucket restringindo o acesso aos buckets do S3 que contêm CloudTrail arquivos de log. Para obter mais informações sobre isso, consulte a política de bucket do Amazon S3 CloudTrail na documentação da AWS CloudTrail .	Arquiteto da solução
Integre CloudTrail com o CloudWatch Logs	Integre trilhas geradas por CloudTrail com o Amazon CloudWatch Logs. Para obter mais informaçõ es sobre isso, consulte Envio de eventos para CloudWatc h registros na CloudTrail documentação da AWS	Arquiteto da solução
Habilitar o AWS Config em todas as regiões necessárias.	Habilite automaticamente o AWS Config em todas as regiões necessárias. Você pode configurar o AWS Config usando a AWS CLI. Para obter mais informações, consulte Configurar o AWS Config usando a AWS CLI na documentação do AWS Config.	Arquiteto da solução

Tarefa	Descrição	Habilidades necessárias
Habilitar o registro em log de acesso ao bucket do S3.	Automatize o registro de acesso ao bucket do S3 com. CloudTrail Para obter mais informações sobre isso, consulte Habilitando o registro de CloudTrail eventos para buckets e objetos do S3 na documentação do Amazon S3.	Arquiteto da solução
Configure as políticas de chaves do AWS KMS para. CloudTrail	Automatize a configuração das principais políticas do AWS Key Management Service (AWS KMS) para. CloudTrail Para obter mais informações sobre isso, consulte Configurar políticas de chaves do AWS KMS CloudTrail na documentação da AWS CloudTrail .	Arquiteto da solução
Criptografe CloudTrail registros em repouso.	Configure a criptografia de CloudTrail registros no lado do servidor usando chaves gerenciadas pelo cliente mantidas no AWS KMS. Para obter mais informações sobre isso, consulte Criptografar arquivos de CloudTrail log com chaves gerenciadas do AWS KMS (SSE-KMS) na documentação da AWS. CloudTrail	Arquiteto da solução

Tarefa	Descrição	Habilidades necessárias
Fazer automaticamente a rotação das chaves do KMS.	Configure a rotação das chaves do AWS KMS. Para obter mais informaçõ es, consulte Como habilitar e desabilitar a rotação automátic a de chaves na documentação do AWS KMS.	Arquiteto da solução
Configure CloudWatch alarmes.	Configure os CloudWatch alarmes da Amazon que são iniciados por eventos específic os. Por exemplo, solicitações APIs ou uso não autorizados da conta raiz. Para obter mais informaçõ es, consulte Como receber notificações quando as chaves de acesso raiz da sua conta da AWS são usadas no blog de segurança da AWS.	Arquiteto da solução
Configurar grupos de segurança.	Configure grupos de segurança para garantir que o tráfego de entrada irrestrito não seja permitido nas portas 22 e 3389.	Arquiteto da solução

Tarefa	Descrição	Habilidades necessárias
habilitar o registro em log de fluxo da VPC.	Capture o tráfego IP rejeitado de e para interfaces de rede em sua nuvem privada virtual (VPC) e configure CloudWatch para capturá-lo. Para obter mais informações, consulte Criar um log de fluxo na documentação da Amazon VPC.	Arquiteto da solução
Modificar o grupo de segurança padrão para restringir todo o tráfego.	Modifique cada grupo de segurança padrão da VPC para que o tráfego seja negado por padrão e o acesso seja concedido explicitamente por meio de seus grupos de segurança. Para obter mais informações, consulte Grupos de segurança para a VPC na documentação da Amazon VPC.	Arquiteto da solução
Configure tabelas de roteamento entre o. VPCs	Configure as tabelas de rotas para emparelhamento de VPC com o mínimo de acesso necessário. Para obter mais informações, consulte Atualizar as tabelas de rotas para uma conexão de emparelhamento da VPC na documentação da VPC do Amazon.	Arquiteto da solução

Configurar atividades para a nova infraestrutura da AWS

Tarefa	Descrição	Habilidades necessárias
Provisionar a infraestrutura da AWS.	Crie as contas e os recursos da AWS. Duração: duas semanas	DevOps engenheiro, arquiteto de soluções
Configure DevOps ferrament as e processos.	Configure DevOps ferrament as e procedimentos, como pipelines de integração e entrega contínuas (CI/CD) e estruturas de teste automatiz adas.	DevOps engenheiro, arquiteto de soluções
Automatizar a migração dos componentes principais.	Use modelos ou scripts existentes para automatizar a instalação e a configuração de OpenText produtos TeamSite, incluindo LiveSite, OpenDeplo y e. MediaBin Duração: uma semana	DevOps engenheiro, arquiteto de soluções, OpenText líder
Automatizar a migração dos componentes adicionais.	Analise e automatize a migração de aplicativos adicionais integrados aos componentes OpenText principais (por exemplo, bancos de dados adicionais, componentes de comunicaç ão, monitoramento ou cache). Duração: duas semanas	DevOps engenheiro, arquiteto de soluções, OpenText líder
Adaptar os componentes principais.	Faça as alterações necessári as nas personalizações dos componentes OpenText	Arquiteto de soluções, OpenText líder, OpenText desenvolvedor, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	principais (por exemplo, integrações).	de integração terceirizado, desenvolvedor front-end
Implementar e configurar serviços adicionais.	Provisione, configure e implemente quaisquer novos serviços da AWS, como funções do AWS Lambda ou Amazon API Gateway.	DevOps engenheiro, arquiteto de soluções, desenvolvedor de integração terceirizado, desenvolvedor front-end
Migrar ou refatorar outros componentes.	Migre componentes adicionais, incluindo qualquer refatoração necessária. Isso inclui aplicativos externos, como portais de relatórios personalizados ou camadas de integração de API existentes.	DevOps engenheiro, arquiteto de soluções, desenvolvedor de integração terceirizado, desenvolvedor front-end
Realizar a migração no ambiente de desenvolvimento.	Atividades de migração automatizada para o ambiente de desenvolvimento, incluindo provisionamento de sistemas, migração de dados, migração de aplicativos, instalação e configuração.	DevOps engenheiro
Executar a migração no ambiente de produção.	Atividades de migração automatizada para o ambiente de produção, incluindo provisionamento de sistemas, migração de dados, migração de aplicativos, instalação e configuração.	DevOps engenheiro

Atividades de rede

Tarefa	Descrição	Habilidades necessárias
Definir blocos CIDR para cada VPC.	Defina o bloco de Encaminhamento Entre Domínios Sem Classificação (CIDR) (o intervalo e a máscara de IP) para cada VPC não padrão. Duração: menos de uma semana	DevOps engenheiro, arquiteto de soluções
Definir sub-redes e zonas de disponibilidade.	Defina as sub-redes e as zonas de disponibilidade que são usadas em cada VPC não padrão. Duração: menos de uma semana	DevOps engenheiro, arquiteto de soluções
Definir grupos de segurança.	Defina grupos de segurança e regras de grupos de segurança para controlar a segurança nos recursos da AWS. Duração: menos de uma semana	DevOps engenheiro, arquiteto de soluções
Defina a rede ACLs.	Defina as listas de controle de acesso à rede (ACLs) para controlar a segurança nos limites da sub-rede. Duração: menos de uma semana	DevOps engenheiro, arquiteto de soluções

Migrar bancos de dados

Tarefa	Descrição	Habilidades necessárias
Preparar os bancos de dados de origem.	Use o AWS DMS para preparar cada banco de dados de origem para a replicação contínua na Nuvem AWS.	DevOps engenheiro, arquiteto de soluções
Crie os bancos de dados para os componentes OpenText principais.	Crie os bancos de dados exigidos pelo Opentext TeamSite, LiveSite, e MediaBin pelos component es. Certifique-se de que os usuários e os direitos de acesso estejam configurados corretamente de acordo com a documentação OpenText de instalação.	Arquiteto de soluções, OpenText líder, OpenText desenvolvedor
Copiar dados dos servidores de banco de dados de origem.	Automatize o processo de cópia de dados dos componentes OpenText principais do servidor de banco de dados de origem para o servidor de banco de dados de destino.	Arquiteto de soluções, OpenText líder, OpenText desenvolvedor
Sincronizar dados dos servidores de banco de dados.	Automatize o processo de realizar a sincronização regular de dados dos bancos de dados de origem para os bancos de dados de destino.	OpenText desenvolvedor

Atividades de migração de conteúdo

Tarefa	Descrição	Habilidades necessárias
Copie os armazenamentos de OpenText TeamSite conteúdo.	Automatize o processo de cópia dos armazenamentos de conteúdo do servidor de origem para o OpenText TeamSite servidor de destino OpenText TeamSite .	Arquiteto de soluções, OpenText líder, OpenText desenvolvedor
Mapear usuários e grupos.	Mapeamento interno do OpenText TeamSite usuário interno IDs para o sistema de destino IDs.	OpenText liderar
Sincronize os armazenam entos OpenText TeamSite de conteúdo.	Automatize o processo de realizar a sincronização regular dos armazenamentos de conteúdo de origem e destino. Isso é implement ado como parte do processo de migração e controle de qualidade.	OpenText desenvolvedor
Copiar dados de servidores web.	Automatize o processo de cópia de dados dos servidore s web de origem para os servidores web de destino.	Arquiteto de soluções, OpenText líder, OpenText desenvolvedor
Sincronizar os dados do servidor web.	Automatize o processo de realizar a sincronização regular dos dados do servidor web de origem e destino.	OpenText desenvolvedor
Copiar dados do sistema de arquivos do servidor web.	Automatize o processo de cópia de conteúdo e outros ativos da web do sistema de	Arquiteto de soluções, OpenText líder, OpenText desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	arquivos do servidor web de origem para os servidores web de destino.	
Sincronizar os sistemas de arquivos do servidor web.	Automatize o processo de sincronizar regularmente o conteúdo e outros ativos da web do sistema de arquivos do servidor web de origem para os servidores web de destino.	OpenText desenvolvedor
Gerar feeds e índices.	Automatize o processo de execução de qualquer processo que gere feeds ou outros índices (por exemplo, pesquisa na web) que use OpenText TeamSite nosso conteúdo do servidor web como fonte de dados.	Arquiteto de soluções, OpenText líder, OpenText desenvolvedor
Sincronizar a geração de feeds e índices.	Automatize o processo de realizar a regeneração regular de feeds e índices após as sincronizações de dados.	OpenText desenvolvedor

Atividades de teste e controle de qualidade

Tarefa	Descrição	Habilidades necessárias
Executar o controle de qualidade da migração.	Teste o ambiente, os aplicativos e os serviços de destino da AWS para garantir que os processos de migração	DevOps engenheiro, OpenText líder, testador de controle de qualidade

Tarefa	Descrição	Habilidades necessárias
	automatizados sejam criados e configurados corretamente.	
Realizar testes de desempenho.	Teste o desempenho em termos de capacidade de resposta e estabilidade sob uma workload específica. Investigue, meça, valide ou verifique outros atributos de qualidade do sistema de destino, como escalabilidade e confiabilidade. Para que este teste seja útil, você deve ter um ambiente de teste do mesmo tamanho do seu ambiente de produção. Duração: entre uma e duas semanas	DevOps engenheiro, OpenText líder

Tarefa	Descrição	Habilidades necessárias
Realizar testes de segurança.	Análise de vulnerabilidades e testes de penetração para revelar possíveis falhas nos mecanismos de segurança de um aplicativo que protege os dados e mantém a funcional idade conforme necessário. Para que este teste seja útil, você deve ter um ambiente de teste equivalente ao seu ambiente de produção em termos de rede e segurança. Duração: entre uma e duas semanas	DevOps engenheiro, OpenText líder

Realizar atividades de integração operacional

Tarefa	Descrição	Habilidades necessárias
Verificar a prontidão operacion al.	Entenda como você executa atualmente as operações de TI e como você operará na Nuvem AWS. Você pode alcançar esse resultado comercial ao definir um modelo operacional em nuvem. Duração: uma semana	DevOps engenheiro, OpenText líder, gerente de prestação de serviços
Investir na automação de operações.	Invista em automação para fornecer um modelo operacion al da AWS.	DevOps engenheiro, OpenText líder, gerente de prestação de serviços

Tarefa	Descrição	Habilidades necessárias
Integrar as operações.	Continue usando as ferrament as de TI atuais e amplie-as por meio da integração com a Nuvem AWS.	DevOps engenheiro, OpenText líder, gerente de prestação de serviços

Realizar atividades de substituição

Tarefa	Descrição	Habilidades necessárias
Trocar o DNS.	Troque manualmente o sistema de nomes de domínio (DNS) de hosts existente s para hosts baseados na Nuvem AWS. Duração: uma hora	DevOps engenheiro, OpenText líder
Testar a recuperação de desastres.	Teste a recuperação de desastres, a restauração de backup e execute seus testes automatizados. Duração: um dia	DevOps engenheiro, OpenText líder, testador de controle de qualidade
Validar o monitoramento e a análise.	Valide se o monitoramento e a análise estão funcionando. Duração: duas horas	DevOps engenheiro, OpenText líder
Desligar o ambiente antigo e solicitar o desligamento do servidor.	Duração: três dias	DevOps engenheiro, OpenText líder

Recursos relacionados

- Políticas gerenciadas pelo cliente
- Criação de um usuário do IAM; na sua conta da AWS
- Grupos de usuários do IAM
- Anexar uma política a um grupo de usuários do IAM
- Monitorar seu uso e seus custos
- Gerenciar uma conta da AWS
- Funções do IAM para a Amazon EC2
- Permissões de acesso para o AWS Support
- Usar create-trail
- Habilitando a validação da integridade do arquivo de log para CloudTrail
- Política de bucket do Amazon S3 para CloudTrail
- Envio de eventos para o CloudWatch Logs
- Configurar o AWS Config com a CLI da AWS
- Habilitando o registro de CloudTrail eventos para buckets e objetos do S3
- Configure as principais políticas do AWS KMS para CloudTrail
- Criptografando arquivos de CloudTrail log com chaves gerenciadas do AWS KMS (SSE-KMS)
- Como habilitar e desabilitar a rotação de chaves automática
- Como receber notificações quando as chaves de acesso raiz da sua conta da AWS são usadas
- Criar um log de fluxo
- Grupos de segurança para a VPC
- Atualizar as tabelas de rotas para uma conexão de emparelhamento da VPC

Migrar valores do Oracle CLOB para linhas individuais no PostgreSQL na AWS

Criado por Sai Krishna Namburu (AWS) e Sindhusha Paturu (AWS)

Resumo

Este padrão descreve como dividir os valores do Oracle Character Large Object (CLOB) em linhas individuais no Amazon Aurora Edição Compatível com PostgreSQL e no Amazon Relational Database Service (Amazon RDS) para o PostgreSQL. O PostgreSQL não dá suporte ao tipo de dados CLOB.

As tabelas com partições de intervalo são identificadas no banco de dados Oracle de origem, e o nome da tabela, o tipo de partição, o intervalo da partição e outros metadados são capturados e carregados no banco de dados de destino. Você pode carregar dados CLOB com menos de 1 GB em tabelas de destino como texto usando o AWS Database Migration Service (AWS DMS) ou pode exportar os dados no formato CSV, carregá-los em um bucket do Amazon Simple Storage Service (Amazon S3) e migrá-los para o banco de dados PostgreSQL de destino.

Após a migração, você pode usar o código PostgreSQL personalizado fornecido com esse padrão para dividir os dados CLOB em linhas individuais com base no novo identificador de caracteres de linha (`CHR(10)`) e preencher a tabela de destino.

Pré-requisitos e limitações

Pré-requisitos

- Uma tabela de banco de dados Oracle que tem partições de intervalo e registros com um tipo de dados CLOB.
- Um banco de dados compatível com o Aurora PostgreSQL ou Amazon RDS para PostgreSQL que tem uma estrutura de tabela semelhante à tabela de origem (mesmas colunas e tipos de dados).

Limitações

- O valor do CLOB não pode exceder 1 GB.
- Cada linha na tabela de destino deve ter um novo identificador de caractere de linha.

Versões do produto

- Oracle 12c

- Aurora Postgres 11.6

Arquitetura

O diagrama a seguir mostra uma tabela Oracle de origem com dados CLOB e a tabela PostgreSQL equivalente na versão 11.6 compatível com o Aurora PostgreSQL.

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID, que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.
- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.
- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

Você pode usar as seguintes ferramentas de cliente para se conectar, acessar e gerenciar seus bancos de dados compatíveis com o Aurora PostgreSQL e o Amazon RDS para PostgreSQL. (Essas ferramentas não são usadas nesse padrão).

- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.
- DBeaveré uma ferramenta de banco de dados de código aberto para desenvolvedores e administradores de banco de dados. Você pode usar a ferramenta para manipular, monitorar, analisar, administrar e migrar seus dados.

Práticas recomendadas

Para obter as práticas recomendadas para migrar seu banco de dados do Oracle para o PostgreSQL, consulte a Publicação de blog da AWS práticas recomendadas para migrar um banco de dados Oracle para o Amazon RDS PostgreSQL ou o Amazon Aurora PostgreSQL: considerações sobre o processo de migração e a infraestrutura.

Para obter as melhores práticas de configuração da tarefa do AWS DMS para migrar objetos binários grandes, consulte Migração de objetos binários grandes () LOBs na documentação do AWS DMS.

Épicos

Identificar os dados do CLOB

Tarefa	Descrição	Habilidades necessárias
Analisar os dados do CLOB.	No banco de dados Oracle de origem, analise os dados CLOB para ver se eles contêm cabeçalhos de coluna, para que você possa determina r o método para carregar os dados na tabela de destino. Para analisar os dados de entrada, use a consulta a seguir. `SELECT * FROM clobdata_or;`	Desenvolvedor
Carregar os dados do CLOB no banco de dados de destino.	Migre a tabela que tem dados CLOB para uma tabela provisória (de teste) no banco de dados de destino do Aurora ou do Amazon RDS. Você pode usar o AWS DMS ou carregar os dados como um	Engenheiro de migração, DBA

Tarefa	Descrição	Habilidades necessárias
	arquivo CSV em um bucket do Amazon S3. Para obter informações sobre o uso do AWS DMS para essa tarefa, consulte Usar um banco de dados Oracle como fonte e Usar um banco de dados PostgreSQL como destino na documentação do AWS DMS. Para obter informações sobre o uso do Amazon S3 para essa tarefa, consulte Usar o Amazon S3 como destino na documentação do AWS DMS.	

Validar a tabela PostgreSQL de destino.	Valide os dados de destino, incluindo cabeçalhos, em relação aos dados de origem usando as seguintes consultas no banco de dados de destino.
	
	`SELECT * FROM clobdata_pg;`
	`SELECT * FROM clobdatatarget;`
	
	Compare os resultados com os resultados da consulta do banco de dados de origem (da primeira etapa).
		Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Dividir os dados do CLOB em linhas separadas.	Execute o código PostgreSQL personalizado fornecido na seção Informações adicionais para dividir os dados CLOB e inseri-los em linhas separadas na tabela PostgreSQL de destino.	Desenvolvedor

Valide os dados.

Tarefa	Descrição	Habilidades necessárias

Validar os dados na tabela de destino.	Valide os dados inseridos na tabela de destino usando as seguintes consultas.
	`SELECT * FROM clobdata_pg;`
	`SELECT * FROM clobdatatarget;`
		Desenvolvedor

Recursos relacionados

- Tipo de dados CLOB (documentação da Oracle)
- Tipos de dados (documentação do PostgreSQL)

Mais informações

Função PostgreSQL para dividir dados CLOB

```
do
$$
declare
totalstr varchar;
```

```
str1 varchar;
str2 varchar;
pos1 integer := 1;
pos2 integer ;
len integer;


begin
        select rawdata||chr(10) into totalstr from clobdata_pg;
        len :=  length(totalstr) ;
        raise notice 'Total length : %',len;
        raise notice 'totalstr : %',totalstr;
        raise notice 'Before while loop';


        while pos1 < len  loop


                  select position (chr(10) in totalstr) into pos2;
                 raise notice '1st position of new line : %',pos2;


                str1 := substring (totalstr,pos1,pos2-1);
                raise notice 'str1 : %',str1;


                   insert into clobdatatarget(data) values (str1);
                   totalstr := substring(totalstr,pos2+1,len);
                   raise notice 'new totalstr :%',totalstr;
                len :=  length(totalstr) ;


        end loop;
end
$$
LANGUAGE 'plpgsql' ;
```

Exemplos de entrada e saída

Você pode usar os exemplos a seguir para testar o código PostgreSQL antes de migrar seus dados.

Crie um banco de dados Oracle com três linhas de entrada.

```
CREATE TABLE clobdata_or (
```

```
id INTEGER GENERATED ALWAYS AS IDENTITY,
rawdata clob  );


insert into clobdata_or(rawdata) values (to_clob('test line 1') || chr(10) ||
 to_clob('test line 2') || chr(10) || to_clob('test line 3') || chr(10));
COMMIT;


SELECT * FROM clobdata_or;
```

Ele exibe a seguinte saída.

id	dados brutos
1	linha de teste 1 linha de teste 2 linha de teste 3

Carregue os dados de origem em uma tabela de preparação do PostgreSQL (`clobdata_pg`) para processamento.

```
SELECT * FROM clobdata_pg;

CREATE TEMP TABLE clobdatatarget (id1 SERIAL,data VARCHAR );

<Run the code in the additional information section.>

SELECT * FROM clobdatatarget;
```

Ele exibe a seguinte saída.

id1	dados
1	linha de teste 1
2	linha de teste 2
3	linha de teste 3

Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump Import direto em um link de banco de dados

Criado por Rizwan Wangde (AWS)

Resumo

Vários padrões abrangem a migração de bancos de dados Oracle locais para o Amazon Relational Database Service (Amazon RDS) for Oracle usando o Oracle Data Pump, um utilitário nativo da Oracle que é a forma preferida de migrar grandes cargas de trabalho da Oracle. Esses padrões geralmente envolvem a exportação de esquemas ou tabelas de aplicativos em arquivos de despejo, a transferência dos arquivos de despejo para um diretório de banco de dados no Amazon RDS para Oracle e, em seguida, a importação dos esquemas e dados do aplicativo dos arquivos de despejo.

Ao usar essa abordagem, a migração pode levar mais tempo, dependendo do tamanho dos dados e do tempo necessário para transferir os arquivos de despejo para a instância do Amazon RDS. Além disso, os arquivos de despejo residem no volume Amazon Elastic Block Store (Amazon EBS) da instância do Amazon RDS, que deve ser grande o suficiente para o banco de dados e os arquivos de despejo. Quando os arquivos de despejo são excluídos após a importação, o espaço vazio não pode ser recuperado, então você continua pagando pelo espaço não utilizado.

Esse padrão atenua esses problemas executando uma importação direta na instância do Amazon RDS usando a API do Oracle Data Pump (`DBMS_DATAPUMP`) em um link de banco de dados. O padrão inicia um pipeline simultâneo de exportação e importação entre os bancos de dados de origem e de destino. Este padrão não exige o dimensionamento de um volume do EBS para os arquivos de despejo porque nenhum arquivo de despejo é criado ou armazenado no volume. Essa abordagem economiza o custo mensal do espaço em disco não utilizado.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa da Amazon Web Services (AWS).
- Uma nuvem privada virtual (VPC) configurada com sub-redes privadas em pelo menos duas zonas de disponibilidade, para fornecer a infraestrutura de rede para a instância do Amazon RDS.
- Um banco de dados Oracle em um data center local ou autogerenciado no Amazon Elastic Compute Cloud (Amazon). EC2

- Uma instância existente do Amazon RDS for Oracle em uma única zona de disponibilidade. Usar uma única zona de disponibilidade melhora o desempenho de gravação durante a migração. Uma implantação Multi-AZ pode ser habilitada de 24 a 48 horas antes da substituição.

  Essa solução também pode usar o Amazon RDS Custom for Oracle como destino.
- AWS Direct Connect (recomendado para bancos de dados de grande porte).
- Regras de conectividade de rede e firewall no on-premises configuradas para permitir uma conexão de entrada da instância do Amazon RDS com o banco de dados Oracle on-premises.

Limitações

- O limite de tamanho do banco de dados no Amazon RDS for Oracle é de 64 tebibytes (TiB) em dezembro de 2022.
- O tamanho máximo de um único arquivo em uma instância de banco de dados Amazon RDS for Oracle é de 16 TiB. É importante saber isso porque talvez seja necessário distribuir tabelas em vários espaços de tabela.

Versões do produto

- Banco de dados de origem: Banco de dados Oracle versão 10g Release 1 e posterior.
- Banco de dados de destino: para obter uma lista de versionamentos e edições compatíveis no Amazon RDS, consulte Amazon RDS para Oracle na documentação da AWS.

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Oracle autogerenciado on-premises ou na nuvem

Pilha de tecnologias de destino

- Amazon RDS para Oracle ou Amazon RDS Custom para Oracle

Arquitetura de destino

O diagrama a seguir mostra a arquitetura para migrar de um banco de dados Oracle on-premises para o Amazon RDS para Oracle em um ambiente single-AZ. As direções das setas mostram o fluxo de dados na arquitetura. O diagrama não mostra qual componente está iniciando a conexão.

1. A instância do Amazon RDS para Oracle se conecta ao banco de dados Oracle de origem on-premises para realizar uma migração de carga completa pelo link do banco de dados.
2. AWS Database Migration Service (AWS DMS) se conecta ao banco de dados Oracle de origem local para realizar a replicação contínua usando a captura de dados de alteração (CDC).
3. As alterações do CDC são aplicadas ao banco de dados do Amazon RDS para Oracle.

Ferramentas

Serviços da AWS

- AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para Nuvem AWS ou entre combinações de configurações na nuvem e no local. Esse padrão usa CDC e a configuração Replicar somente alterações de dados.
- AWS Direct Connectconecta sua rede interna a um AWS Direct Connect local por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para o público, Serviços da AWS ignorando os provedores de serviços de Internet em seu caminho de rede.
- O Amazon Relational Database Service ajuda você a configurar, operar e escalar um banco de dados relacional Oracle na nuvem da AWS.

Outras ferramentas

- O Oracle Data Pump ajuda você a mover dados e metadados de um banco de dados para outro em alta velocidade.
- Ferramentas de cliente, como Oracle Instant Client ou SQL Developer, são usadas para conectar e executar consultas SQL no banco de dados.

Práticas recomendadas

Embora AWS Direct Connect use conexões de rede privadas dedicadas entre a rede local e AWS, considere as seguintes opções para segurança adicional e criptografia de dados para dados em trânsito:

- Uma rede privada virtual (VPN) usando AWS Site-to-Site VPN ou uma conexão IPsec VPN da rede local para a AWS rede
- Criptografia de rede nativa do banco de dados Oracle configurada no banco de dados Oracle on-premises
- Criptografia usando TLS

Épicos

Preparar o banco de dados Oracle de origem on-premises

Tarefa	Descrição	Habilidades necessárias
Configurar a conectividade de rede entre o banco de dados de destino e o banco de dados de origem.	Configure a rede e o firewall on-premises para permitir a conexão de entrada da instância de destino do Amazon RDS com o banco de dados Oracle de origem on-premises.	Administrador de rede, engenheiro de segurança

Criar um usuário do banco de dados com os privilégios apropriados.	Crie um usuário de banco de dados no banco de dados Oracle de origem local com privilégios para migrar dados entre a origem e o destino usando o Oracle Data Pump:
	`GRANT CONNECT to <migration_user>;`
	`GRANT DATAPUMP_EXP_FULL_DATABASE to <migration_user>;`
		DBA

Tarefa	Descrição	Habilidades necessárias
	`GRANT SELECT ANY TABLE to <migration_user>;`	

Prepare o banco de dados de origem local para a migração do AWS DMS CDC.	(Opcional) Prepare o banco de dados Oracle de origem local para a migração do AWS DMS CDC após a conclusão do Oracle Data Pump Full Load:
	1. Configure os privilégios adicionais necessários para gerenciar o FLASHBACK durante a migração do Oracle Data Pump:
	`GRANT FLASHBACK ANY TABLE to <migration_user>;`
	`GRANT FLASHBACK ARCHIVE ADMINISTER to <migration_user>;`
	2. Para configurar os privilégios de conta de usuário necessários em uma fonte Oracle autogerenciada para AWS DMS, consulte a AWS DMS documentação.
	3. Para preparar um banco de dados de origem autogerenciado Oracle para uso do CDC AWS DMS, consulte a AWS DMS documentação.
		DBA

Tarefa	Descrição	Habilidades necessárias
Instalar e configure o SQL Developer.	Instale e configure o SQL Developer para conectar e executar consultas SQL nos bancos de dados de origem e destino.	DBA, Engenheiro de migração
Gerar um script para criar os espaços de tabela.	Use o exemplo de consulta SQL a seguir para gerar o script no banco de dados de origem: `SELECT 'CREATE TABLESPACE ' tablespace_name ' DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE UNLIMITED;' from dba_tablespaces where tablespace_name not in ('SYSTEM', 'SYSAUX','TEMP','UNDOTBS1') order by 1;` O script será aplicado no banco de dados de destino.	DBA

Tarefa	Descrição	Habilidades necessárias
Gerar um script para criar usuários, perfis, funções e privilégios.	Para gerar um script para criar usuários, perfis, funções e privilégios do banco de dados, use os scripts do documento do Oracle Support Como extrair DDL para o usuário, incluindo privilégios e perfis, usando dbms_metadata.get_ddl (Doc ID 2739952.1) (é necessária uma conta Oracle). O script será aplicado no banco de dados de destino.	DBA

Prepare a instância de destino do Amazon RDS para Oracle

Tarefa	Descrição	Habilidades necessárias
Criar um link de banco de dados com o banco de dados de origem e verificar a conectividade.	Para criar um link de banco de dados para o banco de dados de origem local, você pode usar o seguinte exemplo de comando: `CREATE DATABASE LINK link2src CONNECT TO <migration_user_account> IDENTIFIED BY <password> USING '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<dns or ip address of remote db>)`	DBA

Tarefa	Descrição	Habilidades necessárias

	`(PORT=<li stener port>))(C ONNECT_DATA=(SID=< remote SID>)))';`
	
	Para verificar a conectividade, execute o seguinte comando SQL:
	
	`select * from dual@link 2src;`
	
	A conectividade será bem-sucedida se a resposta for X.	

Executar os scripts para preparar a instância de destino.	Executar os scripts gerados anteriormente para preparar a instância de destino do Amazon RDS para Oracle: 1. Tablespaces 2. Perfis 3. Perfis Isso ajuda a garantir que a migração do Oracle Data Pump possa criar os esquemas e respectivos objetos.	DBA, Engenheiro de migração

Executar uma migração de carga completa usando o Oracle Data Pump Import em um link de banco de dados

Tarefa	Descrição	Habilidades necessárias
Migrar os esquemas necessários.	Para migrar os esquemas necessários do banco de dados on-premises de origem para a instância de destino do Amazon RDS, use o código na seção Informações adicionais: • Para migrar um único esquema, execute o Código 1 na seção Informações adicionais. • Para migrar um único esquema, execute o Código 2 na seção Informações adicionais. Para ajustar o desempenho da migração, você pode ajustar o número de processos paralelos executando o seguinte comando: `DBMS_DATAPUMP.SET_ PARALLEL (handle => v_hdnl, degree => 4);`	DBA
Coletar estatísticas do esquema para melhorar o desempenho.	O comando Coletar estatísticas do esquema retorna as estatísticas do otimizador de consultas Oracle coletadas para objetos de banco de dados. Usando essas	DBA

Tarefa	Descrição	Habilidades necessárias
	informações, o otimizado r pode selecionar o melhor plano de execução para qualquer consulta com esses objetos: `EXECUTE DBMS_STAT S.GATHER_SCHEMA_ST ATS(ownname => '<schema_name>');`	

Execute uma migração de carga completa e uma replicação de CDC usando o Oracle Data Pump e AWS DMS

Tarefa	Descrição	Habilidades necessárias
Capturar o SCN no banco de dados Oracle on-premises de origem.	Capturar o número de alteração do sistema (SCN) no banco de dados Oracle on-premises de origem. Você usará o SCN para importaçã o de carga total e como ponto de partida para a replicação do CDC. Para gerar o SCN atual no banco de dados de origem, execute a seguinte instrução SQL: `SELECT current_scn FROM V$DATABASE;`	DBA
Executar a migração de carga total dos esquemas.	Para migrar os esquemas necessários (`FULL LOAD`) do	DBA

Tarefa	Descrição	Habilidades necessárias
	banco de dados on-premises de origem para a instância de destino do Amazon RDS, faça o seguinte: • Para migrar um único esquema, execute o Código 3 na seção Informações adicionais. • Para migrar múltiplos esquemas, execute o Código 4 na seção Informações adicionais. No código, <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE> substitua pelo SCN que você capturou do banco de dados de origem: `DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value => <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>);` Para ajustar o desempenho da migração, você pode ajustar o número de processos paralelos:	

Tarefa	Descrição	Habilidades necessárias
	`DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);`	
Desative os triggers nos esquemas migrados.	Antes de iniciar a tarefa AWS DMS somente do CDC, desative o nos `TRIGGERS` esquemas migrados.	DBA
Coletar estatísticas do esquema para melhorar o desempenho.	O comando Gather Schema Statistics retorna as estatísticas do otimizador de consultas Oracle coletadas para objetos de banco de dados: `EXECUTE DBMS_STATS.GATHER_SCHEMA_STATS(ownname => '<schema_name>');` Ao usar essas informações, o otimizador pode selecionar o melhor plano de execução para qualquer consulta nesses objetos.	DBA

Tarefa	Descrição	Habilidades necessárias
Use AWS DMS para realizar uma replicação contínua da origem para o destino.	Use AWS DMS para realizar uma replicação contínua do banco de dados Oracle de origem para a instância de destino do Amazon RDS for Oracle. Para obter mais informações, consulte Criação de tarefas para uso contínuo de replicação AWS DMS e a postagem do blog Como trabalhar com suporte nativo do CDC em. AWS DMS	DBA, Engenheiro de migração

Substituição para o Amazon RDS para Oracle

Tarefa	Descrição	Habilidades necessárias
Ativar o multi-AZ na instância 48 horas antes da substituição.	Se for uma instância de produção, recomendamos habilitar a implantação Multi-AZ na instância do Amazon RDS para oferecer os benefícios de alta disponibilidade (HA) e recuperação de desastres (DR).	DBA, Engenheiro de migração
Pare a tarefa AWS DMS somente do CDC (se o CDC estiver ativado).	1. Garanta que a latência de origem e a latência de destino nas CloudWatch métricas da Amazon da AWS DMS tarefa mostrem 0 segundos.	DBA

Tarefa	Descrição	Habilidades necessárias
	2. Pare a tarefa AWS DMS somente do CDC.	
Ative os triggers.	Ative o `TRIGGERS` que você desativou antes da criação da tarefa do CDC.	DBA

Recursos relacionados

AWS

- Preparando um banco de dados de origem autogerenciado Oracle para CDC usando AWS DMS
- Criação de tarefas para replicação contínua usando AWS DMS
- Multi-AZ deployments for high availability
- Como trabalhar com o suporte nativo do CDC em AWS DMS (postagem do blog)

Documentação da Oracle

- DBMS_DATAPUMP

Mais informações

Código 1: somente migração de carga total, esquema de aplicativo único

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')'); --
 To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
```

```
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Código 2: somente migração de carga total, vários esquemas de aplicativos

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Código 3: migração de carga total antes da tarefa somente do CDC, esquema de aplicativo único

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
```

```
/
```

Código 4: migração de carga total antes da tarefa somente do CDC, vários esquemas de aplicativos

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN (operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE (handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Cenário em que uma abordagem de migração mista pode funcionar melhor

Em raros cenários em que o banco de dados de origem contém tabelas com milhões de linhas e colunas LOBSEGMENT de tamanho muito grande, esse padrão retardará a migração. O Oracle migra LOBSEGMENTs pelo link de rede, um por vez. Ele extrai uma única linha (junto com os dados da coluna LOB) da tabela de origem e insere a linha na tabela de destino, repetindo o processo até que todas as linhas sejam migradas. O Oracle Data Pump over the database link não suporta carregamento em massa ou mecanismos de carregamento de caminho direto para LOBSEGMENTs.

Nesta situação, recomendamos o seguinte:

- Ignore as tabelas identificadas durante a migração do Oracle Data Pump adicionando o seguinte filtro de metadados:

  ```
  dbms_datapump.metadata_filter(handle =>h1, name=>'NAME_EXPR', value => 'NOT IN
   (''TABLE_1'',''TABLE_2'')');
  ```

- Use uma AWS DMS tarefa (migração de carga total, com replicação CDC, se necessário) para migrar as tabelas identificadas. AWS DMS extrairá várias linhas do banco de dados Oracle

de origem e as inserirá em um lote na instância de destino do Amazon RDS, o que melhora o desempenho.

Migre o Oracle E-Business Suite para o Amazon RDS Custom

Criado por Simon Cunningham (AWS), Jaydeep Nandy (AWS), Nitin Saxena (AWS) e Vishnu Vinnakota (AWS)

Resumo

O Oracle E-Business Suite é uma solução de Planejamento de recursos empresariais (ERP - Enterprise Resource Planning) para automatizar processos em toda a empresa, como finanças, recursos humanos, cadeias de suprimentos e manufatura. Ele tem uma arquitetura de três camadas: cliente, aplicação e banco de dados. Anteriormente, você precisava executar seu banco de dados Oracle E-Business Suite em uma instância autogerenciada do Amazon Elastic Compute Cloud (Amazon EC2), mas agora você pode se beneficiar do Amazon Relational Database Service (Amazon RDS) Custom.

O Amazon RDS Custom para Oracle é um serviço de banco de dados gerenciado para aplicações herdadas, personalizadas e em pacote que exigem acesso ao sistema operacional subjacente e ao ambiente de banco de dados. Ele automatiza tarefas e operações de administração de banco de dados e permite que você, como administrador de banco de dados, acesse e personalize seu ambiente de banco de dados e sistema operacional. Quando você migra seu banco de dados Oracle para o Amazon RDS Custom, o Amazon Web Services (AWS) cuida do trabalho pesado, como tarefas de backup e garantia de alta disponibilidade, enquanto você pode se concentrar na manutenção do aplicativo e da funcionalidade do Oracle E-Business Suite. Para ver os principais fatores a considerar em uma migração, consulte as Estratégias de migração do banco de dados Oracle no Recomendações da AWS.

Esse padrão se concentra nas etapas para migrar um banco de dados Oracle autônomo na Amazon para o EC2 Amazon RDS Custom usando um backup do Oracle Recovery Manager (RMAN) e um sistema de arquivos compartilhado do Amazon Elastic File System (Amazon EFS) entre a instância EC2 e o Amazon RDS Custom. O padrão usa um backup completo do RMAN (que às vezes é chamado de backup de nível 0). Para simplificar, ele usa um backup frio em que o aplicativo é desligado e o banco de dados é montado e não aberto. (Você também pode usar o Oracle Data Guard ou a duplicação RMAN para backup. No entanto, esse padrão não abrange essas opções).

Para obter informações sobre a arquitetura do Oracle E-Business Suite na AWS para alta disponibilidade e recuperação de desastres, consulte o padrão Configurar uma arquitetura de HA/DR para o Oracle E-Business Suite no Amazon RDS Custom com um banco de dados ativo em espera.

> **Note**
>
> Esse padrão fornece links para notas de suporte da Oracle. Você precisa de uma conta do Oracle Support para acessar esses documentos.

Pré-requisitos e limitações

Pré-requisitos

- Um banco de dados de origem Oracle versão 12.1.0.2 ou 19c (mínimo 19.3) que está sendo executado na Amazon EC2 com Oracle Linux 7 ou Red Hat Enterprise Linux (RHEL) versão 7.x. Esse padrão pressupõe que o nome do banco de dados de origem seja `VIS` e que o nome adicional do banco de dados de contêiner do Oracle 19c seja`VISCDB`, mas você pode usar outros nomes.

  > **Note**
  >
  > Você também pode usar esse padrão com bancos de dados de origem Oracle locais, desde que tenha a conectividade de rede adequada entre a rede local e a Amazon Virtual Private Cloud (Amazon VPC).

- Um aplicativo Oracle E-Business Suite versão 12.2.x (instância de visão). Este procedimento foi testado na versão 12.2.11.
- Um único nível de aplicativo Oracle E-Business Suite. No entanto, você pode adaptar esse padrão para trabalhar com vários níveis de aplicativos.
- Para o Oracle 12.1.0.2, o Amazon RDS Custom foi configurado com pelo menos 16 GB de espaço de swap. Caso contrário, o CD de exemplos 12c exibirá um aviso. (O Oracle 19c não exige o CD de exemplos, conforme mencionado posteriormente neste documento).

Conclua as etapas a seguir antes de iniciar a migração:

1. No console do Amazon RDS, crie uma instância de banco de dados Amazon RDS Custom for Oracle com o nome do banco de dados `VIS` (ou o nome do seu banco de dados de origem). Para obter instruções, consulte Como trabalhar com o Amazon RDS Custom na documentação da AWS e a postagem do blog Amazon RDS Custom for Oracle: New Control Capabilities in Database Environment. Isso garante que o nome do banco de dados seja definido com o mesmo nome

do banco de dados de origem. (Se deixado em branco, o nome da EC2 instância e do banco de dados será definido como`ORCL`.) Certifique-se de criar sua versão personalizada do mecanismo (CEV) com os patches que foram aplicados à fonte, no mínimo. Para obter mais informações, consulte Preparação para criar um CEV na documentação do Amazon RDS.

Observação para o Oracle 19c: Atualmente, para o Oracle 19c, o nome do banco de dados de contêineres do Amazon RDS pode ser personalizado. O padrão é `RDSCDB`. Certifique-se de criar a instância Oracle personalizada do RDS com a mesma ID do sistema (SID) da instância de origem EC2 . Por exemplo, nesse padrão, presume-se que o SID Oracle 19c esteja `VISCDB` na instância de origem. Portanto, o SID Oracle 19c de destino no Amazon RDS Custom também deve ser `VISCDB`.

2. Configure a instância de banco de dados personalizada do Amazon RDS com armazenamento, vCPU e memória suficientes para corresponder ao banco de dados de origem da EC2 Amazon. Para fazer isso, você pode combinar os tipos de EC2 instância da Amazon com base na vCPU e na memória.
3. Crie um sistema de arquivos Amazon EFS e monte-o nas instâncias personalizadas da Amazon EC2 e do Amazon RDS. Para obter instruções, consulte a postagem do blog Integrar Amazon RDS Custom for Oracle com o Amazon EFS. Esse padrão pressupõe que você montou o volume do Amazon EFS `/RMAN` nas instâncias de banco de dados personalizadas do Amazon RDS de origem EC2 e de destino, e que a conectividade de rede é possível entre a origem e o destino. Você também pode usar o mesmo método usando a Amazon FSx ou qualquer drive compartilhado.

Suposições

Esse padrão pressupõe que seu aplicativo e banco de dados estejam usando nomes de host lógicos, o que reduz o número de etapas de migração. Você pode ajustar essas etapas para usar nomes de host físicos, mas nomes de host lógicos reduzem a complexidade do processo de migração. Para obter informações sobre as vantagens de usar nomes de host lógicos, consulte as seguintes notas de suporte:

- Para 12c, Observação de Suporte da Oracle 2246690.1
- Para 19c, Observação de Suporte da Oracle 2617788.1

Esse padrão não abrange o cenário de atualização do Oracle 12c para 19c e se concentra na migração da mesma versão do banco de dados Oracle executado na Amazon para o EC2 Amazon RDS Custom for Oracle.

O Amazon RDS Custom para Oracle oferece suporte à personalização do Oracle Home. (O Oracle Home armazena os binários do Oracle). Você pode alterar o caminho padrão de `/rdsdbbin/oracle` para um caminho que você especifica, como`/d01/oracle/VIS/19c`. Para simplificar, as instruções nesse padrão assumem o caminho padrão`/rdsdbbin/oracle`.

Limitações

Esse padrão não é compatível com os seguintes atributos e configurações:

- Definindo o parâmetro `ARCHIVE_LAG_TARGET` do banco de dados para um valor fora do intervalo de 60 a 7200
- Desabilitando o modo de log da instância de banco de dados () `NOARCHIVELOG`
- Desativando o `EBS-optimized` atributo da EC2 instância
- Modificação dos volumes originais do Amazon Elastic Block Store (Amazon EBS) anexados à instância EC2
- Adicionar novos volumes do EBS ou alterar o tipo de volume de para `gp2` `gp3`
- Suporte para o arquivo TNS
- Alterando a `control_file` localização e o nome (deve ser`/rdsdbdata/db/VISCDB_A/controlfile/control-01.ctl`, onde `VISCDB` está o nome do CDB)

Para obter informações adicionais sobre essas e outras configurações não suportadas, consulte Corrigindo configurações não suportadas na documentação do Amazon RDS.

Versões do produto

Para versões do banco de dados Oracle e classes de instância suportadas pelo Amazon RDS Custom, consulte Disponibilidade e requisitos do Amazon RDS Custom for Oracle.

Arquitetura

O diagrama de arquitetura a seguir representa um sistema Oracle E-Business Suite executado em uma única zona de disponibilidade na AWS. O nível do aplicativo é acessado por meio de um Application Load Balancer, tanto o aplicativo quanto os bancos de dados estão em sub-redes

privadas, e o nível de banco de dados Amazon RDS Custom e EC2 Amazon usa um sistema de arquivos compartilhado Amazon EFS para armazenar e acessar os arquivos de backup do RMAN.

Ferramentas

Serviços da AWS

- O Amazon RDS Custom para Oracle é um serviço de banco de dados gerenciado para aplicações herdadas, personalizadas e em pacote que exigem acesso ao sistema operacional subjacente e ao ambiente de banco de dados. Ele automatiza tarefas e operações de administração de banco de dados e permite que você, como administrador de banco de dados, acesse e personalize seu ambiente de banco de dados e sistema operacional.
- O Amazon Elastic File System (Amazon EFS) é um sistema de arquivos simples, de tecnologia sem servidor e elástico para adicionar e remover arquivos sem a necessidade de gerenciamento ou provisionamento. Esse padrão usa um sistema de arquivos compartilhado Amazon EFS para armazenar e acessar os arquivos de backup do RMAN.
- O AWS Secrets Manager é um serviço gerenciado da AWS que permite alternar, gerenciar e recuperar credenciais de banco de dados, chaves de API e outras informações secretas. O Amazon RDS Custom armazena o par de chaves e as credenciais do usuário do banco de dados no Secrets Manager após a criação do banco de dados. Nesse padrão, você recupera as senhas de usuário do banco de dados do Secrets Manager para criar os usuários `RDSADMIN` e `ADMIN` e alterar as senhas do sys e do sistema.

Outras ferramentas

- O RMAN é uma ferramenta que fornece suporte de backup e recuperação para bancos de dados Oracle. Esse padrão usa o RMAN para realizar um backup a frio do banco de dados Oracle de origem na Amazon, EC2 que é restaurado no Amazon RDS Custom.

Práticas recomendadas

- Use nomes de host lógicos. Isso reduz significativamente o número de scripts pós-clone que você precisa executar. Para obter mais informações, consulte o documento Oracle Support Note 2246690.1.

- O Amazon RDS Custom usa o Oracle Automatic Memory Management (AMM) por padrão. Se quiser usar o kernel hugemem, você pode configurar o Amazon RDS Custom para usar o Gerenciamento Automático de Memória Compartilhada (ASMM) em vez disso.
- Deixe o `memory_max_target` parâmetro habilitado por padrão. A estrutura usa esse parâmetro em segundo plano para criar réplicas de leitura.
- Ative o banco de dados Oracle Flashback. Esse atributo é útil em cenários de teste de failover (não de transição) para restabelecer o modo de espera.
- Para parâmetros de inicialização do banco de dados, personalize o PFILE padrão fornecido pela instância de banco de dados do Amazon RDS Custom para o Oracle E-Business Suite em vez de usar o SPFILE do banco de dados de origem da Oracle. Isso ocorre porque espaços em branco e comentários causam problemas ao criar réplicas de leitura no Amazon RDS Custom. Para obter mais informações sobre os parâmetros de inicialização do banco de dados, consulte a Observação de Suporte da Oracle 396009.1.

Na seção Épicos a seguir, fornecemos instruções separadas para Oracle 12.1.0.2 e 19c, onde os detalhes são diferentes.

Épicos

Encerre o aplicativo de origem

Tarefa	Descrição	Habilidades necessárias

Feche o aplicativo.	Para desligar o aplicativo de origem, use estes comandos:
	`$ su - applmgr`
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adstpall.sh`
		DBA

Crie o arquivo .zip.	Crie o `appsutil.zip` arquivo na camada do aplicativo de origem. Você usará esse arquivo posteriormente para configurar o nó de	DBA

Tarefa	Descrição	Habilidades necessárias
	banco de dados do Amazon RDS Custom. `$ perl $AD_TOP/bin/admkappsutil.pl`	
Copie o arquivo .zip para o Amazon EFS.	Copie `appsutil.zip` de `$INST_TOP/admin/out` para seu volume compartilhado do Amazon EFS (`/RMAN/appsutil`). Você pode transferir o arquivo manualmente usando cópia segura (SCP) ou outro mecanismo de transferência.	DBA

Faça pré-clonagem do banco de dados de origem

Tarefa	Descrição	Habilidades necessárias

Pré-clone a camada do banco de dados na Amazon. EC2	Faça login como usuário Oracle e execute:
	
	`$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`
	`$ perl adpreclone.pl dbTier`
	
	Verifique o arquivo de log gerado para confirmar se a operação foi concluída com êxito.
		DBA

Tarefa	Descrição	Habilidades necessárias

Copie o appsutil.zip para o sistema de arquivos do Amazon EFS Compartilhado.	Crie um backup tar e copie `$ORACLE_HOME/appsutil` para o sistema de arquivos compartilhado do Amazon EFS (por exemplo, `/RMAN/appsutil`):
	`$ cd $ORACLE_HOME`
	`$ tar cvf sourceappsutil.tar appsutil`
	`$ cp sourceappsutil.tar /RMAN/appsutil`
		DBA

Execute um backup completo do RMAN a frio do banco de dados de origem da Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Crie um script de backup.	Execute um backup completo do RMAN do banco de dados de origem no sistema de arquivos compartilhado do Amazon EFS. Para simplificar, esse padrão executa um backup RMAN frio. No entanto, você pode modificar essas etapas para realizar um backup dinâmico do RMAN com o Oracle Data Guard para reduzir o tempo de inatividade.	DBA

Tarefa	Descrição	Habilidades necessárias

	1. Inicie o EC2 banco de dados de origem da Amazon no modo de montagem:
	
	`$ sqlplus / as sysdba`
	`$ SQL> shutdown immediate`
	`$ SQL> startup mount`
	
	2. Crie um script de backup RMAN (use um dos exemplos a seguir, dependendo da sua versão do Oracle, ou execute um de seus scripts RMAN existentes) para fazer backup do banco de dados no sistema de arquivos Amazon EFS que você montou (`/RMAN`neste exemplo).
	
	Para Oracle 12.1.0.2
	
	`$ vi FullRMANColdBackup.sh`
	`#!/bin/bash`
	`. /home/oracle/.bash_profile`
	
	`export ORACLE_SID=VIS`
	`export ORACLE_HOME=/d01/oracle/VIS/12.1.0`
	`export DATE=$(date +%y-%m-%d_%H%M%S)`
	
	`rman target / log=/RMAN/VISDB_${DATE}.log <<EOF`
	`run`	

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	allocate channel ch1
	 device type disk format
	 '/RMAN/visdb_full_
	bkp_%u';
	allocate channel ch2
	 device type disk format
	 '/RMAN/visdb_full_
	bkp_%u';
	crosscheck backup;
	delete noprompt
	 obsolete;
	BACKUP AS COMPRESSED
	 BACKUPSET DATABASE PLUS
	 ARCHIVELOG;
	backup archivelog all;
	release channel ch1;
	release channel ch2;
	}
	EOF</pre> Para Oracle 19c: <pre>$ vi FullRMANColdBackup
	.sh
	#!/bin/bash
	. /home/oracle/.bash
	_profile
	
	export ORACLE_SI
	D=VISCDB
	export ORACLE_HOME=/
	d01/oracle/VIS/19c
	export DATE=$(date +
	%y-%m-%d_%H%M%S)
	
	rman target / log=/RMAN
	/VISDB_${DATE}.log <<
	 EOF
	run
	{</pre>	

Tarefa	Descrição	Habilidades necessárias

	`allocate channel ch1 device type disk format '/RMAN/visdb_full_bkp_%u';`
	`allocate channel ch2 device type disk format '/RMAN/visdb_full_bkp_%u';`
	`crosscheck backup;`
	`delete noprompt obsolete;`
	`BACKUP AS COMPRESSED BACKUPSET DATABASE PLUS ARCHIVELOG;`
	`backup archivelog all;`
	`backup current controlfile format '/RMAN/cntrl.bak';`
	`release channel ch1;`
	`release channel ch2;`
	`}`
	`EOF`	

Execute o script de backup.	Altere as permissões, faça login como usuário Oracle e execute o script:
	`$ chmod 755 FullRMANColdBackup.sh`
	`$ ./FullRMANColdBackup.sh`
		DBA

Tarefa	Descrição	Habilidades necessárias

Verifique se há erros e anote o nome do arquivo de backup.	Verifique se há erros no arquivo de log RMAN. Se tudo estiver bem, liste o backup do arquivo de controle. Anote o nome do arquivo de saída.
	
	Para Oracle 12.1.0.2
	
	`RMAN> connect target /`
	
	`RMAN> list backup of controlfile;`
	
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`------- ---- -- ---------- ----------- ------------ ---------- --- ------------ ---------- ---------- ----------

Tarefa	Descrição	Habilidades necessárias

	restaurar o banco de dados no Amazon RDS Custom.
	
	Para Oracle 19c:
	
	`RMAN> connect target /`
	
	`RMAN> list backup of controlfile;`
	
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`------- ---- -- ---------- --------- ---------- ---------- ---------- 38 Full 17.92M DISK 00:00:01 25-NOV-22 BP Key: 38 Status: AVAILABLE Compressed: NO Tag: TAG20221125T095014 Piece Name: /RMAN/cntrl.bak Control File Included: Ckp SCN: 122046201 88873 Ckp time: 23-NOV-22`
	
	Você usará o arquivo de backup `/RMAN/cntrl.bak` posteriormente, ao restaurar o banco de dados no Amazon RDS Custom.	

Configurar o banco de dados do Amazon RDS Custom de destino

Tarefa	Descrição	Habilidades necessárias

Altere o arquivo hosts e defina o nome do host.	**Note**
	Os comandos nesta seção devem ser executados como usuário root.
	
	1. Edite o `/etc/hosts` arquivo na instância de banco de dados Amazon RDS Custom. Uma maneira simples de fazer isso é copiar as entradas do banco de dados e do host do aplicativo do arquivo de origem dos hosts do EC2 banco de dados da Amazon.
	
	`<IP-address> OEBS-app01.localdomain OEBS-app01 OEBS-app01log.localdomain OEBS-app01log`
	`<IP-address> OEBS-db01.localdomain OEBS-db01 OEBS-db01log.localdomain OEBS-db01log`
	
	em que `<IP-address>` é o endereço IP do nó do banco de dados, que você deve substituir pelo endereço IP do Amazon RDS Custom. Os
		DBA

Tarefa	Descrição	Habilidades necessárias

	nomes de host lógicos são anexados com `*log`.
	
	2. Altere o nome do host do banco de dados executando o `hostnamectl` comando:
	
	`$ sudo hostnamectl set-hostname --static persistent-hostname`
	
	Por exemplo:
	
	`$ sudo hostnamectl set-hostname --static OEBS-db01log`
	
	Para obter informações adicionais, consulte o artigo do Knowledge Center sobre a atribuição de nomes de host estáticos.
	
	3. Reiniciar a instância de banco de dados do Amazon RDS Custom Não se preocupe em desligar o banco de dados, pois você o eliminará em uma etapa posterior.
	
	`$ reboot`
	
	4. Quando a instância de banco de dados do Amazon RDS Custom voltar	

Tarefa	Descrição	Habilidades necessárias

	a funcionar, faça login e verifique se o nome do host foi alterado:
	
	`$ hostname`
	`oebs-db01`	

Tarefa	Descrição	Habilidades necessárias

Instale o software Oracle E-Business Suite.	Instale o Oracle E-Business Suite recomendado RPMs na localização inicial da Oracle na instância de banco de dados personalizada do Amazon RDS. Para obter detalhes, consulte a Oracle Suporte Note #1330701.
	1. Veja a seguir uma lista parcial. A lista de RPM muda para cada versão, portanto, verifique se todos os requisitos RPMs estão instalados.
	
	Como usuário raiz, execute:
	
	`$ sudo yum -y update`
	`$ sudo yum install -y elfutils-libelf-devel*`
	`$ sudo yum install -y libXp-1.0.2-2.1*.i686`
	`$ sudo yum install -y libXp-1.0.2-2.1*`
	`$ sudo yum install -y compat-libstdc++-*`
	
	Verifique se todos os patches necessários estão instalados antes de prosseguir com a próxima etapa.
		DBA

Tarefa	Descrição	Habilidades necessárias

Instale o servidor VNC.	**Note**
	Você pode omitir essa etapa para o Oracle 19c porque o CD de exemplos não é mais necessário; consulte a Nota de Suporte 2782085.1 da Oracle.
	
	Para Oracle 12.1.0.2
	
	Instale o servidor VNC e seus pacotes de desktop dependentes. Esse é um requisito para instalar o CD de exemplos 12c na próxima etapa.
	
	1. Como usuário raiz, execute:
	
	`$ sudo yum install -y tigervnc-server`
	`$ sudo yum install -y *kde*`
	`$ sudo yum install -y *xorg*`
	
	2. Inicie o servidor VNC para o `rdsdb` usuário e defina a senha para o VNC:
	
	`$ su - rdsdb`
	`$ vncserver :1`
	`$ vncpassword`
		DBA

Tarefa	Descrição	Habilidades necessárias

Instale o CD de exemplos 12c.	**Note**
	Você pode omitir essa etapa para o Oracle 19c porque o CD de exemplos não é mais necessário; consulte a Nota de Suporte 2782085.1 da Oracle.
	
	Para Oracle 12.1.0.2
	
	1. Baixe os arquivos de instalação em https://edelivery.oracle.com/. Para o Oracle E-Business Suite 12.2.11: Oracle Database 12c Versão 1 (12.1.0.2), procure exemplos para Linux x86-64 V100102-01.zip.
	
	2. Crie um diretório para armazenar o CD de exemplos:
	
	`$ mkdir /RMAN/12c examples`
	
	3. Copie o arquivo .zip do CD de exemplos para esse diretório usando o mecanismo de transferência de sua escolha (por exemplo, SCP):
	
	`V100102-01.zip`
		DBA

Tarefa	Descrição	Habilidades necessárias

	4. Altere a propriedade para`rdsdb`:
	`$ chown -R rdsdb:rdsdb /RMAN/12cexamples`
	5. Como usuário `rdsdb`, descompacte o arquivo:
	`$ unzip V10010201.zip`
	6. Conecte-se a partir de um cliente que tenha acesso ao cliente VNC e ao Amazon RDS Custom. Certifique-se de que você tem a conectividade de rede e as portas de firewall necessárias abertas para permitir o acesso do VNC. Por exemplo, um servidor VNC em execução `display :1` precisará abrir a porta 5901 no grupo de segurança associado ao host personalizado do Amazon RDS. EC2
	7. Vá para o diretório em que você copiou o CD Examples:
	`$ cd /RMAN/12cexamples/examples`
	8. Execute o instalador. Certifique-se de verificar a	

Tarefa	Descrição	Habilidades necessárias

	localização do `oraInst.loc` arquivo.
	
	`./runInstaller -invPtrLoc /rdsdbbin/oracle.12.1.custom.r1.EE.1/oraInst.loc`
	
	9. Use os seguintes parâmetros durante a instalação do CD de exemplos:
	
	`Skip Software Updates`
	`Select Oracle Home 12.1.0.2 (Oracle Base = /rdsdbbin)`
	`(Software Location = /rdsdbbin/oracle/12.1.custom.r1.EE.1)`
	
	10. O programa de instalação inclui cinco etapas com instruções. Siga as etapas até que a instalação seja concluída.	

Elimine o banco de dados inicial e crie os diretórios para armazenar os arquivos do banco de dados

Tarefa	Descrição	Habilidades necessárias
Pausar o modo de automação.	Você precisa pausar o modo de automação em sua instância de banco de dados do Amazon RDS Custom	DBA

Tarefa	Descrição	Habilidades necessárias
	antes de prosseguir com as próximas etapas, para garantir que a automação não interfira na atividade do RMAN. Faça uma pausa na automação usando o comando (AWS Command Line Interface (AWS CLI) a seguir. (Certifique-se de ter configurado primeiro a AWS CLI). `aws rds modify-db-instance \ --db-instance-id entifier VIS \ --automation-mode all-paused \ --resume-full-au tomation-mode-minute 360 \ --region eu-west-1` Ao especificar a duração da pausa, certifique-se de deixar tempo suficiente para a restauração do RMAN. Isso depende do tamanho do banco de dados de origem, portanto modifique o valor 360 devidamente.	

Tarefa	Descrição	Habilidades necessárias

Remova o banco de dados inicial.	Elimine o banco de dados do Amazon RDS Custom existente.
	
	Execute os comandos a seguir estão os comandos a seguir estão os comandos a seguir. (O usuário padrão é `rdsdb`, a menos que você o personali ze).
	
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate ;`
	`SQL> startup nomount restrict;`
	`SQL> alter database mount;`
	`SQL> drop database;`
	`SQL> exit`
		DBA

Tarefa	Descrição	Habilidades necessárias

Crie diretórios para armazenar os arquivos do banco de dados.	Para Oracle 12.1.0.2
	
	Crie diretórios para o banco de dados, o arquivo de controle, os arquivos de dados e o log on-line. Use o diretório pai do `control_files` parâmetro no comando anterior (nesse caso,`VIS_A`). Execute os comandos a seguir como usuário doméstico do Oracle (por padrão,`rdsdb`).
	
	`$ mkdir -p /rdsdbdata/db/VIS_A/controlfile`
	`$ mkdir -p /rdsdbdata/db/VIS_A/datafile`
	`$ mkdir -p /rdsdbdata/db/VIS_A/onlinelog`
	
	Para Oracle 19c:
	
	Crie diretórios para o banco de dados, o arquivo de controle, os arquivos de dados e o log on-line. Use o diretório pai do `control_files` parâmetro no comando anterior (nesse caso,`VISCDB_A`). Execute os comandos a seguir como usuário doméstico do Oracle (por padrão,`rdsdb`).
		DBA

Tarefa	Descrição	Habilidades necessárias

	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/controlfile`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/datafile`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog/arch`
	`$ mkdir /rdsdbdata/db/pdb/VISCDB_A`	

Tarefa	Descrição	Habilidades necessárias
Crie e modifique o arquivo de parâmetros para o Oracle E-Business Suite.	Nesta etapa, você não copiará o arquivo de parâmetro do servidor (SPFILE) do banco de dados de origem. Em vez disso, você usará o arquivo de parâmetros padrão (PFILE) criado com a instância de banco de dados do Amazon RDS Custom e adicionará os parâmetros necessários para o Oracle E-Business Suite. Quando você descarta o banco de dados, a automação do Amazon RDS cria um backup do `init.ora` arquivo, que é associado ao banco de dados do Amazon RDS Custom. Esse arquivo é chamado `oracle_pfile` e está localizado em`/rdsdbdata/config` . Para Oracle 12.1.0.2 1. Copie `/rdsdbdata/config/oracle_pfile` para `$ORACLE_HOME` . `$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVIS.ora` 2. Edite o `initVIS.ora` arquivo na instância de banco de dados Amazon	DBA

Tarefa	Descrição	Habilidades necessárias
	RDS Custom. Valide todos os parâmetros na fonte e adicione os parâmetros conforme necessário. Para obter detalhes, consulte a Oracle Suporte Note 396009.1. ⚠ Important Certifique-se de que não haja comentári os nos parâmetros que você adiciona. Os comentários causarão problemas com a automação, como criar réplicas de leitura e emitir point-in-time recuperações (). PITRs 3. Adicione parâmetros semelhantes aos seguintes ao `initVIS.ora` arquivo, com base em seus requisitos: `*.workarea_size_po licy='AUTO' *.plsql_code_ty pe='INTERPRETED' *.cursor_sharing='E XACT' *._b_tree_bitmap_plan s=FALSE`	

Tarefa	Descrição	Habilidades necessárias
	*.session_cached_cursors=500 *.optimizer_adaptive_features=false *.optimizer_secure_view_merging=false *.SQL92_SECURITY=TRUE *.temp_undo_enabled=true _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_characters = "." nls_comp = binary nls_sort = binary nls_date_format = DD-MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_elimination_cost_ratio =5 _like_with_bind_as_equality = TRUE _fast_full_scan_enabled = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view_merging = FALSE _optimizer_autostats_job = FALSE parallel_max_servers = 8 parallel_min_servers = 0 parallel_degree_policy = MANUAL	

Tarefa	Descrição	Habilidades necessárias

	`sec_case_sensitive_logon = FALSE`
	`compatible = 12.1.0`
	`o7_dictionary_accessibility = FALSE`
	`utl_file_dir =/tmp`
	
	4. Altere os seguintes Os valores dependerão do seu sistema de origem, então revise-os com base na sua configuração atual.
	
	`*.open_cursors=500`
	`*.undo_tablespace='APPS_UNDOTS1`
	
	5. Remova a referência SPFILE.
	
	`*.spfile='/rdsdbbin/oracle/dbs/spfileVIS.ora'`
	
	Observações:
	
	• Não altere os valores fornecidos pelo Amazon RDS Custom PFILE para e. `control_files` `db_unique_name` O Amazon RDS espera esses valores. Desviar-se deles causará problemas se você tentar criar uma réplica de leitura no futuro.	

Tarefa	Descrição	Habilidades necessárias

	• O Amazon RDS Custom usa o Gerenciamento Automático de Memória (AMM) por padrão. Se quiser usar o hugemem, você pode configurar o Amazon RDS Custom para usar o Gerenciamento Automático de Memória Compartilhada (ASMM).
	• Deixe o `memory_max_target` parâmetro habilitado por padrão. A estrutura do Amazon RDS usa isso em segundo plano para criar réplicas de leitura.
	
	6. Confirme se não há problemas com o `initVIS.ora` arquivo que executa o `startup nomount` comando:
	
	`SQL> startup nomount pfile=/rdsdbbin/oracle/dbs/initVIS.ora;`
	`SQL> create spfile='/rdsdbdata/admin/VIS/pfile/spfileVIS.ora' from pfile;`
	`SQL> exit`
	
	7. Crie um link simbólico para o SPFILE.
	
	`$ ln -s /rdsdbdata/admin/VIS/pfile/`	

Tarefa	Descrição	Habilidades necessárias

	`spfileVIS.ora $ORACLE_HOME/dbs/`
	
	Para Oracle 19c:
	
	1. Copie `/rdsdbdata/config/oracle_pfile` para `$ORACLE_HOME` .
	
	`$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVISCDB.ora`
	
	2. Edite o `initVISCDB.ora` arquivo na instância de banco de dados Amazon RDS Custom. Valide todos os parâmetros na fonte e adicione os parâmetros conforme necessário. Para obter detalhes, consulte a Oracle Suporte Note 396009.1.
	
	Important
	Certifique-se de que não haja comentários nos parâmetros que você adiciona. Se houver comentários, eles causarão problemas com a automação, como criar réplicas de leitura e	

Tarefa	Descrição	Habilidades necessárias

	emitir point-in-time recuperações (). PITRs
	
	3. Adicione parâmetros semelhantes aos seguintes ao `initVISCDB.ora` arquivo, com base em seus requisitos:
	
	`*.instance_name=VISCDB`
	`*.sec_case_sensitive_logon= FALSE`
	`*.result_cache_max_size = 600M`
	`*.optimizer_adaptive_plans =TRUE`
	`*.optimizer_adaptive_statistics = FALSE`
	`*.pga_aggregate_limit = 0`
	`*.temp_undo_enabled = FALSE`
	`*._pdb_name_case_sensitive = TRUE`
	`*.event='10946 trace name context forever, level 8454144'`
	`*.workarea_size_policy='AUTO'`
	`*.plsql_code_type='INTERPRETED'`
	`*.cursor_sharing='EXACT'`
	`*._b_tree_bitmap_plans=FALSE`
	`*.session_cached_cursors=500`	

Tarefa	Descrição	Habilidades necessárias
	*.optimizer_secu re_view_merging=false *.SQL92_SECURITY=TRUE _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_charact ers = "." nls_comp = binary nls_sort = binary nls_date_format = DD- MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_eliminatio n_cost_ratio =5 _like_with_bind _as_equality = TRUE _fast_full_scan_enable d = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view _merging = FALSE _optimizer_autostats_ job = FALSE parallel_max_servers = 8 parallel_min_servers = 0 parallel_degree_policy = MANUAL 4. Altere os seguintes Os valores dependerão do seu sistema de origem, então	

Tarefa	Descrição	Habilidades necessárias

	revise-os com base na sua configuração atual.
	
	`*.open_cursors=500`
	`*.undo_tablespace`
	`='UNDOTBS1'`
	
	5. Remova a referência SPFILE.
	
	`*.spfile='/rdsdbbi`
	`n/oracle/dbs/spfil`
	`eVISCDB.ora'`
	
	Observações:
	
	• Não altere os valores fornecidos pelo Amazon RDS Custom PFILE para e. `control_files` `db_unique_name` O Amazon RDS espera esses valores. Desviar-se deles causará problemas se você tentar criar uma réplica de leitura no futuro.
	• O Amazon RDS Custom usa o Gerenciamento Automático de Memória (AMM) por padrão. Se quiser usar o hugemem, você pode configurar o Amazon RDS Custom para usar o Gerenciamento Automático de Memória Compartilhada (ASMM).	

Tarefa	Descrição	Habilidades necessárias

	• Deixe o `memory_max_target` parâmetro habilitado por padrão. A estrutura do Amazon RDS usa isso em segundo plano para criar réplicas de leitura.
	
	6. Confirme se não há problemas com o `initVISCDB.ora` arquivo que executa o `startup nomount` comando:
	
	`SQL> startup nomount pfile=/rdsdbbin/oracle/dbs/initVISCDB.ora;`
	`SQL> create spfile='/rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora' from pfile;`
	`SQL> exit`
	
	7. Crie um link simbólico para o SPFILE.
	
	`$ ln -s /rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora $ORACLE_HOME/dbs/`	

Tarefa	Descrição	Habilidades necessárias

Restaure o banco de dados do Amazon RDS Custom a partir do backup.	Para Oracle 12.1.0.2
	
	1. Restaure o arquivo de controle usando o arquivo de backup que você capturou na fonte anteriormente:
	
	`RMAN> connect target /`
	`RMAN> RESTORE CONTROLFILE FROM '/RMAN/visdb_full_bkp_100rlsbt';`
	
	`Starting restore at 10-APR-22`
	`using target database control file instead of recovery catalog`
	`allocated channel: ORA_DISK_1`
	`channel ORA_DISK_1: SID=201 device type=DISK`
	
	`channel ORA_DISK_1: restoring control file`
	`channel ORA_DISK_1: restore complete, elapsed time: 00:00:01`
	`output file name=/rdsdbdata/db/VIS_A/controlfile/control-01.ctl`
	`Finished restore at 10-APR-22`
	
	2. Catalogue as peças de backup, para que você possa emitir um `RMAN restore`:
		DBA

Tarefa	Descrição	Habilidades necessárias

	`RMAN> alter database mount;`
	`RMAN> catalog start with '/RMAN/visdb';`
	
	3. Crie um script para restaurar o banco de dados:
	
	`$ vi restore.sh`
	`rman target / log=/home/rdsdb/rman.log << EOF`
	`run`
	`{`
	`set newname for database to '/rdsdbdata/db/VIS_A/datafile/%b';`
	`restore database;`
	`switch datafile all;`
	`switch tempfile all;`
	`}`
	`EOF`
	
	4. Restaure a origem no banco de dados do Amazon RDS Custom de destino. Você deve alterar as permissões do script para permitir sua execução e, em seguida, executar o `restore.sh` script para restaurar o banco de dados.
	
	`$ chmod 755 restore.sh`
	`$ nohup ./restore.sh &`
	
	Para Oracle 19c:	

Tarefa	Descrição	Habilidades necessárias

	1. Restaure o arquivo de controle usando o arquivo de backup que você capturou na fonte anteriormente:
	
	`RMAN> connect target /`
	`RMAN> RESTORE CONTROLFILE FROM '/RMAN/cntrl.bak';`
	`Starting restore at 07-JUN-23`
	`using target database control file instead of recovery catalog`
	`allocated channel: ORA_DISK_1`
	`channel ORA_DISK_1: SID=201 device type=DISK`
	`channel ORA_DISK_1: restoring control file`
	`channel ORA_DISK_1: restore complete, elapsed time: 00:00:01`
	`output file name=/rdsdbdata/db/cdb/VISCDB_A/controlfile/control-01.ctl`
	`Finished restore at 07-JUN-23`
	
	2. Catalogue as peças de backup, para que você possa emitir um `RMAN restore`:
	
	`RMAN> alter database mount;`
	`RMAN> catalog start with '/RMAN/visdb';`	

Tarefa	Descrição	Habilidades necessárias

	Se você tiver problemas com o `start with` comando, poderá adicionar as peças de backup individualmente; por exemplo:
	`RMAN> catalog backuppiece '/RMAN/visdb_full_bkp_1d1e507m';`
	e, em seguida, repita o comando para cada peça de backup.
	3. Crie um script para restaurar o banco de dados: Altere o nome do banco de dados conectável dependendo das suas necessidades. Aloque canais paralelos com base no número de v CPUs disponíveis para acelerar o processo de restauração.
	`$ vi restore.sh`
	`rman target / log=/home/rdsdb/rmancdb.log <<`
	`EOF`
	`run {`
	`allocate channel c1`
	`type disk;`
	`allocate channel c2`
	`type disk;`
	`.... .... ....`
	`allocate channel c<N>`
	`type disk;`
	`set newname for database`
	`to '/rdsdbdata/db/cdb`	

Tarefa	Descrição	Habilidades necessárias
	`/VISCDB_A/datafile/ %b'; set newname for database root to '/rdsdbda ta/db/cdb/VISCDB_A/ datafile/%f_%b'; set newname for database "PDB$SEED" to '/rdsdbdata/db/cdb/ pdbseed/%f_%b'; set newname for pluggable database VIS to '/rdsdbdata/db/pdb /VISCDB_A/%f_%b'; restore database; switch datafile all; switch tempfile all; release channel c1; release channel c2; release channel c3; .... release channel c<N>; } EOF`  4. Restaure a origem no banco de dados do Amazon RDS Custom de destino. Você deve alterar as permissões do script para permitir sua execução e, em seguida, executar o `restore.sh` script para restaurar o banco de dados.  `$ chmod 755 restore.sh $ nohup ./restore.sh &`	

Tarefa	Descrição	Habilidades necessárias

Verifique se há problemas nos arquivos de log.	Para Oracle 12.1.0.2
	
	1. Confirme se não há problemas revisando o `rman.log` arquivo:
	
	`$ cat /home/rdsdb/rman.log`
	
	2. Confirme o caminho dos arquivos de log registrados no arquivo de controle:
	
	`SQL> select member from v$logfile;`
	`MEMBER`
	`----------`
	`/d01/oracle/VIS/data/log1.dbf`
	`/d01/oracle/VIS/data/log2.dbf`
	`/d01/oracle/VIS/data/log3.dbf`
	
	3. Renomeie os arquivos de log para que correspondam ao caminho do arquivo de destino. Substitua o caminho para corresponder à saída da etapa anterior:
	
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log1.`
		DBA

Tarefa	Descrição	Habilidades necessárias
	dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log1.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log2.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log2.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log3.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log3.dbf'; Para Oracle 19c: 1. Confirme se não há problemas revisando o `rmancdb.log` arquivo: `$ cat /home/rdsdb/rmancdb.log` 2. Confirme o caminho dos arquivos de log registrados no arquivo de controle: SQL> select member from v$logfile; MEMBER ---------- ---------- ---------- ---------- --------	

Tarefa	Descrição	Habilidades necessárias

	`/d01/oracle/VIS/oradata/VISCDB/redo03.log`
	`/d01/oracle/VIS/oradata/VISCDB/redo02.log`
	`/d01/oracle/VIS/oradata/VISCDB/redo01.log`
	
	3. Renomeie os arquivos de log para que correspondam ao caminho do arquivo de destino. Substitua o caminho para corresponder à saída da etapa anterior:
	
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/oradata/VISCDB/redo01.log' TO '/rdsdbdata/db/cdb/VISCDB_A/onlinelog/log1.dbf';`
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/oradata/VISCDB/redo02.log' TO '/rdsdbdata/db/cdb/VISCDB_A/onlinelog/log2.dbf';`
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/oradata/VISCDB/redo03.log' TO '/rdsdbdata/db/cdb/VISCDB_A/onlinelog/log3.dbf';`	

Tarefa	Descrição	Habilidades necessárias

	4. Confirme o caminho, o status dos arquivos de log e o número do grupo registrado no arquivo de controle:
	
	`SQL> column REDOLOG_FILE_NAME format a50`
	`SQL> SELECT a.GROUP#, a.status, b.MEMBER AS REDOLOG_FILE_NAME, (a.BYTES/1024/1024) AS SIZE_MB`
	`FROM v$log a`
	`JOIN v$logfile b ON a.Group#=b.Group#`
	`ORDER BY a.GROUP#;`
	
	`GROUP# STATUS REDOLOG_FILE_NAME SIZE_MB`
	`1 CURRENT /rdsdbdata/db/cdb/VISCDB_A/onlinelog/log1.dbf 512`
	`2 INACTIVE /rdsdbdata/db/cdb/VISCDB_A/onlinelog/log2.dbf 512`
	`3 INACTIVE /rdsdbdata/db/cdb/VISCDB_A/onlinelog/log3.dbf 512`	

Tarefa	Descrição	Habilidades necessárias
Confirme se você pode abrir o banco de dados do Amazon RDS Custom e criar arquivos de log OMF.	O Amazon RDS Custom for Oracle usa o Oracle Managed Files (OMF) para simplific ar as operações. Você pode promover réplicas de leitura para instâncias autônomas , mas primeiro precisa criar os arquivos de log usando o OMF. Isso é para garantir que o caminho correto seja usado quando a instância for promovida. Para obter mais informações sobre como promover réplicas de leitura, consulte a documentação do Amazon RDS. A falha no uso de arquivos OMF pode causar problemas ao tentar promover réplicas de leitura. 1. Abra o banco de dados com `resetlogs` : `SQL> alter database open resetlogs;` **Note** Se você receber o erro ORA-00392: o log xx do thread 1 está sendo apagado, operação não permitida, siga as etapas na seção	DBA

Tarefa	Descrição	Habilidades necessárias
	Solução de problemas do ORA-00392.	

	2. Confirme se o banco de dados está aberto:
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`----------`
	`READ WRITE`	

	3. Crie os arquivos de log OMF. Altere os números dos grupos, o número de grupos e o tamanho, dependendo dos seus requisitos, usando a saída da consulta anterior do arquivo de log. O exemplo a seguir começa no grupo 4 e adiciona três grupos para simplificar.
	`SQL> alter database add logfile group 4 size 512M;`
	`Database altered.`
	`SQL> alter database add logfile group 5 size 512M;`
	`Database altered.`
	`SQL> alter database add logfile group 6 size 512M;`
	`Database altered.`	

Tarefa	Descrição	Habilidades necessárias

	4. Elimine os arquivos anteriores não OMF. Aqui está um exemplo que você pode personalizar com base nos seus requisitos e na saída da consulta nas etapas anteriores:
	`SQL> alter database drop logfile group 1;`
	`System altered.`
	`SQL> alter database drop logfile group 2;`
	`System altered.`
	`SQL> alter database drop logfile group 3;`
	`System altered.`
	Note
	Se você receber um erro ORA-01624 ao tentar eliminar os arquivos de log, consulte a seção Solução de problemas.
	5. Confirme se você pode ver os arquivos OMF que foram criados. (O caminho do diretório varia para Oracle 12.1.0.2 e 19c, mas o conceito é o mesmo).	

Tarefa	Descrição	Habilidades necessárias

	`SQL> select member from v$logfile;`
	
	`MEMBER`
	`----------`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_4_ksrbslny_.log`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_5_ksrchw0k_.log`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_6_ksrcnl9v_.log`
	
	6. Reinicie o banco de dados e confirme se o SPFILE está sendo usado pela instância:
	
	`SQL> shutdown immediate`
	`SQL> startup`
	`SQL> show parameter spfile`
	
	Para o Oracle 12.1.0.2, essa consulta retorna:
	
	`spfile /rdsdbbin/oracle/dbs/spfileVIS.ora`
	
	Para o Oracle 19c, a consulta retorna:	

Tarefa	Descrição	Habilidades necessárias

	`spfile /rdsdbbin /oracle/dbs/spfile VISCDB.ora`
	
	7. Somente para o Oracle 19c, verifique o status do banco de dados do contêiner e abra-o, se necessário:
	
	`SQL> show pdbs`
	`CON_ID CON_NAME OPEN MODE RESTRICTED`
	`---------- --------- ---------- ----------`
	`2 PDB$SEED READ ONLY NO`
	`3 VIS MOUNTED NO`
	
	`SQL> alter session set container=VIS;`
	`Session altered.`
	
	`SQL> alter database open;`
	`Database altered.`
	
	`SQL> alter database save state;`
	`Database altered.`
	
	`SQL> show pdbs`
	`CON_ID CON_NAME OPEN MODE RESTRICTED`
	`---------- --------- ---------- ----------`
	`2 PDB$SEED READ ONLY NO`
	`3 VIS READ WRITE NO`	

Tarefa	Descrição	Habilidades necessárias

	3 VIS READ WRITE NO
	
	SQL> exit
	
	8. Exclua o `init.ora` arquivo de`$ORACLE_HOME/dbs` , porque você não está usando o PFILE:
	
	`$ cd $ORACLE_HOME/dbs`
	
	Para o Oracle 12.1.0.2, use o comando:
	
	`$ pwd`
	`/rdsdbbin/oracle/dbs`
	`$ rm initVIS.ora`
	
	Para o Oracle 19c, use o comando:
	
	`$ pwd`
	`/rdsdbbin/oracle/dbs`
	`$ rm initVISCDB.ora`	

Recupere as senhas do Secrets Manager, crie usuários e altere senhas

Tarefa	Descrição	Habilidades necessárias
Recupere senhas do Secrets Manager.	Você pode executar essas etapas no console ou usando a CLI da AWS. As etapas a	DBA

Tarefa	Descrição	Habilidades necessárias
	seguir fornecem instruções para o console. 1. Faça login no AWS Management Console e abra o console do Amazon RDS em https://console.aws.amazon.com/rds/. 2. No painel de navegação, escolha Databases (Bancos de dados) e, depois, selecione o banco de dados Amazon RDS. 3. Escolha Configuração e anote o ID do recurso da instância (ele estará no formato: `db-WZ4WLCK6AOQ6TJGZKMGRCDCI3Y`). 4. Abra o console do AWS Secrets Manager em https://console.aws.amazon.com/secretsmanager/. 5. Escolha o segredo que tem o mesmo nome de `do-not-delete-custom-<resource_id>` , onde `resource-id` se refere ao ID da instância que você anotou na etapa 3.	

Tarefa	Descrição	Habilidades necessárias
	6. Escolha Recuperar valor do segredo.	

Tarefa	Descrição	Habilidades necessárias

Crie o usuário RDSADMIN.	`RDSADMIN` é um usuário de banco de dados de monitoramento e orquestrador na instância de banco de dados do Amazon RDS Custom. Como o banco de dados inicial foi descartado e o banco de dados de destino foi restaurado da origem usando o RMAN, você deve recriar esse usuário após a operação de restauração para garantir que o monitoramento do Amazon RDS Custom funcione conforme o esperado. Você também precisa criar uma função e um espaço de tabela separados para o usuário. `RDSADMIN` As instruções são um pouco diferentes para o Oracle 12.1.0.2 e 19c.
	
	Para Oracle 12.1.0.2
	
	1. Insira o seguinte comando no prompt SQL:
	
	`SQL> set echo on feedback on serverout on SQL> @?/rdbms/admin/utlpwdmg.sql`
	
	`SQL> ALTER PROFILE DEFAULT LIMIT`
		DBA

Tarefa	Descrição	Habilidades necessárias
	FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL; 2. Para criar a funçãoRDSADMIN: SQL> create profile RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400	

Tarefa	Descrição	Habilidades necessárias
	PASSWORD_GRACE_TIME 604800/86400; 3. Defina os perfis SYS, SYSTEM, e DBSNMP de usuário para RDSADMIN: SQL> set echo on feedback on serverout on SQL> alter user SYS profile RDSADMIN; SQL> alter user SYSTEM profile RDSADMIN; SQL> alter user DBSNMP profile RDSADMIN; 4. Crie o espaço RDSADMIN de tabela: SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent managemen t local autoallocate default nocompress segment space managemen t auto; 5. Criar o usuário RDSADMIN Substitua a RDSADMIN senha pela senha que você obteve anteriormente no Secrets Manager:	

Tarefa	Descrição	Habilidades necessárias

	`SQL> create user rdsadmin identified by xxxxxxxxxx`
	`Default tablespace rdsadmin`
	`Temporary tablespace temp`
	`profile rdsadmin ;`
	
	6. Conceda privilégios para`RDSADMIN`:
	
	`SQL> grant select on sys.v_$instance to rdsadmin;`
	`SQL> grant select on sys.v_$archived_log to rdsadmin;`
	`SQL> grant select on sys.v_$database to rdsadmin;`
	`SQL> grant select on sys.v_$database_incarnation to rdsadmin;`
	`SQL> grant select on dba_users to rdsadmin;`
	`SQL> grant alter system to rdsadmin;`
	`SQL> grant alter database to rdsadmin;`
	`SQL> grant connect to rdsadmin with admin option;`
	`SQL> grant resource to rdsadmin with admin option;`
	`SQL> alter user rdsadmin account unlock identified by xxxxxxxxxxx;`	

Tarefa	Descrição	Habilidades necessárias

	`SQL> @?/rdbms/admin/userlock.sql`
	`SQL> @?/rdbms/admin/utlrp.sql`
	
	Para Oracle 19c:
	
	1. Insira o seguinte comando no prompt SQL:
	
	`SQL> set echo on feedback on serverout on`
	`SQL> @?/rdbms/admin/utlpwdmg.sql`
	
	`SQL> alter profile default LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL;`
	
	2. Para criar a funçãoRDSADMIN.
	
	Note
	RDSADMINtem um prefixo de C## no Oracle 19c. Isso ocorre porque o parâmetro do banco de dados common_user_prefix está	

Tarefa	Descrição	Habilidades necessárias
	definido comoC##. RDSADMINnão tem prefixo no Oracle 12.1.0.2. `SQL> create profile C##RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400 PASSWORD_GRACE_TIME 604800/86400;`	

Tarefa	Descrição	Habilidades necessárias

	3. Defina os perfis `SYS`, `SYSTEM`, e `DBSNMP` de usuário para `RDSADMIN`:
	`SQL> alter user SYS profile C##RDSADMIN;`
	`SQL> alter user SYSTEM profile C##RDSADMIN;`
	`SQL> alter user DBSNMP profile C##RDSADMIN;`
	4. Crie o espaço `RDSADMIN` de tabela:
	`SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent managemen t local autoallocate default nocompress segment space managemen t auto;`
	5. Criar o usuário `RDSADMIN` Substitua a senha `RDSADMIN` pela senha que você obteve anteriormente no Secrets Manager.
	`SQL> create user C##rdsadmin identifie d by xxxxxxxxxx profile C##rdsadmin container=all;`	

Tarefa	Descrição	Habilidades necessárias

	6. Conceda privilégios para`RDSADMIN`:
	
	`SQL> grant select on sys.v_$instance to c##rdsadmin;`
	`SQL> grant select on sys.v_$archived_log to c##rdsadmin;`
	`SQL> grant select on sys.v_$database to c##rdsadmin;`
	`SQL> grant select on sys.v_$database_incarnation to c##rdsadmin;`
	`SQL> grant select on dba_users to c##rdsadmin;`
	`SQL> grant alter system to C##rdsadmin;`
	`SQL> grant alter database to C##rdsadmin;`
	`SQL> grant connect to C##rdsadmin with admin option;`
	`SQL> grant resource to C##rdsadmin with admin option;`
	`SQL> alter user C##rdsadmin account unlock identified by xxxxxxxxxxx;`
	`SQL> @?/rdbms/admin/userlock.sql`
	`SQL> @?/rdbms/admin/utlrp.sql`	

Tarefa	Descrição	Habilidades necessárias

Crie o usuário mestre.	Como o banco de dados inicial foi descartado e o banco de dados de destino foi restaurado da origem usando o RMAN, você deverá recriar o usuário mestre. Neste exemplo, o nome de usuário mestre é `admin`.
	
	Para Oracle 12.1.0.2
	
	`SQL> create user admin identified by <password>; SQL> grant dba to admin`
	
	Para Oracle 19c:
	
	`SQL> alter session set container=VIS;`
	
	`Session altered.`
	
	`SQL> create user admin identified by <password>;`
	
	`User created.`
	
	`SQL> grant dba to admin;`
	
	`Grant succeeded.`
		DBA

Tarefa	Descrição	Habilidades necessárias

Altere as senhas do superusuário.	1. Altere as senhas do sistema usando a senha que você recuperou do Secrets Manager.
	
	Para Oracle 12.1.0.2
	
	`SQL> alter user sys identified by xxxxxxxxxxx;`
	`SQL> alter user system identified by xxxxxxxxxx;`
	
	Para Oracle 19c:
	
	`SQL> alter user sys identified by xxxxxxxxxxx container =all;`
	`SQL> alter user system identified by xxxxxxxxxx container =all;`
	
	1. Alterar as `EBS_SYSTEM` senhas
	
	Para Oracle 12.1.0.2
	
	`SQL> alter user ebs_system identified by xxxxxxxxxx;`
	
	Para Oracle 19c:
		DBA

Tarefa	Descrição	Habilidades necessárias

	Para esta versão, você também precisa se conectar ao banco de dados do contêiner para atualizar a `EBS_SYSTEM` senha lá.
	
	`SQL> alter session set container=vis;`
	`SQL> alter user ebs_system identified by xxxxxxxxxx;`
	
	`SQL> exit;`
	
	Se você não alterar essas senhas, o Amazon RDS Custom exibirá a mensagem de erro: o usuário de monitoramento do banco de dados ou as credenciais do usuário foram alteradas.	

Crie diretórios para o Oracle E-Business Suite, instale o ETCC e execute o Autoconfig

Tarefa	Descrição	Habilidades necessárias
Crie os diretórios necessários para o Oracle E-Business Suite.	1. No banco de dados Oracle do Amazon RDS Custom, execute o seguinte script como usuário doméstico do Oracle para criar o `9idata` diretório em`$ORACLE_HOME/nls/data/9idata` . Esse diretório é necessário para o Oracle E-Business Suite.	

Tarefa	Descrição	Habilidades necessárias

	`perl $ORACLE_HOME/nls/data/old/cr9idata.pl`
	
	Ignore a `ORA_NLS10` mensagem, pois você criará o ambiente contextual em etapas posteriores.
	
	2. Copie o `appsutil.tar` arquivo, que você criou anteriormente a partir do sistema de arquivos compartilhado do Amazon EFS, e descompacte-o no diretório inicial do Oracle no Amazon RDS Custom. Isto cria o diretório `appsutil` no diretório `$ORACLE_HOME` .
	
	`$ cd /RMAN/appsutil`
	`$ cp sourceappsutil.tar $ORACLE_HOME`
	`$ cd $ORACLE_HOME`
	`$ tar xvf sourceappsutil.tar appsutil`
	
	3. Copie o arquivo `appsutil.zip` , que você salvou anteriormente no sistema de arquivos compartilhados Amazon EFS. Esse foi o arquivo que você criou na camada do aplicativo.	

Tarefa	Descrição	Habilidades necessárias

	Como `rdsdb` usuário na instância de banco de dados Amazon RDS Custom:
	`$ cp /RMAN/appsutil/appsutil.zip $ORACLE_HOME`
	`$ cd $ORACLE_HOME`
	4. Descompacte o `appsutil.zip` arquivo para criar o `appsutil` diretório e os subdiretórios no diretório inicial do Oracle:
	`$ unzip -o appsutil.zip`
	A `-o` opção significa que alguns dos arquivos serão sobrescritos.	

Tarefa	Descrição	Habilidades necessárias

Configure os arquivos tsanames.ora e sqlnet.ora.	Você precisa configurar o arquivo `tnsnames.ora` para poder se conectar ao banco de dados com a ferrament a Autoconfig. No exemplo a seguir, você pode ver que o arquivo `tnsnames.ora` está vinculado automaticamente, mas está vazio por padrão.
	`$ cd $ORACLE_HOME/netwo rk/admin`
	`$ ls -ltr`
	`-rw-r--r-- 1 rdsdb database 373 Oct 31 2013 shrept.lst`
	`lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 listener.ora -> /rdsdbdata/config/ listener.ora`
	`lrwxrwxrwx 1 rdsdb database 28 Feb 9 17:17 sqlnet.ora -> /rdsdbdata/config/ sqlnet.ora`
	`lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 tnsnames.ora -> /rdsdbdata/config/ tnsnames.ora`
	1. Crie a entrada `tnsnames.ora`. Devido à forma como a automação do Amazon RDS analisa os arquivos, você precisa garantir que a entrada não contenha espaços em
		DBA

Tarefa	Descrição	Habilidades necessárias

	branco, comentários ou linhas extras. Caso contrário, você poderá ter problemas ao usar alguns deles APIs , como create-db-instance-read - replica. Use o modelo a seguir como um exemplo.
	
	2. Substitua a porta, o host e o SID de acordo com seus requisitos:
	
	`$ vi tnsnames.ora`
	`VIS=(DESCRIPTION=`
	`(ADDRESS_LIST=(ADD`
	`RESS=(PROTOCOL=TCP`
	`)(PORT=1521)(HOST=`
	`xx.xx.xx.xx)))(CON`
	`NECT_DATA=(SID=VIS)`
	`(SERVER=DEDICATED)))`
	
	Note
	Não deve haver linhas extras no arquivo. Se não remover as linhas, você pode encontrar problemas ao criar uma réplica de leitura no futuro. A criação de uma réplica de leitura pode falhar com a mensagem de erro: Exceção de lançament o de atividade:: Não é possível chamar	

Tarefa	Descrição	Habilidades necessárias

	com êxito o RestrictR eplication em nenhum host. HostManag erException
	
	3. Confirme se o banco de dados pode ser acessado:
	
	`$ tnsping vis`
	`OK (0 msec)`
	
	4. Somente para o Oracle 19c, atualize o `sqlnet.or a` arquivo. Não fazer isso resultará no erro ORA-01017 : nome de usuário/senha inválidos; logon negado ao tentar se conectar ao banco de dados. Edite `sqlnet.or a` `$ORACLE_HOME/netwo rk/admin` para correspon der ao seguinte:
	
	`NAMES.DIRECTORY_PA`
	`TH=(TNSNAMES, ONAMES,`
	`HOSTNAME)`
	`SQLNET.EXPIRE_TIME= 10`
	`SQLNET.INBOUND_`
	`CONNECT_TIMEOUT =60`
	`SQLNET.ALLOWED`
	`_LOGON_VERSION_SER`
	`VER=10`
	`HTTPS_SSL_VERSION=un`
	`determined`
	
	5. Teste de conectividade:	

Tarefa	Descrição	Habilidades necessárias
	`$ sqlplus apps/****@vis`	

Tarefa	Descrição	Habilidades necessárias

Configurar o banco de dados	Agora que você testou a conectividade com o banco de dados, você pode configura r o banco de dados com o utilitário appsutil para criar o ambiente contextual.
	
	Para Oracle 12.1.0.2
	
	1. Execute os seguintes comandos :
	
	`$ cd $ORACLE_HOME/appsu til/bin`
	`$ perl adbldxml.pl  appsuser=apps`
	`Enter Hostname of  Database server: oebs- db01`
	`Enter Port of Database  server: 1521`
	`Enter SID of Database  server: VIS`
	`Enter Database Service  Name: VIS`
	`Enter the value for  Display Variable: :1`
	`The context file has  been created at: /rdsdbbin/oracle/ appsutil/VIS_oebs- db01.xml`
	
	2. Crie `oraInst.loc` a partir do usuário raiz:
	
	`$ vi /etc/oraInst.loc`
	`inventory_loc=/rdsd bbin/oracle.12.1.c`
		DBA

Tarefa	Descrição	Habilidades necessárias

	ustom.r1.EE.1/oraI
	nventory
	inst_group=database
	
	3. Clone o arquivo de contexto para definir o nome do host lógico usando o arquivo de contexto criado na etapa anterior. Como usuário `rdsdb`, execute:
	
	`$ cd $ORACLE_HOME/appsu`
	`til/clone/bin`
	`$ perl adclonectx.pl \`
	`contextfile=[ORA`
	`CLE_HOME]/appsutil/`
	`[current context file] \`
	`template=[ORACLE`
	`_HOME]/appsutil/te`
	`mplate/adxdbctx.tmp`
	
	em que `oebs-db01log` se refere ao nome do host lógico. Por exemplo:
	
	`$ perl adclonectx.pl \`
	`contextfile=/rdsdbbin/`
	`oracle.12.1.custom.r1`
	`.EE.1/appsutil/VIS`
	`_oebs-db01.xml \`
	`template=/rdsdbbin/`
	`oracle/appsutil/`
	`template/adxdbctx.tmp`
	`Target System Hostname`
	` (virtual or normal)`
	` [oebs-db01] : oebs-`
	`db01log`	

Tarefa	Descrição	Habilidades necessárias
	Target System Base Directory : /rdsdbbin/ oracle Target Instance is RAC (y/n) [n] : n Target System Database SID : VIS Oracle OS User [rdsdb] : Oracle OS Group [rdsdb] : database Role separation is supported y/n [n] ? : n Target System utl_file_ dir Directory List : / tmp Number of DATA_TOP's on the Target System [1] : Target System DATA_TOP Directory 1 [/rdsdbbi n/oracle/data] : / rdsdbdata/db/VIS_A/ datafile/ Target System RDBMS ORACLE_HOME Directory [/rdsdbbin/oracle/ 12.1.0] : /rdsdbbin/ oracle Do you want to preserve the Display [:1] (y/n) : y Do you want the target system to have the same port values as	

Tarefa	Descrição	Habilidades necessárias
	the source system (y/n) [y] ? : y The new database context file has been created : /rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml contextfile=/rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml	
	Para Oracle 19c: 1. Execute os seguintes comandos : $ cd $ORACLE_HOME/appsutil/bin $ perl adbldxml.pl appsuser=apps Enter Hostname of Database server: oebs-db01 Enter Port of Database server: 1521 Enter SID of Database server: VIS Enter the database listener name:L_VISCDB_001 Enter the value for Display Variable: :1 The context file has been created at: /rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml	

Tarefa	Descrição	Habilidades necessárias

	2. Crie `oraInst.loc` a partir do usuário raiz:
	`$ vi /etc/oraInst.loc`
	`inventory_loc=/rdsdbbin/oracle/oraInventory`
	`inst_group=database`
	3. Clone o arquivo de contexto para definir o nome do host lógico usando o arquivo de contexto criado na etapa anterior. Como usuário `rdsdb`, execute:
	`$ cd $ORACLE_HOME/appsutil/clone/bin`
	`$ perl adclonectx.pl \`
	`contextfile=[ORACLE_HOME]/appsutil/[current context file] \`
	`template=[ORACLE_HOME]/appsutil/template/adxdbctx.tmp`
	em que `oebs-db01log` se refere ao nome do host lógico. Por exemplo:
	`$ perl adclonectx.pl \`
	`contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml \`
	`template=/rdsdbbin/oracle/appsutil/template/adxdbctx.tmp`	

Tarefa	Descrição	Habilidades necessárias
	Target System Hostname (virtual or normal) [oebs-db01] : oebs-db01log Target System Base Directory : /rdsdbbin/oracle Target Instance is RAC (y/n) [n] : n Target System CDB Name : VISCDB Target System PDB Name : VIS Oracle OS User [oracle] : rdsdb Oracle OS Group [dba] : database Role separation is supported y/n [n] ? : n Number of DATA_TOP's on the Target System [2] : Target System DATA_TOP Directory 1 [/d01/oracle/VISCDB] : /rdsdbdata/db/pdb/VISCDB_A Target System DATA_TOP Directory 2 [/d01/oracle/data] : /rdsdbdata/db/pdb/VISCDB_A/datafile Specify value for OSBACKUPDBA group [database] : Specify value for OSDGDBA group [database] : Specify value for OSKMDBA group [database] :	

Tarefa	Descrição	Habilidades necessárias
	Specify value for OSRACDBA group [database] : Target System RDBMS ORACLE_HOME Directory [/d01/oracle/19.0.0] : /rdsdbbin/oracle Do you want to preserve the Display [:1] (y/n) : y Do you want the target system to have the same port values as the source system (y/n) [y] ? : y Validating if the source port numbers are available on the target system.. Complete port information available at /rdsdbbin/oracle/appsutil/clone/bin/out/VIS_oebs-db01log/portpool.lst New context path and file name [VIS_oebs-db01log.xml] : /rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml Do you want to overwrite it (y/n) [n] ? : y Replacing /rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml file. The new database context file has been created : contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml	

Tarefa	Descrição	Habilidades necessárias
	`Check Clone Context logfile /rdsdbbin/oracle/appsutil/clone/bin/CloneContext_0609141428.log for details.`	

Tarefa	Descrição	Habilidades necessárias

Instale o ETCC e execute o Autoconfig.	1. Instale o Oracle E-Business Suite Technology Codelevel Checker (ETCC).
	
	Baixe o patch 17537119 do My Oracle Support e siga as instruções em `README.txt` . Você criará um diretório chamado `etcc` no `$ORACLE_HOME` diretório , descompactará o patch para criar um script chamado `echeckMTpatch.sh` , em seguida, executará o script para verificar as versões do patch.
	
	2. Execute o utilitário Autoconfig e passe o novo arquivo lógico de contexto do nome do host.
	
	Para Oracle 12.1.0.2
	
	`cd $ORACLE_HOME/appsutil/bin`
	`$ ./adconfig.sh contextfile=/rdsdbbin/oracle.12.1.customstom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml`
	
	Para Oracle 19c:
	
	O Autoconfig espera que o nome do receptor correspon
		DBA

Tarefa	Descrição	Habilidades necessárias

	da a CDBNAME. Portanto, o arquivo de configuração do receptor original do backup será usado L_<CDBNAME>_001 temporariamente.
	
	`$ lsnrctl stop L_VISCDB_001`
	`$ cp -rp /rdsdbdata/config/listener.ora /rdsdbdata/config/listener.ora_orig`
	`$ vi /rdsdbdata/config/listener.ora`
	`:%s/L_VISCDB_001/VISCDB/g`
	`$ lsnrctl start VISCDB`
	`$ cd /rdsdbbin/oracle/appsutil`
	`$ . ./txkSetCfgCDB.env dboraclehome=/rdsdbbin/oracle.19.custom.r1.EE-CDB.1`
	
	`Oracle Home being passed: /rdsdbbin/oracle`
	
	`$ echo $ORACLE_HOME`
	`/rdsdbbin/oracle.19.custom.r1.EE-CDB.1`
	`$ export ORACLE_SID=VISCDB`
	`$ cd $ORACLE_HOME/appsutil/bin`
	`$ perl $ORACLE_HOME/appsutil/bin/txkPostPDBCreationTasks.pl -dboraclehome=$ORACLE_HOME -outdir=`	

Tarefa	Descrição	Habilidades necessárias

	`$ORACLE_HOME/appsutil/log -cdbsid=VISCDB -pdbsid=VIS -appsuser=apps -dbport=1521 -servicetype=onpremise`
	
	`Enter the APPS Password: <apps password>`
	
	`Enter the CDB SYSTEM Password:<password from secrets manager>`
	
	Note
	Se os diretórios do banco de dados tiverem sido alterados, siga as instruções na Nota de Suporte Oracle 2525754.1.	

Configure as entradas do TNS para o Amazon RDS Custom e o Oracle E-Business Suite

Tarefa	Descrição	Habilidades necessárias
Configure as entradas do TNS para o Amazon RDS Custom e o Oracle E-Business Suite	O Autoconfig gera os arquivos TNS nos locais padrão. Para o Oracle 12.1.0.2 (que não é CDB) e para o Oracle19c PDB, o local padrão é `$ORACLE_HOME/network/admin/$<CONTEXT_NAME>` . O CDB para Oracle	DBA

Tarefa	Descrição	Habilidades necessárias
	19c usa o padrão`$ORACLE_HOME/network/admin/` , conforme definido `$TNS_ADMIN` nos arquivos de ambiente que são gerados quando você executou o Autoconfig nas etapas anteriores. Para o Oracle 12.1.0.2 e o 19c CDB, você não os usará porque os arquivos `tnsnames.ora` e `listener.ora` gerados pelo Autoconfig não atendem aos requisitos do Amazon RDS, como a ausência de espaços em branco ou comentários. Em vez disso, você usa os arquivos genéricos fornecidos com o banco de dados do Amazon RDS Custom para garantir a conformidade com o que o sistema espera e reduzir a margem de erro. Por exemplo, o Amazon RDS Custom espera o seguinte formato de nomenclatura: `L_<INSTANCE_NAME>_001` Para o Oracle 12.1.0.2, isso seria:	

Tarefa	Descrição	Habilidades necessárias

	`L_VIS_001`
	
	Para o Oracle 19c, isso seria:
	
	`L_VISCDB_001`
	
	Aqui está um exemplo do `listener.ora` arquivo que você usará. Isso foi gerado quando você criou o banco de dados do Amazon RDS Custom. Neste ponto, você não fez nenhuma alteração nesse arquivo e o deixará como padrão.
	
	Para Oracle 12.1.0.2
	
	`$ cd $ORACLE_HOME/network/admin`
	`$ cat listener.ora`
	`ADR_BASE_L_VIS_001=/rdsdbdata/log/`
	`SID_LIST_L_VIS_001=(SID_LIST =`
	`(SID_DESC = (SID_NAME = VIS)(GLOBAL_DBNAME = VIS) (ORACLE_HOME = /rdsdbbin/oracle)))`
	`L_VIS_001=(DESCRIPTION_LIST =`
	`(DESCRIPTION =`
	`(ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx.xx))) (DESCRIPTION =`
	`(ADDRESS = (PROTOCOL =`	

Tarefa	Descrição	Habilidades necessárias

	TCP)(PORT = 1521)(HOST = 127.0.0.1))))
	SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_VIS_001=OFF
	
	Para Oracle 19c: restaure o arquivo original `listener.ora` com o nome do receptorL_<INSTANCE_NAME>_001 .
	
	$ cd $ORACLE_HOME/network/admin
	
	$ cp -rp /rdsdbdata/config/listener.ora /rdsdbdata/config/listener.ora_autoconfig
	$ cp -rp /rdsdbdata/config/listener.ora_orig /rdsdbdata/config/listener.ora
	
	$ cat listener.ora
	SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_VISCDB_001=OFF
	ADR_BASE_L_VISCDB_001=/rdsdbdata/log/
	USE_SID_AS_SERVICE_L_VISCDB_001=ON
	L_VISCDB_001=(DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx.xx))) (DESCRIPTION = (ADDRESS = (PROTOCOL =	

Tarefa	Descrição	Habilidades necessárias

	TCP)(PORT = 1521)(HOST = 127.0.0.1))))
	SID_LIST_L_VISCDB_001=
	(SID_LIST = (SID_DESC
	= (SID_NAME = VISCDB)(G
	LOBAL_DBNAME = VISCDB)
	(ORACLE_HOME = /
	rdsdbbin/oracle)))
	
	Inicie o receptor L_<INSTAN CE_NAME>_001 para operações padrão do Amazon RDS:
	
	$ lsnrctl stop
	$ lsnrctl start
	L_VISCDB_001
	
	Para Oracle 12.1.0.2
	
	Edite o arquivo de ambiente do Oracle E-Business Suite para alterar o $TNS_ADMI N caminho para usar os arquivos TNS genéricos do Amazon RDS Custom. O arquivo de ambiente foi criado quando você executou o Autoconfig anteriormente. Edite a TNS_ADMIN variável removendo o <CONTEXT_ NAME> postfix.
	
	Note
	Você deve editar o arquivo de ambiente	

Tarefa	Descrição	Habilidades necessárias

	somente no Oracle 12.1.0.2, porque o home padrão para 19c é `$ORACLE_HOME/network/admin`, que é o mesmo padrão para o Amazon RDS Custom.
	
	Por exemplo, no Oracle 12.1.0.2, edite o arquivo:
	
	`$ vi $ORACLE_HOME/VIS_oebs-db01log.env`
	
	Mude o caminho de:
	
	`TNS_ADMIN="/rdsdbbin/oracle/network/admin/VIS_oebs-db01log"`
	`export TNS_ADMIN`
	
	para:
	
	`TNS_ADMIN="/rdsdbbin/oracle/network/admin"`
	`export TNS_ADMIN`
	
	Note
	Toda vez que você executa o Autoconfig, repita essa etapa para garantir que os arquivos TNS corretos	

Tarefa	Descrição	Habilidades necessárias
	estejam sendo usados. (somente 12.1.0.2).	
	Para Oracle 19c: 1. Altere o valor da variável de contexto da camada do banco de dados `s_cdb_tnsadmin` para `<ORACLE_HOME>/network/admin` em vez de`<ORACLE_HOME>/network/admin/<CONTEXT_NAME>` . **Note** Não atualize a variável de `s_db_tnsadmin` contexto. Salve-o como `<ORACLE_HOME>/network/admin/<CONTEXT_NAME>` . ``` $. $ORACLE_HOME/VIS_oebs-db01log.env $ vi $CONTEXT_FILE ``` 2. Salve as alterações feitas no valor des`_cdb_tnsadmin` .	

Tarefa	Descrição	Habilidades necessárias

	Os valores de `s_db_tnsadmin` e `s_cdb_tnsadmin` devem ser semelhantes aos seguintes, com o nome do PDB como `VIS` e o nome lógico do nó do banco de dados como`oebs-db01log` .
	
	`$ grep -i tns_admin $CONTEXT_FILE`
	`<TNS_ADMIN oa_var="s_db_tnsadmin">/rdsdbbin/oracle/network/admin/VIS_oebs-db01log</TNS_ADMIN>`
	`<CDB_TNS_ADMIN oa_var="s_cdb_tnsadmin">/rdsdbbin/oracle/network/admin</CDB_TNS_ADMIN>`
	
	3. Execute o Autoconfig na camada do banco de dados:
	
	`$ . $ORACLE_HOME/VISCDB_oebs-db01log.env`
	`$ export ORACLE_PDB_SID=VIS`
	`$ sqlplus "/ as sysdba" @$ORACLE_HOME/appsutil/admin/adgrants.sql APPS`
	`$ sqlplus "/ as sysdba" @$ORACLE_HOME/rdbms/admin/utlrp.sql`
	
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env`	

Tarefa	Descrição	Habilidades necessárias
	``` $ echo $ORACLE_SID VIS $ cd $ORACLE_HOME/appsu til/scripts/$CONTE XT_NAME $ ./adautocfg.sh ```	

Tarefa	Descrição	Habilidades necessárias

Defina o ambiente para o usuário rdsdb.	Ignore esta etapa para o Oracle 19c.
	
	Para Oracle 12.1.0.2
	
	Agora que você concluiu as entradas do Autoconfig e do TNS, você precisa carregar o arquivo do ambiente configurando-o no perfil do `rdsdb` usuário.
	
	Atualize `.bash_profile` para chamar o `.env` arquivo de banco de dados do Oracle E-Business Suite. Você precisa atualizar o perfil para garantir que o ambiente seja carregado. O arquivo de ambiente foi criado quando você executou o Autoconfig anteriormente.
	
	O arquivo de ambiente de exemplo a seguir é criado quando você executa o Autoconfig:
	
	`. /rdsdbbin/oracle/VIS_oebs-db01log.env`
	
	Como usuário `rdsdb`:
	
	`cd $HOME`
	`vi .bash_profile`
		DBA

Tarefa	Descrição	Habilidades necessárias

	`export LD_LIBRARY_PATH=${ORACLE_HOME}/lib:${ORACLE_HOME}/ctx/lib`
	`export SHLIB_PATH=${ORACLE_HOME}/lib`
	`export PATH=$PATH:${ORACLE_HOME}/bin`
	`alias sql='rlwrap -c sqlplus / as sysdba'`
	`. ${ORACLE_HOME}/VIS_oebs-db01log.env`
	
	Note
	Para o Oracle 19c, você não precisa carregar o ambiente CDB. `.bash_profile` Isso ocorre porque o padrão `ORACLE_HOME` é definido como o caminho padrão`$ORACLE_HOME/network/admin`, que é a página inicial padrão do usuário `rdsdb` (Oracle home).	

Tarefa	Descrição	Habilidades necessárias
Configure o aplicativo e o banco de dados para o Amazon RDS Custom.	Conclua as duas primeiras etapas do Oracle 12.1.0.2 e do 19c. As etapas subsequentes são diferentes para cada versão. 1. No nível do aplicativo, edite `/etc/hosts` e altere o endereço IP do banco de dados para o endereço IP do Amazon RDS Custom: `xx.xx.xx.xx OEBS-db01.localdomain OEBS-db01 OEBS-db01log.localdomain OEBS-db01log` Como você está usando nomes de host lógicos, você pode substituir o nó do banco de dados quase sem problemas. 2. Na instância de banco de dados personalizada do Amazon RDS, adicione ou altere o grupo de segurança atribuído à instância de origem para refletir a EC2 instância de banco de dados personalizada do Amazon RDS, para garantir que o aplicativo possa acessar o nó. Para Oracle 12.1.0.2	DBA

Tarefa	Descrição	Habilidades necessárias

	3. Execute o Autoconfig. Como proprietário do aplicativo (por exemplo, `applmgr`), execute:
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adautocfg.sh`
	`AutoConfig completed successfully.`
	4. Verifique as `fnd_nodes` entradas:
	`SQL> select node_name from apps.fnd_nodes`
	`NODE_NAME`
	`----------`
	`AUTHENTICATION`
	`OEBS-APP01LOG`
	`OEBS-DB01LOG`
	5. Confirme que você pode fazer login e inicie o aplicativo:
	`$ ./adstrtal.sh`
	Para Oracle 19c:
	1. Verifique se o PDB está aberto e abra-o, se necessário:	

Tarefa	Descrição	Habilidades necessárias

	`SQL> show pdbs`
	
	`CON_ID CON_NAME OPEN MODE RESTRICTED`
	`---------- --------- ---------- ---------- ----------`
	`2 PDB$SEED READ ONLY NO`
	`3 VIS MOUNTED`
	
	`SQL> alter session set container=vis;`
	
	`SQL> alter database open;`
	
	`SQL> alter database save state;`
	
	2. Teste a conectividade como apps:
	
	`SQL> sqlplus apps/**** @vis`
	
	3. Execute o Autoconfig na camada do banco de dados:
	
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env`
	`$ echo $ORACLE_SID`
	`VIS`
	
	`$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`
	`$ ./adautocfg.sh`	

Tarefa	Descrição	Habilidades necessárias

	4. Execute o Autoconfig na camada do aplicativo como proprietário do aplicativo (por exemplo,`applmgr`):
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adautocfg.sh`
	`AutoConfig completed successfully.`
	5. Verifique as `fnd_nodes` entradas:
	`SQL> select node_name from apps.fnd_nodes`
	`NODE_NAME`
	`----------`
	`AUTHENTICATION`
	`OEBS-APP01LOG`
	`OEBS-DB01LOG`
	6. Iniciar o aplicativo
	`$ ./adstrtal.sh`	

Execute etapas de pós-migração

Tarefa	Descrição	Habilidades necessárias

Retome a automação para confirmar se ela funciona.	Reinicie a automação usando o seguinte comando da CLI da AWS:
	`aws rds modify-db-instance \ --db-instance-identifier vis \ --automation-mode full \`
	O banco de dados agora é gerenciado pelo Amazon RDS Custom. Por exemplo, se o receptor ou o banco de dados ficarem inativos, o agente do Amazon RDS Custom os reiniciará. Para testar isso, execute os comandos a seguir.
	Exemplo de interrupção do receptor:
	`-bash-4.2$ lsnrctl stop vis`
	Exemplo de desligamento do banco de dados:
	`SQL> shutdown immediate ;`
		DBA

Tarefa	Descrição	Habilidades necessárias
Valide o esquema, as conexões e as tarefas de manutenção.	Para finalizar a migração, é necessário executar as seguintes tarefas no mínimo. • Execute `FS_CLONE` para sincronizar o sistema de arquivos de patch. • Colete estatísticas do esquema. • Garanta que interfaces e sistemas externos possam se conectar ao novo banco de dados Amazon RDS Custom. • Configure seus backups e cronogramas de manutenção. • Verifique se o AD Online Patching (ADOP) está funcionando conforme o esperado emitindo uma substituição para alternar os sistemas de arquivos.	DBA

Solução de problemas

Problema	Solução
Você recebe um erro ORA-01624 ao tentar eliminar os arquivos de log.	Se você receber um erro ORA-01624 ao tentar eliminar os arquivos de log, siga estas etapas. Execute o comando a seguir e aguarde até que o status dos arquivos de log que você deseja eliminar seja`INACTIVE`. Para ter mais

Problema	Solução

	informações sobre os códigos de status, `V $log`consulte a documentação da Oracle. Este é um exemplo do comando e sua saída:
	
	`SQL> select group#, status from v$log;`
	
	`GROUP# STATUS`
	`---------- ----------`
	`1 ACTIVE`
	`2 CURRENT`
	`3 UNUSED`
	`4 UNUSED`
	`5 UNUSED`
	`6 UNUSED`
	`6 rows selected.`
	
	Neste exemplo, o arquivo de log 1 é`ACTIVE`, então você precisa forçar uma troca de arquivo de log três vezes para garantir que o primeiro novo arquivo de log adicionado anteriormente tenha o status de`CURRENT`:
	
	`SQL> alter system switch logfile;`
	`System altered.`
	`SQL> alter system switch logfile;`
	`System altered.`
	`SQL> alter system switch logfile;`
	`System altered.`
	
	Espere até que todos os arquivos de log que você deseja descartar estejam`INACTIVE`, como no exemplo a seguir, e execute o `DROP LOGFILE` comando.
	
	`SQL> select group#, status from v$log;`
	`GROUP# STATUS`
	`---------- ----------`
	`1 INACTIVE`

Problema	Solução
	2 INACTIVE 3 INACTIVE 4 CURRENT 5 UNUSED 6 UNUSED 6 rows selected.
Você recebe um erro ORA-00392 ao abrir o banco de dados com `resetlogs` .	Se você receber o erro ORA-00392: o log xx do thread 1 está sendo apagado, a operação não é permitida, execute o seguinte comando (`xx`substitua pelo número do arquivo de log) e execute novamente o comando open: `resetlogs` SQL> alter database clear logfile group xx; SQL> alter database open resetlogs;

Problema	Solução

Você tem problemas para se conectar ao aplicativo usando o Sysadmin ou o usuário do aplicativo.	Execute a seguinte consulta SQL para confirmar o problema:
	
	`SQL> select dbms_java.get_jdk_ version() from dual;`
	`select dbms_java.get_jdk_version()`
	` from dual`
	` ERROR at line 1:`
	`ORA-29548: Java system class reported:`
	` release of Java system classes in the database (19.0.0.0.220719 1.8) does`
	` not match that of the oracle executabl e (19.0.0.0.0 1.8)`
	
	Causa raiz: o banco de dados de origem foi aplicado com vários patches, mas o Amazon RDS Custom `DB_HOME` é uma instalação nova ou o CEV não incluiu todos os patches porque você não usou os patches de RSU necessários, como o OJVM, ao criar o CEV. Para validar isso, verifique se os detalhes do patch de origem estão listados em `$ORACLE_HOME/sqlpath` , `$ORACLE_HOME/.patch_storage` e `opatch – lsinventory` .
	
	Referência: datapatch - verbose falha com erro: “Patch xxxxxx: o diretório de patch arquivado está vazio” (ID do documento 2235541.1)
	
	Correção: copie os arquivos ausentes relacionados ao patch da fonte (`$ORACLE_HOME/sqlpatch/`) para o Amazon RDS Custom (`$ORACLE_HOME/sqlpatch/`) e, em seguida, execute novamente `./datapatch -verbose`.
	
	Por exemplo:

Problema	Solução

	`-bash-4.2$ cp -rp 18793246 20204035 20887355 22098146 22731026 $ORACLE_HOME/sqlpatch/`
	
	Como alternativa, você pode usar uma solução alternativa executando o seguinte comando no CDB e no PDB:
	
	`@?/javavm/install/update_javavm_db.sql`
	
	Em seguida, execute o seguinte comando no PBD:
	
	`sql> alter session set container=vis; @?/javavm/install/update_javavm_db.sql`
	
	Agora, execute o teste novamente:
	
	`SQL> select dbms_java.get_jdk_version() from dual;`

Recursos relacionados

- Trabalhando com o Amazon RDS Custom (Documentação do Amazon RDS)
- Amazon RDS Custom para Oracle: novos recursos de controle no ambiente de banco de dados (blog de notícias da AWS)
- Integre o Amazon RDS Custom for Oracle com o Amazon EFS (blog do banco de dados da AWS)
- Migração do Oracle E-Business Suite na AWS (whitepaper da AWS)
- Arquitetura do Oracle E-Business Suite na AWS (whitepaper da AWS)
- Configure uma arquitetura de HA/DR para o Oracle E-Business Suite no Amazon RDS Custom com um banco de dados ativo em espera (Recomendações da AWS)

Mais informações

Operações de manutenção

Corrigindo a página inicial do banco de dados do Oracle E-Business Suite com novos patches

Como o volume do compartimento (`/rdsdbbin`) é um out-of-place upgrade, o conteúdo do volume do compartimento é descartado durante o upgrade do CEV. Portanto, você precisa criar uma cópia do `appsutil` diretório antes de realizar qualquer atualização usando o CEV.

Na instância do Amazon RDS Custom de origem, antes de atualizar o CEV, faça um backup do `$ORACLE_HOME/appsutil`.

> **Note**
>
> Este exemplo usa um volume NFS. No entanto, em vez disso, você pode usar uma cópia para o Amazon Simple Storage Service (Amazon S3).

1. Crie um diretório para armazenar o appsutil na instância do Amazon RDS Custom de origem:

```
$ mkdir /RMAN/appsutil.preupgrade
```

2. Passe o cursor e copie para o volume do Amazon EFS:

```
$ tar cvf /RMAN/appsutil.preupgrade appsutil
```

3. Verifique se o arquivo tar existe:

```
$ bash-4.2$ ls -l /RMAN/appsutil.preupgrade
-rw-rw-r-- 1 rdsdb rdsdb 622981120 Feb  8 20:16 appsutil.tar
```

4. Atualize para o CEV mais recente (o CEV de pré-requisito já foi criado) seguindo as instruções em Atualização de uma instância de banco de dados personalizada do RDS na documentação do Amazon RDS).

Você também pode corrigir diretamente usando o OPATCH. Consulte a seção Requisitos e considerações para o RDS Custom for Oracle Upgrades da documentação do Amazon RDS.

> **Note**
>
> O endereço IP da máquina host não muda durante o processo de correção do CEV. Esse processo realiza uma out-of-place atualização e, durante a inicialização, um novo volume de compartimento é anexado à mesma instância.

Migre o Oracle PeopleSoft para o Amazon RDS Custom

Criado por Gaurav Gupta (AWS)

Resumo

PeopleSoftO Oracle é uma solução de planejamento de recursos corporativos (ERP) para processos em toda a empresa. PeopleSoft tem uma arquitetura de três camadas: cliente, aplicativo e banco de dados. PeopleSoft pode ser executado no Amazon Relational Database Service (Amazon RDS). Agora, você também pode executar PeopleSoft no Amazon RDS Custom, que fornece acesso ao sistema operacional subjacente.

O Amazon RDS Custom para Oracle é um serviço de banco de dados gerenciado para aplicações herdadas, personalizadas e em pacote que exigem acesso ao sistema operacional subjacente e ao ambiente de banco de dados. Quando você migra seu banco de dados Oracle para o Amazon RDS Custom, o Amazon Web Services (AWS) pode gerenciar tarefas de backup e alta disponibilidade, enquanto você pode se concentrar na manutenção de seu PeopleSoft aplicativo e funcionalidade. Para ver os principais fatores a considerar em uma migração, consulte as Estratégias de migração do banco de dados Oracle no Recomendações da AWS.

Esse padrão se concentra nas etapas para migrar um PeopleSoft banco de dados no Amazon Elastic Compute Cloud (Amazon EC2) para o Amazon RDS Custom usando um backup do Oracle Recovery Manager (RMAN). Ele usa um sistema de arquivos compartilhado do Amazon Elastic File System (Amazon EFS) entre a EC2 instância e o Amazon RDS Custom, embora você também possa usar o Amazon FSx ou qualquer drive compartilhado. O padrão usa um backup completo do RMAN (às vezes chamado de backup de nível 0).

Pré-requisitos e limitações

Pré-requisitos

- Um banco de dados de origem Oracle versão 19C que está sendo executado na Amazon EC2 com Oracle Linux 7, Oracle Linux 8, Red Hat Enterprise Linux (RHEL) 7 ou RHEL 8. Nos exemplos desse padrão, o nome do banco de dados de origem é `FSDM092`, mas isso não é um requisito.

> **Note**
>
> Você também pode usar esse padrão com bancos de dados de origem Oracle locais. É necessário ter a conectividade de rede adequada entre a rede on-premises e uma nuvem privada virtual (VPC).

- Uma instância de demonstração PeopleSoft 9.2.
- Um único nível PeopleSoft de aplicativo. No entanto, você pode adaptar esse padrão para trabalhar com vários níveis de aplicativos.
- Amazon RDS Custom configurado com pelo menos 8 GB de espaço de troca.

Limitações

Esse padrão não é compatível com as seguintes configurações:

- Definindo o parâmetro `ARCHIVE_LAG_TARGET` do banco de dados para um valor fora do intervalo de 60 a 7200
- Desabilitando o modo de log da instância de banco de dados (`NOARCHIVELOG`)
- Desativando o atributo otimizado Amazon Elastic Block Store (Amazon EBS) da instância EC2
- Modificando os volumes originais do EBS anexados à instância EC2
- Adicionar novos volumes do EBS ou alterar o tipo de volume de gp2 para gp3
- Alterar o formato da extensão para o parâmetro `LOG_ARCHIVE_FORMAT` (obrigatório `*.arc`)
- Multiplexar ou alterar a localização e o nome do arquivo de controle (tem que ser `/rdsdbdata/db/*DBNAME*/controlfile/control-01.ctl`)

Para obter informações adicionais sobre essas e outras configurações não suportadas, consulte a documentação do Amazon RDS.

Versões do produto

Para versões do banco de dados Oracle e classes de instância suportadas pelo Amazon RDS Custom, consulte Requisitos e limitações do Amazon RDS Custom for Oracle.

Arquitetura

Pilha de tecnologias de destino

- Application Load Balancer
- Amazon EFS
- Amazon RDS Custom para Oracle
- AWS Secrets Manager

- Amazon Simple Storage Service (Amazon S3)

Arquitetura de destino

O diagrama de arquitetura a seguir representa um PeopleSoft sistema em execução em uma única zona de disponibilidade na AWS. Não é possível acessar o aplicativo por meio de um Application Load Balancer. Tanto o aplicativo quanto os bancos de dados estão em sub-redes privadas, e a instância de EC2 banco de dados Amazon RDS Custom e Amazon usam um sistema de arquivos compartilhado Amazon EFS para armazenar e acessar os arquivos de backup do RMAN. O Amazon S3 é usado para criar o mecanismo Oracle RDS personalizado e para armazenar os metadados de logs redo.

Ferramentas

Ferramentas

Serviços da AWS

- O Amazon RDS Custom para Oracle é um serviço de banco de dados gerenciado para aplicações herdadas, personalizadas e em pacote que exigem acesso ao sistema operacional subjacente e ao ambiente de banco de dados. Ele automatiza as tarefas de administração do banco de dados, como backups e alta disponibilidade.
- O Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS. Esse padrão usa um sistema de arquivos compartilhado Amazon EFS para armazenar e acessar os arquivos de backup do RMAN.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente. Nesse padrão, você recupera as senhas de usuário do banco de dados do Secrets Manager para criar os usuários `RDSADMIN` e `ADMIN`, e alterar as senhas `sys` e `system`.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade. Este padrão usa um Application Load Balancer.

Outras ferramentas

- O Oracle Recovery Manager (RMAN) fornece suporte de backup e recuperação para bancos de dados Oracle. Esse padrão usa o RMAN para realizar um backup dinâmico do banco de dados Oracle de origem na Amazon, EC2 que é restaurado no Amazon RDS Custom.

Práticas recomendadas

- Para parâmetros de inicialização do banco de dados, personalize o perfil padrão fornecido pela instância de banco de dados personalizada do Amazon RDS PeopleSoft em vez de usar o spfile do banco de dados de origem Oracle. Isso ocorre porque espaços em branco e comentários causam problemas ao criar réplicas de leitura no Amazon RDS Custom. Para obter mais informações sobre os parâmetros de inicialização do banco de dados, consulte a Observação de Suporte Oracle 1100831.1 (requer uma conta do Oracle Support).
- O Amazon RDS Custom usa o gerenciamento automático de memória Oracle por padrão. Se quiser usar o kernel Hugemem, você pode configurar o Amazon RDS Custom para usar o gerenciamento automático de memória compartilhada em vez disso.
- Deixe o `memory_max_target` parâmetro habilitado por padrão. A estrutura usa isso em segundo plano para criar réplicas de leitura.
- Ative o banco de dados Oracle Flashback. Esse atributo é útil ao restabelecer o modo de espera em cenários de teste de failover (não transição).

Épicos

Configurar a instância de banco de dados e o sistema de arquivos

Tarefa	Descrição	Habilidades necessárias
Criar a instância de banco de dados.	No console do Amazon RDS, crie uma instância de banco de dados Amazon RDS Custom for Oracle com um nome de banco de dados chamado FSDMO92 (ou o nome do seu banco de dados de origem).	DBA

Tarefa	Descrição	Habilidades necessárias
	Para obter instruções, consulte Como trabalhar com o Amazon RDS Custom na documentação da AWS e a postagem do blog Amazon RDS Custom for Oracle: New Control Capabilities in Database Environment. Isso garante que o nome do banco de dados seja definido com o mesmo nome do banco de dados de origem. (Se mantido em branco, o nome da EC2 instância e do banco de dados será definido como`ORCL`.)	

Execute um backup completo do RMAN do banco de dados de origem da Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Crie um script de backup.	Crie um script de backup RMAN para fazer backup do banco de dados no sistema de arquivos Amazon EFS que você montou (`/efs`no exemplo a seguir). Você pode usar o código de exemplo ou executar um dos scripts RMAN existentes. `#!/bin/bash` `Dt=`date +'%Y%m%d-%H` `%M'` `BACKUP_LOG="rman-${O` `RACLE_SID}-$Dt"`	DBA

Tarefa	Descrição	Habilidades necessárias
	export TAGDATE=`date + %Y%m%d%H%M`; LOGPATH=/u01/scripts/l ogs rman target / >> $LOGPATH/rman-${OR ACLE_SID}-$Dt << EOF SQL "ALTER SYSTEM SWITCH LOGFILE"; SQL "ALTER SESSION SET NLS_DATE_FORMAT="D D.MM.YYYY HH24:MI:S S""; RUN { ALLOCATE CHANNEL ch11 TYPE DISK MAXPIECESIZE 5G; ALLOCATE CHANNEL ch12 TYPE DISK MAXPIECESIZE 5G; BACKUP AS COMPRESSED BACKUPSET FULL DATABASE FORMAT '/efs/rma n_backup/FSCM/%d_%T_ %s_%p_FULL' ; SQL "ALTER SYSTEM ARCHIVE LOG CURRENT"; BACKUP FORMAT '/efs/ rman_backup/FSCM/%d_ %T_%s_%p_ARCHIVE' ARCHIVELOG ALL DELETE ALL INPUT ; BACKUP CURRENT CONTROLFILE FORMAT '/ efs/rman_backup/FSCM/ %d_%T_%s_%p_CONTROL'; } EXIT; EOF	

Tarefa	Descrição	Habilidades necessárias

Execute o script de backup.	Para executar o script de backup do RMAN, faça login como Oracle Home User e execute o script.
	`$  chmod a+x rman_backup.sh`
	`$ ./rman_backup.sh &`
		DBA

Tarefa	Descrição	Habilidades necessárias

Verifique se há erros e anote o nome do arquivo de backup.	Verifique se há erros no arquivo de log RMAN. Se tudo estiver bem, liste o backup do arquivo de controle executando o comando a seguir.
	`RMAN> list backup of controlfile;`
	`using target database control file instead of recovery catalog`
	Anote o nome do arquivo de saída.
	`List of Backup Sets`
	`==========`
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`12 Full 21.58M DISK 00:00:01 13-JUL-22`
	`BP Key: 12 Status: AVAILABLE Compressed: NO Tag: TAG20220713T150155`
	`Piece Name: /efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL`
	`Control File Included: Ckp SCN: 165591599`
		DBA

Tarefa	Descrição	Habilidades necessárias
	`85898 Ckp time: 13-JUL-22` Você usará o arquivo de controle de backup `/efs/rman_backup/FSCM/FSDM092_20220713_12_1_CONTROL` ao restaurar o banco de dados no Amazon RDS Custom.	

Encerre o nível do aplicativo de origem

Tarefa	Descrição	Habilidades necessárias

Feche o aplicativo.	Para desligar a camada do aplicativo de origem, use o utilitário `psadmin` ou o utilitário de linha de comando `psadmin`.
	
	1. Para desligar o servidor web, execute o comando a seguir.
	
	`psadmin -w shutdown -d "webserver domain name"`
	
	2. Para desligar o servidor de aplicativo, execute o comando a seguir.
	
	`psadmin -c shutdown -d "application server domain name"`
		DBA, administrador PeopleSoft

Tarefa	Descrição	Habilidades necessárias
	3. Para encerrar o programador de processos, execute o comando a seguir. `psadmin -p stop -d "process scheduler domain name"`	

Configurar o banco de dados do Amazon RDS Custom de destino

Tarefa	Descrição	Habilidades necessárias
Instale o pacote rpm nfs-utils.	Para instalar o pacote `nfs-utils rpm`, execute o seguinte comando. `$ yum install -y nfs-utils`	DBA
Monte o armazenamento EFS.	Obtenha o comando de montagem do Amazon EFS na página do console do Amazon EFS. Monte o sistema de arquivos EFS na instância do Amazon RDS usando um cliente de Sistema de arquivos de rede (NFS). `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-xxxxxxxxxx.efs.eu-west-1.amazonaws.com:/ /efs`	DBA

Tarefa	Descrição	Habilidades necessárias
	`sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-xxxxxxxxxx.efs.eu-west-1.amazonaws.com:/ /efs`	

Elimine o banco de dados inicial e crie os diretórios para armazenar os arquivos do banco de dados

Tarefa	Descrição	Habilidades necessárias
Pausar o modo de automação.	Você precisa pausar o modo de automação em sua instância de banco de dados do Amazon RDS Custom antes de prosseguir com as próximas etapas, para garantir que a automação não interfira na atividade de restauração do RMAN. É possível pausar a automação usando o console da AWS ou o comando AWS Command Line Interface (AWS CLI) (AWS CLI) (certifique-se de configurar a AWS CLI primeiro). `aws rds modify-db-instance \ --db-instance-id entifier peoplesoft-fscm-92 \`	DBA

Tarefa	Descrição	Habilidades necessárias

	`--automation-mode all-paused \`
	`--resume-full-automation-mode-minute 360 \`
	`--region eu-west-1`
	
	Ao especificar a duração da pausa, certifique-se de deixar tempo suficiente para a restauração do RMAN. Isso depende do tamanho do banco de dados de origem, portanto modifique o valor 360 devidamente.
	
	Além disso, certifique-se de que o tempo total da automação pausada não se sobreponha à janela de backup ou manutenção do banco de dados.	

Tarefa	Descrição	Habilidades necessárias

Crie e modifique o arquivo de parâmetros para PeopleSoft	Para criar e modificar o pfile para PeopleSoft, use o pfile padrão criado com a instância de banco de dados personalizada do Amazon RDS. Adicione os parâmetros necessários PeopleSoft.
	
	1. Alterne para `rds user rdsdb` ao executar o seguinte comando.
	
	`$ sudo su - rdsdb`
	
	2. Faça login no SQL*Plus no banco de dados inicial e crie o pfile executando o comando a seguir.
	
	`SQL> create pfile from spfile;`
	
	Isso cria o perfil em `$ORACLE_HOME/dbs` .
	
	3. Faça um backup desse arquivo.
	4. Edite o arquivo para adicionar ou atualizar PeopleSoft parâmetros.
	
	`*._gby_hash_aggregation_enabled=false`
	
	`*._unnest_subquery=false`
		DBA

Tarefa	Descrição	Habilidades necessárias

	`*.nls_language='AMERICAN'`
	
	`*.nls_length_semantics='CHAR'`
	
	`*.nls_territory='AMERICA'`
	
	`*.open_cursors=1000`
	
	`*.db_files=1200`
	
	`*.undo_tablespace='UNDOTBS1'`
	
	PeopleSoft os parâmetros relacionados podem ser encontrados na Nota de Suporte da Oracle 1100831.1.
	5. Remova a referência spfile do pfile.
	
	`*.spfile='/rdsdbbin/oracle/dbs/spfileFSDMO92.ora'`	

Tarefa	Descrição	Habilidades necessárias

Remova o banco de dados inicial.	Para remover o banco de dados Amazon RDS Custom existente, use o código a seguir.
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate ;`
	`SQL> startup mount exclusive restrict;`
	`SQL> drop database;`
	`SQL> exit`	

Tarefa	Descrição	Habilidades necessárias
Restaure o banco de dados do Amazon RDS Custom a partir do backup.	Restaure o banco de dados usando o script a seguir. O script primeiro restaurará o arquivo de controle e, em seguida, restaurará todo o banco de dados a partir das partes de backup armazenadas na montagem do EFS. `#!/bin/bash` `Dt=`date +'%Y%m%d-%H%M'` `BACKUP_LOG="rman-${ORACLE_SID}-$Dt"` `export TAGDATE=`date +%Y%m%d%H%M`;` `LOGPATH=/rdsdbdata/scripts/logs` `rman target / >> $LOGPATH/rman-${ORACLE_SID}-$Dt << EOF` `restore controlfile from "/efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL";` `alter database mount;` `run` `{` `set newname for database to '/rdsdbdata/db/FSDMO92_A/datafile/%f_%b';` `SET NEWNAME FOR TEMPFILE 1 TO '/rdsdbdata/db/FSDMO92_A/datafile/%f_%b';` `RESTORE DATABASE;` `SWITCH DATAFILE ALL;` `SWITCH TEMPFILE ALL;`	DBA

Tarefa	Descrição	Habilidades necessárias
	RECOVER DATABASE; } EOF sqlplus / as sysdba >> $LOGPATH/rman-${OR ACLE_SID}-$Dt<<-EOF ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 1.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo01.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 2.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo02.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 3.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo03.log'; alter database clear unarchived logfile group 1; alter database clear unarchived logfile group 2; alter database clear unarchived logfile group 3; alter database open resetlogs; EXIT EOF	

Recupere as senhas do Secrets Manager, crie usuários e altere senhas

Tarefa	Descrição	Habilidades necessárias
Recupere a senha do Secrets Manager.	É possível executar esta etapa usando o console da AWS ou a CLI da AWS. As etapas a seguir mostram instruções para o console. 1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon RDS. 2. No painel de navegação, escolha Databases (Bancos de dados) e, depois, selecione o banco de dados Amazon RDS. 3. Selecione a guia Configuração e anote o ID do recurso para a instância de banco de dados. Esse procedimento estará no formato `db-<ID>`, (por exemplo, `db-73GJNHLGDNZNDOXNWXSECUW6LE`). 4. Abra o console do Secrets Manager. 5. Escolha o segredo que tem o mesmo nome de `do-not-delete-custom-<resource_id>` , sendo que `resource-id` se refere ao ID do recurso que você anotou na etapa 3.	DBA

Tarefa	Descrição	Habilidades necessárias
	6. Escolha Recuperar valor do segredo. Essa senha será a mesma para os usuários `sys`, `system`, `rdsadmin` e `admin`.	

Tarefa	Descrição	Habilidades necessárias

Crie o usuário RDSADMIN.	`RDSADMIN` é o usuário do banco de dados para monitorar e orquestrar a instância de banco de dados do Amazon RDS Custom. Como o banco de dados inicial foi descartado e o banco de dados de destino foi restaurado da origem usando o RMAN, você deverá recriar esse usuário após a operação de restauração para garantir que o monitoramento do Amazon RDS Custom funcione conforme o esperado. Você também precisa criar um perfil e um espaço de tabela separados para o usuário `RDSADMIN`.
	
	1. Insira o seguinte comando no prompt SQL.
	
	`SQL> set echo on feedback on serverout on`
	`SQL> @?/rdbms/admin/utlpwdmg.sql`
	`SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL;`
		DBA

Tarefa	Descrição	Habilidades necessárias
	2. Criar o perfil RDSADMIN. `SQL> set echo on feedback on serverout on SQL> alter session set "_oracle_script"=t rue; SQL> CREATE PROFILE RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER _CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTE MPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400`	

Tarefa	Descrição	Habilidades necessárias
	PASSWORD_GRACE_TIME 604800/86400; 3. Crie o espaço de tabela RDSADMIN. SQL> CREATE BIGFILE TABLESPACE rdsadmin '/rdsdbdata/db/FSD MO92_A/datafile/rd sadmin.dbf' DATAFILE SIZE 7M AUTOEXTEND ON NEXT 1m LOGGING ONLINE PERMANENT BLOCKSIZE 8192 EXTENT MANAGEMEN T LOCAL AUTOALLOCATE DEFAULT NOCOMPRES S SEGMENT SPACE MANAGEMENT AUTO; 4. Criar o usuário RDSADMIN Substitua a senha RDSADMIN pela senha que você obteve anteriormente no Secrets Manager. SQL> CREATE USER rdsadmin IDENTIFIED BY xxxxxxxxxx DEFAULT TABLESPACE rdsadmin TEMPORARY TABLESPACE TEMP profile rdsadmin ; 5. Conceda privilégios ao RDSADMIN.	

Tarefa	Descrição	Habilidades necessárias
	``` SQL> GRANT "CONNECT" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "RESOURCE " TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "DBA" TO RDSADMIN; SQL> GRANT "SELECT_C ATALOG_ROLE" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT ALTER SYSTEM TO RDSADMIN; SQL> GRANT UNLIMITED TABLESPACE TO RDSADMIN; SQL> GRANT SELECT ANY TABLE TO RDSADMIN; SQL> GRANT ALTER DATABASE TO RDSADMIN; SQL> GRANT ADMINISTER DATABASE TRIGGER TO RDSADMIN; SQL> GRANT ANY OBJECT PRIVILEGE TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT INHERIT ANY PRIVILEGES TO RDSADMIN; SQL> ALTER USER RDSADMIN DEFAULT ROLE ALL; ``` 6. Set the SYS, SYSTEM, and DBSNMP user profiles to RDSADMIN.	

Tarefa	Descrição	Habilidades necessárias

	`SQL> set echo on`
	`feedback on serverout`
	`on`
	`SQL> alter user SYS`
	`profile RDSADMIN;`
	`SQL> alter user SYSTEM`
	`profile RDSADMIN;`
	`SQL> alter user DBSNMP`
	`profile RDSADMIN;`	

Crie o usuário mestre.	Como o banco de dados inicial foi descartado e o banco de dados de destino foi restaurado da origem usando o RMAN, você deverá recriar o usuário mestre. Neste exemplo, o nome do usuário mestre é `admin`.
	`SQL> create user`
	`admin identified by`
	`<password>;`
	`SQL> grant dba to admin`
		DBA

Tarefa	Descrição	Habilidades necessárias

Alterar as senhas do sistema.	Altere as senhas do sistema usando a senha que você recuperou do Secrets Manager.
	`SQL> alter user sys identified by xxxxxxxxxx;`
	`SQL> alter user system identified by xxxxxxxxxx;`
	Se você não alterar essas senhas, o Amazon RDS Custom exibirá a mensagem de erro “O usuário de monitoramento do banco de dados ou as credenciais do usuário foram alteradas”.
		DBA

Configure as entradas de TNS para Amazon RDS Custom e PeopleSoft

Tarefa	Descrição	Habilidades necessárias
Configure o arquivo tnsnames.	Para se conectar ao banco de dados a partir da camada do aplicativo, configure o arquivo `tnsnames.ora` para que você possa se conectar ao banco de dados a partir da camada do aplicativo. No exemplo a seguir, você pode ver que há um link virtual para o `tnsnames.ora` arquivo,	DBA

Tarefa	Descrição	Habilidades necessárias

	mas o arquivo está vazio por padrão.
	
	`$ cd /rdsdbbin/oracle/network/admin`
	`$ ls -ltr`
	`-rw-r--r-- 1 rdsdb database 1536 Feb 14 2018 shrept.lst`
	`lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 listener.ora -> /rdsdbdata/config/listener.ora`
	`lrwxrwxrwx 1 rdsdb database 28 Apr 5 13:19 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora`
	`lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora`
	
	1. Crie a entrada `tsnames.ora` . Devido à forma como a automação do Amazon RDS analisa os arquivos, você precisa garantir que a entrada não contenha espaços em branco, comentários ou linhas extras. Caso contrário, você poderá ter problemas ao usar alguns dos APIs, como create-db-instance-read - replica.	

Tarefa	Descrição	Habilidades necessárias

	2. Substitua a porta, o host e o SID de acordo com os requisitos do seu PeopleSoft banco de dados. Use o código a seguir como um exemplo.
	
	`$ vi tnsnames.ora`
	
	`FSDMO92=(DESCRIP TION = (ADDRESS_ LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_ DATA = (SERVER = DEDICATED) (SID = FSDMO92)))`
	
	3. Para confirmar que o PeopleSoft banco de dados pode ser acessado, execute o comando a seguir.
	
	`$ tnsping FSDMO92`
	
	`TNS Ping Utility for Linux: Version 19.0.0.0.0 - Production on 14-JUL-2022 10:16:45`
	
	`Copyright (c) 1997, 2021, Oracle. All rights reserved.`
	
	`Used parameter files: /rdsdbbin/oracle/network/admin/sqlnet.ora`	

Tarefa	Descrição	Habilidades necessárias
	Used TNSNAMES adapter to resolve the alias Attempting to contact (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_DATA = (SERVER = DEDICATED) (SID = FSDMO92))) OK (0 msec)	

Crie o softlink spfile

Tarefa	Descrição	Habilidades necessárias

Crie o softlink spfile.	1. Para criar spfile no local `/rdsdbdata/admin/FSDMO92/pfile` , execute o comando a seguir.
	`SQL> create spfile='/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' from pfile;`
	2. Navegue até `$ORACLE_HOME/dbs` , e crie um link virtual para o spfile.
	`ln -s '/rdsdbdata/admin/FSDMO92/pfile/`
		DBA

Tarefa	Descrição	Habilidades necessárias
	`spfileFSDMO92.ora' spfileFSDMO92.ora` 3. Depois que esse arquivo for criado, você poderá desligar e iniciar o banco de dados usando o spfile.	

Execute etapas de pós-migração

Tarefa	Descrição	Habilidades necessárias
Valide o esquema, as conexões e as tarefas de manutenção.	Para finalizar a migração, realize as tarefas a seguir. • Colete estatísticas do esquema. • Certifique-se de que o nível do PeopleSoft aplicativo possa se conectar ao novo banco de dados personali zado do Amazon RDS. • Configure seus cronogram as de backup e manutençã o.	DBA

Recursos relacionados

- Trabalhar com o Amazon RDS Custom
- Amazon RDS Custom para Oracle: novos recursos de controle no ambiente de banco de dados (publicação no blog)
- Integre o Amazon RDS Custom for Oracle com o Amazon EFS (publicação no blog)
- Configurando o Amazon RDS como um PeopleSoft banco de dados Oracle (whitepaper da AWS)

Migre a funcionalidade Oracle ROWID para o PostgreSQL na AWS

Criado por Rakesh Raghav (AWS) e Ramesh Pathuri (AWS)

Resumo

Esse padrão descreve as opções para migrar a funcionalidade de `ROWID` pseudocoluna no Oracle Database para um banco de dados PostgreSQL no Amazon Relational Database Service (Amazon RDS) para PostgreSQL, Amazon Aurora PostgreSQL Compatible Edition ou Amazon Elastic Compute Cloud (Amazon). EC2

Em um banco de dados Oracle, a pseudocoluna `ROWID` é o endereço físico de uma linha em uma tabela. Essa pseudocoluna é usada para identificar de forma exclusiva uma linha, mesmo que a chave primária não esteja presente em uma tabela. O PostgreSQL tem uma pseudocoluna similar chamada `ctid`, mas ela não pode ser usada como a `ROWID`. Conforme explicado na documentação do PostgreSQL, `ctid` pode mudar se for atualizado ou após cada processo `VACUUM`.

Há três maneiras de criar a funcionalidade de pseudocoluna `ROWID` no PostgreSQL:

- Use uma coluna de chave primária em vez de `ROWID` para identificar uma linha em uma tabela.
- Use uma chave lógica primária/exclusiva (que pode ser uma chave composta) na tabela.
- Adicione uma coluna com valores gerados automaticamente e torne-a uma chave primária/exclusiva para imitar `ROWID`.

Esse padrão mostra todas as três implementações e descreve as vantagens e desvantagens de cada opção.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Experiência em codificação (processualLanguage/PostgreSQL (PL/pgSQL)
- Origem: banco de dados Oracle
- Um cluster compatível com o Amazon RDS for PostgreSQL ou Aurora PostgreSQL, ou uma instância para hospedar o banco de dados PostgreSQL EC2

Limitações

- Esse padrão fornece soluções alternativas para a funcionalidade `ROWID`. O PostgreSQL não fornece um equivalente a `ROWID` do Oracle Database.

Versões do produto

- PostgreSQL 11.9 ou superior

Arquitetura

Pilha de tecnologia de origem

- Oracle Database

Pilha de tecnologias de destino

- Compatível com Aurora PostgreSQL, Amazon RDS for PostgreSQL ou uma instância com um banco de dados PostgreSQL EC2

Opções de implementação

Há três opções para contornar a falta de suporte de `ROWID` no PostgreSQL, dependendo se sua tabela tem uma chave primária ou um índice exclusivo, uma chave primária lógica ou um atributo de identidade. Sua escolha depende dos cronogramas do projeto, da fase atual de migração e das dependências do código do aplicativo e do banco de dados.

Opção	Descrição	Vantagens	Desvantagens
Chave primária ou índice exclusivo	Se sua tabela Oracle tiver uma chave primária, você poderá usar os atributos dessa chave para identificar uma linha de forma exclusiva.	• Sem dependência de atributos de banco de dados proprietários. • Impacto mínimo no desempenho, pois os campos da	• Requer alterações no código do aplicativo e do banco de dados que depende da mudança `ROWID` para campos de chave primária.

		chave primária são indexados.	
Chave lógica primária/ exclusiva	Se sua tabela Oracle tiver uma chave primária, lógica, você poderá usar os atributos dessa chave para identificar uma linha de forma exclusiva. Uma chave primária lógica consiste em um atributo ou conjunto de atributos que pode identificar uma linha de forma exclusiva, mas não é aplicada ao banco de dados por meio de uma restrição.	• Sem dependência de atributos de banco de dados proprietários.	• Requer alterações no código do aplicativo e do banco de dados que depende da mudança `ROWID` para campos de chave primária. • Impacto significativo no desempenho se os atributos da chave primária lógica não forem indexados. No entanto, você pode adicionar um índice exclusivo para evitar problemas de desempenho.

Atributo de identidade	se sua tabela Oracle não tiver uma chave primária, você poderá criar um campo adicional como `GENERATED ALWAYS AS IDENTITY`. Esse atributo gera um valor exclusivo sempre que os dados são inseridos na tabela, portanto, ele pode ser usado para identificar de forma exclusiva uma linha para operações de linguagem de manipulação de dados (DML).	• Sem dependência de atributos de banco de dados proprietários. • O banco de dados PostgreSQL preenche o atributo e mantém sua exclusividade.	• Requer alterações no código do aplicativo e do banco de dados que depende de `ROWID` para mudar para o atributo de identidade. • Impacto significativo no desempenho se o campo adicional não estiver indexado. No entanto, você pode adicionar um índice para evitar problemas de desempenho.

Ferramentas

- O Amazon Relational Database Service (Amazon RDS) para PostgreSQL ajuda você a configurar, operar e escalar um banco de dados relacional PostgreSQL na Nuvem AWS.
- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando. Nesse padrão, você pode usar a AWS CLI para executar comandos SQL por meio do pGADmin.
- O pgAdmin é uma ferramenta de gerenciamento de código aberto para PostgreSQL. Ele fornece uma interface gráfica que ajuda você a criar, manter e usar objetos de banco de dados.
- O AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.

Épicos

Identificar as tabelas de fontes

Tarefa	Descrição	Habilidades necessárias
Identifique as tabelas Oracle que usam o `ROWID` atributo.	Use a AWS Schema Conversion Tool (AWS SCT) para identificar tabelas Oracle que tenham a funcional idade `ROWID`. Para obter mais informações, consulte a documentação da AWS SCT. —ou— No Oracle, use a visualização `DBA_TAB_COLUMNS` para identificar tabelas que tenham um atributo `ROWID`. Esses campos podem ser usados para armazenar caracteres alfanuméricos de 10 bytes. Determine o uso e converta-os em um campo `VARCHAR`, se for apropriado.	DBA ou desenvolvedor
Identifique o código que faz referência a essas tabelas.	Use o AWS SCT para gerar um relatório de avaliação de migração para identific ar procedimentos afetados por `ROWID`. Para obter mais informações, consulte a documentação da AWS SCT. —ou— No banco de dados Oracle de origem, use o campo de texto	DBA ou desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	da tabela `dba_source` para identificar objetos que usam a funcionalidade `ROWID`.	

Determine o uso de chaves primárias

Tarefa	Descrição	Habilidades necessárias
Identifique tabelas que não têm chaves primárias.	No banco de dados Oracle de origem, use `DBA_CONSTRAINTS` para identificar tabelas que não têm chaves primárias. Essas informações ajudarão você a determinar a estratégia para cada tabela. Por exemplo: `select dt.* from dba_tables dt where not exists (select 1 from all_constraints ct where ct.owner = Dt.owner and ct.table_name = Dt.table_name and ct.constraint_type = 'P' ) and dt.owner = '{schema}'`	DBA ou desenvolvedor

Identifique e aplique a solução

Tarefa	Descrição	Habilidades necessárias
Aplique alterações em tabelas que tenham uma chave primária lógica ou definida.	Faça as alterações no código do aplicativo e do banco de dados mostradas na seção Informações adicionais para usar uma chave primária exclusiva ou uma chave primária lógica para identificar uma linha na tabela.	DBA ou desenvolvedor
Inclua um campo adicional às tabelas que não tenham uma chave primária lógica ou definida.	Adicione um atributo do tipo `GENERATED ALWAYS AS IDENTITY`. Faça as alteraçõe s no código do aplicativo e do banco de dados mostradas na seção de Informações adicionais.	DBA ou desenvolvedor
Adicione um índice, se necessário.	Inclua um índice ao campo adicional ou à chave primária lógica para melhorar o desempenho do SQL.	DBA ou desenvolvedor

Recursos relacionados

- PostgreSQL CTID (Documentação do PostgreSQL)
- Colunas geradas (Documentação do PostgreSQL)
- Pseudocoluna ROWID (Documentação da Oracle)

Mais informações

As seções a seguir fornecem códigos de exemplos Oracle e PostgreSQL para ilustrar as três abordagens.

Cenário 1: usar uma chave primária exclusiva

Nos exemplos a seguir, você cria a tabela `testrowid_s1` com `emp_id` como a chave primária.

Código Oracle:

```
create table testrowid_s1 (emp_id integer, name varchar2(10), CONSTRAINT testrowid_pk
 PRIMARY KEY (emp_id));
INSERT INTO testrowid_s1(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s1(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s1(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s1(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 empname2
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4

UPDATE testrowid_s1 SET name = 'Ramesh' WHERE rowid = 'AAAF3pAAAAAAAMOAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 Ramesh
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s1
(
    emp_id integer,
    name character varying,
    primary key (emp_id)
);

insert into public.testrowid_s1 (emp_id,name) values
```

```
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s1 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Cenário 2: usar uma chave primária lógica

Nos exemplos a seguir, você cria a tabela `testrowid_s2` com `emp_id` a chave primária.

Código Oracle:

```
create table testrowid_s2 (emp_id integer, name varchar2(10) );
INSERT INTO testrowid_s2(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s2(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s2(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s2(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 empname2
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4

UPDATE testrowid_s2 SET name = 'Ramesh' WHERE rowid = 'AAAF3rAAAAAAAMeAAB' ;
commit;
```

```
SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 Ramesh
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s2
(
    emp_id integer,
    name character varying
);

insert into public.testrowid_s2 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s2 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Cenário 3: usar um atributo de identidade

Nos exemplos a seguir, você cria a tabela `testrowid_s3` sem chave primária e usando um atributo de identidade.

Código Oracle:

```
create table testrowid_s3 (name varchar2(10));
INSERT INTO testrowid_s3(name) values ('empname1');
INSERT INTO testrowid_s3(name) values ('empname2');
INSERT INTO testrowid_s3(name) values ('empname3');
INSERT INTO testrowid_s3(name) values ('empname4');
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB empname2
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4

UPDATE testrowid_s3 SET name = 'Ramesh' WHERE rowid = 'AAAF3sAAAAAAAMmAAB' ;
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB Ramesh
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s3
(
    rowid_seq bigint generated always as identity,
    name character varying
);

insert into public.testrowid_s3 (name) values
('empname1'),('empname2'),('empname3'),('empname4');

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         2 | empname2
         3 | empname3
```

```
         4 | empname4

update testrowid_s3 set name = 'Ramesh' where rowid_seq = 2 ;

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         3 | empname3
         4 | empname4
         2 | Ramesh
```

Migre códigos de erro do banco de dados Oracle para um banco de dados compatível com Amazon Aurora PostgreSQL

Criado por Sai Parthasaradhi (AWS) e Veeranjaneyulu Grandhi (AWS)

Resumo

Esse padrão mostra como migrar códigos de erro do banco de dados Oracle para um banco de dados do Amazon Aurora Edição Compatível com PostgreSQL usando uma tabela de metadados predefinida.

Os códigos de erro do Oracle Database nem sempre têm um código de erro PostgreSQL correspondente. Essa diferença nos códigos de erro pode dificultar a configuração da lógica de processamento dos procedimentos ou funções na arquitetura PostgreSQL de destino.

Você pode simplificar o processo armazenando os códigos de erro do banco de dados de origem e destino que sejam significativos para seu programa PL/pgSQL em uma tabela de metadados. Em seguida, configure a tabela para sinalizar códigos de erro válidos do banco de dados Oracle e mapeá-los para seus equivalentes do PostgreSQL antes de continuar com a lógica restante do processo. Se o código de erro do Oracle Database não estiver na tabela de metadados, o processo será encerrado com a exceção. Em seguida, você pode revisar manualmente os detalhes do erro e adicionar o novo código de erro à tabela, se o programa exigir.

Ao usar essa configuração, seu banco de dados compatível com Amazon Aurora PostgreSQL pode lidar com erros da mesma forma que seu banco de dados Oracle de origem.

> **Note**
>
> Configurar um banco de dados PostgreSQL para lidar corretamente com os códigos de erro do banco de dados Oracle geralmente requer alterações no banco de dados e no código do aplicativo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle de origem com serviços de instância e de receptor em execução

- Um cluster compatível com o Amazon Aurora PostgreSQL que está em execução
- Familiaridade com o Oracle Database
- Familiaridade com bancos de dados PostgreSQL

Arquitetura

O diagrama a seguir mostra um exemplo de fluxo de trabalho de banco de dados compatível com Amazon Aurora PostgreSQL para validação e tratamento de códigos de erro de dados:

O diagrama mostra o seguinte fluxo de trabalho:

1. Uma tabela contém os códigos de erro e as classificações do Oracle Database e seus códigos de erro e classificações equivalentes do PostgreSQL. A tabela inclui uma coluna valid_error que classifica se códigos de erro específicos e predefinidos são válidos ou não.
2. Quando uma função PL/pgSQL (func_processdata) gera uma exceção, ela invoca uma segunda função PL/pgSQL (error_validation).
3. A função error_validation aceita o código de erro do Oracle Database como argumento de entrada. Em seguida, a função verifica o código de erro recebido em relação à tabela para ver se o erro está incluído na tabela.
4. Se o código de erro do banco de dados Oracle estiver incluído na tabela, a função error_validation retornará um valor VERDADEIRO e a lógica do processo continuará. Se o código de erro não estiver incluído na tabela, a função retornará um valor FALSO e a lógica do processo será encerrada com uma exceção.
5. Quando a função retorna um valor FALSE, os detalhes do erro são revisados manualmente pelo líder funcional do aplicativo para determinar sua validade.
6. O novo código de erro é então adicionado manualmente à tabela ou não. Se o código de erro for válido e adicionado à tabela, a função error_validation retornará um valor TRUE na próxima vez que a exceção ocorrer. Se o código de erro não for válido e o processo falhar quando a exceção ocorrer, o código de erro não será adicionado à tabela.

Pilha de tecnologia

- Amazon Aurora PostgreSQL
- pgAdmin

- Oracle SQL Developer

Ferramentas

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID, que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.
- O pgAdmin é uma ferramenta de gerenciamento e desenvolvimento de código aberto para o PostgreSQL. Fornece uma interface gráfica que simplifica a criação, manutenção e uso de objetos de banco de dados.
- O Oracle SQL Developer é um ambiente de desenvolvimento gratuito e integrado que simplifica o desenvolvimento e o gerenciamento do Oracle Database em implantações tradicionais e na nuvem.

Épicos

Migre códigos de erro do banco de dados Oracle para seu banco de dados compatível com Amazon Aurora PostgreSQL

Tarefa	Descrição	Habilidades necessárias

Crie uma tabela no Amazon Aurora compatível com PostgreSQL.	Execute o seguinte comando CREATE TABLE do PostgreSQL:
	`(`
	`source_error_code numeric NOT NULL,`
	`target_error_code character varying NOT NULL,`
	`valid_error character varying(1) NOT NULL`
		Desenvolvedor do PostgreSQL, Oracle, RDS/Aurora para PostgreSQL

Tarefa	Descrição	Habilidades necessárias
	); ```	

Tarefa	Descrição	Habilidades necessárias

Adicione os códigos de erro do PostgreSQL e seus códigos de erro do Oracle Database correspondentes à tabela.	Execute o comando INSERT do PostgreSQL para adicionar os valores de código de erro necessários à tabela error_codes.
	
	Os códigos de erro do PostgreSQL devem usar o tipo de dados variável de caracteres (valor SQLSTATE). Os códigos de erro do Oracle devem usar o tipo de dados numéricos (valor SQLCODE).
	
	Exemplo de instruções de inserção:
	
	`insert into error_codes values (-1817,'22007','Y');`
	`insert into error_codes values (-1816,'22007','Y');`
	`insert into error_codes values (-3114,'08006','N');`
	
	Note
	Se você estiver detectando exceções de conectividade de banco de dados Java (JDBC) específicas da Oracle, deverá substituí-las por exceções genéricas
		Desenvolvedor do PostgreSQL, Oracle, RDS/Aurora para PostgreSQL

Tarefa	Descrição	Habilidades necessárias
	entre bancos de dados ou alternar para exceções específicas do PostgreSQL.	
Crie uma função PL/pgSQL para validar códigos de erro.	Crie uma função PL/pgSQL executando o comando CREATE FUNCTION do PostgreSQL. Certifique-se de que a função faça o seguinte: • Aceita os códigos de erro Oracle lançados por um programa. • Verifica se os códigos de erro estão presentes na tabela error_codes. • Retorna o valor TRUE ou FALSE, com base no fato de o código de erro estar presente na tabela de metadados ou não.	Desenvolvedor do PostgreSQL, Oracle, RDS/Aurora para PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Revise manualmente os novos códigos de erro conforme eles são registrados pela função PL/pgSQL.	Revise manualmente os novos códigos de erro. Se um novo código de erro for válido para seu caso de uso, adicione-o à tabela error_codes executando o comando INSERT do PostgreSQL. - ou - Se um novo código de erro não for válido para seu caso de uso, não o adicione à tabela. A lógica do processo continuará falhando e será encerrada, com exceção, quando o erro ocorrer.	Desenvolvedor do PostgreSQL, Oracle, RDS/Aurora para PostgreSQL

Recursos relacionados

Apêndice A. Códigos de erro do PostgreSQL (Documentação do PostgreSQL)

Mensagens de erro do banco de dados (Documentação do Oracle Database)

Migre cargas de trabalho do Redis para o Redis Enterprise Cloud na AWS

Criado por Antony Prasad Thevaraj (AWS) e Srinivas Pendyala (Redis)

Resumo

Esse padrão discute o processo de alto nível para migrar workloads do Redis para o Redis Enterprise Cloud na Amazon Web Services (AWS). Ele descreve as etapas de migração, fornece informações sobre a seleção de ferramentas disponíveis e discute as vantagens, desvantagens e etapas do uso de cada ferramenta. Opcionalmente, se precisar de ajuda adicional na migração de workloads do Redis, você pode contratar o Redis Professional Services.

Se você executa o Redis OSS ou o Redis Enterprise Software on-premises, está familiarizado com a significativa sobrecarga administrativa e a complexidade operacional de manter seus bancos de dados Redis em seu datacenter. Ao migrar suas cargas de trabalho para a nuvem, você pode reduzir significativamente essa carga operacional e aproveitar o Redis Enterprise Cloud, que é uma oferta de banco de dados como serviço (DBaaS) totalmente hospedada da Redis. Essa migração ajuda a aumentar sua agilidade comercial, melhora a confiabilidade do aplicativo e reduz os custos gerais, enquanto você obtém acesso aos mais novos atributos do Redis Enterprise Cloud on AWS, como disponibilidade de 99,999%, simplicidade arquitetônica e escala.

Existem possíveis aplicações para o Redis Enterprise Cloud nos setores de serviços financeiros, varejo, saúde e jogos, bem como em casos de uso que exigem soluções para detecção de fraudes, inventário em tempo real, processamento de reclamações e gerenciamento de sessões. Você pode usar o Redis Enterprise Cloud para se conectar aos seus recursos da AWS – por exemplo, a um servidor de aplicativos executado em instâncias do Amazon Elastic Compute Cloud (EC2Amazon) ou a um microsserviço implantado como um serviço AWS Lambda.

Pré-requisitos e limitações

Suposições

- No momento, você está operando um sistema de banco de dados on-premises que deseja migrar para a nuvem.
- Você identificou os requisitos de migração para suas workloads, incluindo
  - Requisitos de consistência de dados.
  - Requisitos de infraestrutura e ambiente do sistema
  - Requisitos de mapeamento e transformação de dados
  - Requisitos de teste funcional

  - Requisitos de teste de desempenho
  - Requisitos de validação
  - Estratégia de substituição definida
- Você avaliou os cronogramas e as estimativas de custo necessários para a migração.
- Seus requisitos levam em consideração o escopo do trabalho e os sistemas e bancos de dados que você identificou como parte da migração.
- Você identificou as partes interessadas junto com suas funções e responsabilidades em uma matriz responsável, consultada e informada (RACI).
- Você recebeu o acordo e as aprovações necessários de todas as partes interessadas.

Custos

Dependendo das especificações técnicas do seu banco de dados de origem existente (por exemplo, tamanho da memória, throughput e tamanho total dos dados), um arquiteto de soluções do Redis pode dimensionar o sistema de destino no Redis Enterprise Cloud. Para obter informações gerais sobre preços, consulte Preços do Redis no site do Redis.

Pessoas e habilidades

O processo de migração envolve as seguintes funções e responsabilidades.

Função	Descrição	Habilidades necessárias
Arquiteto de soluções de migração	Um arquiteto técnico com experiência em definir, planejar e implementar estratégias de migração	Compreensão técnica e em nível de aplicativo dos sistemas de origem e destino; experiência com a migração de cargas de trabalho para a nuvem
Arquiteto de dados	Um arquiteto técnico com ampla experiência na definição, implementação e entrega de soluções de dados para uma ampla variedade de bancos de dados	Modelagem de dados para dados estruturados e não estruturados, profundo entendimento e experiência na implementação de bancos de dados para uma empresa

Arquiteto de soluções Redis	Um arquiteto técnico que pode ajudar a arquitetar um cluster Redis de tamanho ideal para o caso de uso adequado	Experiência em arquitetura e implantação de soluções Redis para uma ampla variedade de casos de uso
Arquiteto de soluções em nuvem	Um arquiteto técnico que tem uma compreensão mais profunda das soluções em nuvem, especialmente na AWS	Experiência em soluções de arquitetura para a nuvem; experiência em migração de workload e modernização de aplicativos
Arquiteto corporativo	Um arquiteto técnico que tem uma compreensão completa do cenário técnico da sua organização, que tem uma visão compartil hada do roteiro do futuro e que pratica e estabelece as melhores práticas arquitetô nicas padronizadas em todas as equipes da sua organizaç ão	Certificações de arquitetura de software, como TOGAF, habilidades básicas de engenharia de software e experiência em arquitetura de soluções e arquitetura corporativa
TI ou DevOps engenheiro	Um engenheiro responsável por criar e manter a infraestr utura, incluindo monitorar a infraestrutura em busca de problemas, realizar tarefas de manutenção e fazer atualizaç ões conforme necessário.	Forte compreensão de várias tecnologias, incluindo sistemas operacionais, redes e computação em nuvem; familiaridade com linguagens de programação como Python, Bash e Ruby, bem como ferramentas como Docker, Kubernetes e Ansible

Arquitetura

Opções de migração

O diagrama a seguir mostra as opções para migrar suas fontes de dados on-premises (baseadas em Redis ou outras) para a AWS. Ele mostra várias ferramentas de migração que você pode escolher, como exportar arquivos do Redis Database (RDB) para o Amazon Simple Storage Service (Amazon S3), usar o atributo de replicação do Redis ou usar o AWS DMS.

1. Fontes de dados on-premises: bancos de dados que não são baseados no Redis, como MySQL, PostgreSQL, Oracle, SQL Server ou MariaDB.
2. Fontes de dados on-premises: bancos de dados baseados no protocolo Redis, como Redis OSS e Redis Enterprise Software.
3. A maneira mais simples de migrar dados de bancos de dados baseados em Redis é exportar arquivos RDB e importá-los para o Redis Enterprise Cloud de destino na AWS.
4. Como alternativa, você pode migrar os dados da origem para o destino usando o atributo de replicação (`ReplicaOf`) no Redis.
5. Se seus requisitos de migração de dados incluírem a transformação de dados, você pode empregar as ferramentas de entrada/saída do Redis (RIOT) para migrar os dados.
6. Como alternativa, você pode usar o AWS Data Migration Service (AWS DMS) para migrar dados de bancos de dados baseados em SQL.
7. Você deve usar o emparelhamento de nuvem privada virtual (VPC) para o AWS DMS para migrar os dados com sucesso para a Redis Enterprise Cloud de destino na AWS.

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura de implantação típica do Redis Enterprise Cloud na AWS e ilustra como ela pode ser usada com os principais serviços da AWS.

1. Você pode se conectar aos aplicativos de negócios que são apoiados pelo Redis Enterprise Cloud na AWS.
2. Você pode executar aplicativos de negócios em sua própria conta da AWS, em uma VPC dentro dessa conta.
3. Você pode usar os endpoints do banco de dados Redis Enterprise Cloud para se conectar aos seus aplicativos. Os exemplos incluem um servidor de aplicativos executado em EC2 instâncias, um microsserviço implantado como um serviço AWS Lambda, um aplicativo Amazon Elastic Container Service (Amazon ECS) ou um aplicativo Amazon Elastic Kubernetes Service (Amazon EKS).

4. Os aplicativos de negócios executados em sua VPC exigem uma conexão de emparelhamento da VPC do Redis Enterprise Cloud. Isso permite que os aplicativos de negócios se conectem com segurança por meio de endpoints privados.
5. O Redis Enterprise Cloud on AWS é uma plataforma de banco de dados NoSQL em memória implantada como S DBaa na AWS e totalmente gerenciada pelo Redis.
6. O Redis Enterprise Cloud é implantado em uma VPC em uma conta padrão da AWS criada pelo Redis.
7. Por motivos de segurança, o Redis Enterprise Cloud é implantado em uma sub-rede privada que pode ser acessada em endpoints públicos e privados. Recomendamos que você conecte seus aplicativos cliente ao Redis em endpoints privados. Se você planeja usar um endpoint público, é altamente recomendável habilitar o TLS para criptografar os dados entre seus aplicativos cliente e o Redis Enterprise Cloud.

A metodologia de migração do Redis se alinha à metodologia de migração da AWS, que é ilustrada em Mobilize sua organização para acelerar migrações em grande escala no site Recomendações da AWS.

Automação e escala

As tarefas de configuração do ambiente para a migração podem ser automatizadas por meio da Zona de Pouso da AWS e de modelos de infraestrutura como código (IaC) para automação e escalabilidade. Eles são discutidos na seção Épicos desse padrão.

Ferramentas

Com base em seus requisitos de migração de dados, você pode escolher entre uma seleção de opções tecnológicas para migrar seus dados para o Redis Enterprise Cloud na AWS. A tabela a seguir descreve e compara essas ferramentas.

Ferramenta	Descrição	Vantagens	Desvantagens
Exportação e importação de RDB	Você exporta os dados do banco de dados de origem (por exemplo, Redis OSS ou Redis Enterprise Software) na forma	• Simples • Funciona com qualquer solução baseada em Redis que possa exportar dados	• Não atende aos requisitos de transformação de dados nem oferece suporte a mesclagens

	de arquivos RDB. Se seu banco de dados for fornecido por meio de um cluster Redis OSS, você exportará cada fragmento mestre para um RDB. Em seguida, você importa todos os arquivos RDB em uma única etapa. Se seu banco de dados de origem for baseado em um cluster OSS, mas seu banco de dados de destino não estiver usando a API OSS Cluster, você precisará alterar o código-fonte do aplicativo para usar uma biblioteca cliente padrão do Redis. Os requisitos de transformação de dados ou mesclagens lógicas de bancos de dados exigem um processo mais complexo, que é explicado em Mesclagem lógica de banco de dados, mais adiante nesta tabela.	no formato RDB como fonte (incluindo Redis OSS e Redis Enterprise Software). • Alcança a consistência de dados com um processo simples.	lógicas de bancos de dados. • Demorado para conjuntos de dados maiores. • Nenhum suporte à migração delta pode levar a um maior tempo de inatividade.

Atributo de replicação do Redis(ativo-passivo)	Você pode replicar continuamente dados de um banco de dados Redis OSS, Enterprise Software ou Enterprise Cloud para um banco de dados Redis Enterprise Cloud. Após a sincronização inicial, o atributo de replicação do Redis (`REPLICAOF`) executa uma migração delta, o que significa que quase não há tempo de inatividade observado do aplicativo. O atributo de replicação do Redis deve ser usado de forma ativa-passiva. O destino é considerado passivo e é totalmente ressincronizado (liberado e sincronizado do banco de dados de origem). Portanto, alternar entre a origem e o destino é um pouco mais complicado. É possível replicar de um cluster do Redis OSS para	• Oferece suporte à replicação contínua (carga inicial de dados seguida por deltas). • Quase nenhum tempo de inatividade (depende do atraso na replicação). • Alcança a consistência de dados.	• Apenas um site deve estar ativo, então alternar entre sites é mais complicado. • Suporta no máximo 32 fragmentos mestres quando você migra de um cluster OSS.

	um banco de dados padrão do Redis Enterprise Cloud em cluster especificando todos os fragmento s principais do OSS Cluster como fontes. No entanto, o atributo de replicação do Redis permite no máximo 32 bancos de dados de origem.		
AWS DMS	Você pode usar o AWS DMS para migrar dados de qualquer banco de dados de origem compatível para um datastore Redis de destino com o mínimo de tempo de inatividade. Para obter mais informações, consulte Usando o Redis como destino para o AWS DMS na documentação do AWS DMS.	• Suporta a migração de fontes de dados NoSQL e SQL. • Funciona bem com outros serviços da AWS • Suporta casos de uso de migração ao vivo e captura de dados de alteração (CDC).	• Os valores-chave do Redis não podem conter caracteres especiais, como%. • Não suporta a migração de dados com caracteres especiais nas linhas ou nos nomes dos campos. • Não é compatível com o modo Full Large Binary Object (LOB).

Mesclagem lógica de banco de dados	Requisitos especiais de mesclagem de bancos de dados podem exigir uma solução personalizada de migração de dados. Por exemplo, você pode ter quatro bancos de dados lógicos (`SELECT 0..3`) no Redis OSS, mas talvez queira usar um único endpoint de banco de dados em vez de mover os dados para vários bancos de dados do Redis Enterprise Cloud. O Redis Enterprise não oferece suporte a bancos de dados lógicos selecionáveis, então você precisaria transformar o modelo de dados físicos do banco de dados de origem. Por exemplo, você pode mapear cada índice de banco de dados para um prefixo (`0` para `usr`, 1 para `cmp`, e assim por diante) e, em seguida, usar um script de migração ou	• Controle granular na modelagem dos dados durante a migração para o sistema de destino usando scripts personalizados.	• Se você decidir não concluir a migração, a reversão pode ser muito desafiadora, especialmente se os dados mais novos precisarem ser revertidos para os sistemas de origem. • O custo de construção pode ser alto se o objetivo for criar uma solução única para uma migração única. • Os custos de manutenção de código, infraestrutura, tempo de desenvolvimento e outras áreas podem ser altos se os requisitos de migração mudarem com frequência.

	uma ferramenta de extração, transformação e carregamento (ETL) para gerar um arquivo RDB, que pode ser importado para o banco de dados de destino.

Além disso, você pode usar as seguintes ferramentas e serviços da AWS.

Ferramentas de avaliação e descoberta:

- AWS Application Discovery Service
- Avaliador de migração

Ferramentas de migração de aplicativos e servidores:

- Serviço de migração de aplicações da AWS

Ferramentas de migração de banco de dados:

- AWS Schema Conversion Tool (AWS SCT)
- AWS Database Migration Service (AWS DMS)

Ferramentas de migração de dados:

- AWS Storage Gateway
- AWS DataSync
- AWS Direct Connect
- AWS Snowball
- Amazon Data Firehose

Gerenciamento de migração:

- AWS Migration Hub

Soluções de parceiro da AWS

- Parceiros de competência em migração da AWS

Épicos

Tarefas completas de descoberta e avaliação

Tarefa	Descrição	Habilidades necessárias
Identificar workloads.	Identifique as workload candidatas adequadas que você deseja migrar. Considere o seguinte antes de escolher uma workload para migração: • Qual é o valor comercial de migrar ou não essa workload? • Existe um plano de contingência se essa workload não migrar com sucesso para o sistema de destino? O ideal é escolher uma workload que tenha o máximo impacto nos negócios com o mínimo de riscos envolvidos. Mantenha o processo geral iterativo e migre em pequenos incrementos.	Arquiteto de dados, campeões de negócios, patrocinadores de projetos de migração

Tarefa	Descrição	Habilidades necessárias
Identifique requisitos e fontes de dados; projete o modelo de dados.	O Redis realiza um workshop para acelerar a descobert a e definir o planejamento de migração para o projeto. Como parte desse workshop, as equipes do Redis identific am as fontes de dados e os requisitos do modelo de dados de origem e analisam como eles podem ser remodelados no Redis Enterprise Cloud. A equipe de migração do Redis (Serviços Profissionais) realiza um exercício detalhado de design do modelo de dados com sua organização. Como parte desse exercício, a equipe do Redis: • Identifica as estruturas de dados de destino do Redis. • Define a estratégia de mapeamento de dados. • Documenta a abordagem e as recomendações de migração. • Analisa e finaliza o modelo de dados com as partes interessadas.	Arquiteto de soluções Redis

Tarefa	Descrição	Habilidades necessárias
Identificar as características do banco de dados de origem.	Identifique o produto Redis que é usado nos ambientes de origem e destino. Por exemplo: • O banco de dados de origem é um banco de dados OSS Cluster, um banco de dados Redis autônomo ou um banco de dados Redis Enterprise? • O banco de dados de destino será um banco de dados padrão do Redis Enterprise ou um banco de dados compatível com o OSS Cluster? • Quais são as implicações em relação ao código-fonte do aplicativo?	Arquiteto de dados
Reúna o SLA atual do sistema e outras métricas de dimensionamento.	Determine os contratos de nível de serviço atuais (SLAs) expressos em termos de taxa de transferência (operaçõe s por segundo), latência, tamanho geral da memória por banco de dados e requisitos de alta disponibilidade (HA).	Arquiteto de dados

Tarefa	Descrição	Habilidades necessárias
Identifique as características do sistema destino.	Determine as respostas para essas perguntas: • Quantos dados precisam ser migrados? • Quanto tempo leva para migrar uma determinada quantidade de dados? • Quais são os requisitos de tempo de inatividade para a migração? É aceitável que seu serviço ou aplicativo fique indisponível por um período específico? Em caso afirmativo, por quanto tempo? • Quão consistentes devem ser os dados migrados? O banco de dados de destino pode estar em um estado ligeiramente inconsistente (desatualizado)? • Os dados precisam ser transformados antes de serem carregados no banco de dados de destino? (Por exemplo, você tem a opção de converter índices de banco de dados selecioná veis em prefixos antes da migração). • O banco de dados de origem pode ser acessado pelo host do banco de	Arquiteto de dados, arquiteto de soluções Redis (opcional)

Tarefa	Descrição	Habilidades necessárias
	dados de destino (por exemplo, de uma VPC de mesmo nível ou de um endpoint público usando criptografia)? • Conclua um exercício de dimensionamento de dados e dimensionamento de clusters do Redis com um arquiteto técnico do Redis. • Identifique os requisitos de rede, os requisitos de infraestrutura, as versões de software e o licenciamento de software e adquira todos os componentes antes da migração. • Há alguma preocupação de segurança associada à transferência desses dados?	

Tarefa	Descrição	Habilidades necessárias
Identificar dependências.	Identifique as dependências ascendentes e posteriores do sistema atual a ser migrado. Certifique-se de que o trabalho de migração esteja alinhado com outras migrações de sistemas dependentes. Por exemplo, se você planeja migrar outros aplicativos de negócios on-premises para a nuvem AWS, identifique esses aplicativos e alinhe-os com base nas metas do projeto, nos cronogramas e nas partes interessadas.	Arquiteto de dados, arquiteto corporativo

Tarefa	Descrição	Habilidades necessárias
Identifique as ferramentas de migração.	Dependendo dos requisitos de migração de dados (como requisitos de dados de origem ou tempo de inatividade), você pode usar qualquer uma das ferramentas descritas anteriormente na seção Ferramentas. Além disso, você pode usar: • Replicação bidirecional (ativa-ativa) usando a implantação do CRDB. • Scripts personalizados de exportação/importação (por exemplo, usando `DUMP`/`RESTORE` comandos). • Ferramentas adicionais de exportação/importação e ferramentas auxiliares, como RIOT ou ferramentas ECstats2 ETL. • Ferramentas de IaC, como modelos do Terraform ou da AWS CloudFormation .	Arquiteto de soluções de migração, arquiteto de soluções Redis
Crie um plano de contingência.	Estabeleça um plano de contingência para reverter, caso você encontre problemas durante a migração.	Gerenciamento de projetos, equipes técnicas, incluindo arquiteto

Tarefas completas de segurança e conformidade

Tarefa	Descrição	Habilidades necessárias
Proteja o console de administração do Redis.	Para proteger o console de administração, siga as instruções na documentação do Redis.	Administrador de infraestrutura de TI
Proteja o banco de dados Redis.	Consulte as seguintes páginas na documentação do Redis para: • Definir controle de acesso com base em função • Defina a segurança da rede. • Ative o TLS.	
Nuvem APIs Redis segura.	Ao ativar a API, você pode gerenciar as chaves de API para todos os proprietários da sua conta do Redis Cloud. Para uma visão geral dos atributo de segurança da API, consulte a documentação de autenticação da API no site do Redis.	Administrador de infraestrutura de TI

Configurar o novo ambiente

Tarefa	Descrição	Habilidades necessárias
Configure um novo ambiente na AWS.	Essa tarefa inclui: • Atividades de configuração da Zona de Pouso da AWS . A zona de pouso suporta:	TI ou DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• Implantações em várias contas • Linha de base de segurança mínima • Forma automatizada de provisionar novas contas com uma linha de base de segurança e pré-requisitos de ISV (rede, configuração de segurança etc). • Notificações, log centraliz ado e monitoramento • Atividades de configuração do software ISV. Isso inclui configurações que precisam ser incluídas na migração, como configurações e alterações do produto e da workload. • Atividades de IaC, como configurar ou personalizar modelos da CloudFormation AWS ou do Terraform.	

Tarefa	Descrição	Habilidades necessárias
Implante a arquitetura de migração.	1. Configure o Redis Enterprise Cloud na AWS. 2. Instale ferramentas de migração, como RIOT ou AWS DMS. Consulte a seção Ferramentas para obter uma lista das ferramentas disponíveis. 3. Estabeleça conectividade entre as camadas de aplicativo, migração e banco de dados. 4. Crie uma workload de amostra que possa fluir por cada camada e migre um pequeno conjunto de dados de amostra. Agora você está pronto para executar os pipelines reais de migração de dados e testá-los.	TI ou DevOps engenheiro

Configurar redes

Tarefa	Descrição	Habilidades necessárias
Estabeleça conectividade.	Estabeleça conectividade entre a infraestrutura on-premises e os recursos da nuvem AWS. Use grupos de segurança, o AWS Direct Connect e outros recursos para obter essa	TI ou DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	funcionalidade. Para obter mais informações, consulte Connect Your DataCenter to AWS no site da AWS.	
Configurar o emparelhamento de VPC.	Estabeleça o emparelhamento de VPC entre a VPC VPCs que executa aplicativos de negócios (ou as EC2 instâncias que executam ferramentas de migração ou o servidor de replicação do AWS DMS) e a VPC que executa o Redis Enterprise Cloud. Para obter instruções, consulte Comece a usar a Amazon VPC na documentação da Amazon VPC e Ativar o emparelhamento de VPC na documentação do Redis.	TI ou DevOps engenheiro

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Escolha uma ferramenta de migração de dados.	Examine a tabela na seção Ferramentas para ver as descrições, vantagens e desvantagens dessas ferramentas: • Exportação e importação de RDS • Atributo de replicação do Redis (`ReplicaOf `)	Arquiteto de soluções de migração

Tarefa	Descrição	Habilidades necessárias
	• AWS DMS • Mesclagem lógica de banco de dados As linhas a seguir descrevem as tarefas de migração de dados associadas a cada ferramenta.	

Tarefa	Descrição	Habilidades necessárias
Opção 1: usar exportação e importação do RDB.	1. Desconectar a origem: interrompa o tráfego no banco de dados de origem (por exemplo, desconectando aplicativos de negócios). 2. Exportar: exporte os dados do banco de dados de origem como um arquivo RDB. 3. Etapa: faça o upload dos dados em um local acessível às instâncias do Redis Enterprise Cloud na AWS (por exemplo, você pode carregá-los em um bucket do S3 ou servidor FTP). 4. Importar: importe os arquivos RDB (listando todos eles em uma etapa de importação) para seu banco de dados de destino do Redis Enterprise Cloud. 5. Recortar: vá para o banco de dados de destino (por exemplo, conectando seu aplicativo a ele). Para obter mais informações, consulte a Documentação do Redis.	Arquiteto de soluções de migração, arquiteto de soluções Redis

Tarefa	Descrição	Habilidades necessárias
Opção 2: Use o atributo de replicação do Redis (ativo-passivo).	1. Conectar banco de dados: Estabeleça um `ReplicaOf` link entre os bancos de dados de origem e de destino. 2. Execute uma sincronização inicial: espere até que a sincronização inicial entre os bancos de dados de origem e de destino seja concluída. 3. Desconectar a origem: interrompa o tráfego no banco de dados de origem (por exemplo, desconectando o aplicativo). 4. Execute a replicação delta: espere até que o delta seja replicado no banco de dados de destino. 5. Recortar: vá para o banco de dados de destino (por exemplo, conectando seu aplicativo a ele). 6. Excluir: remova o `ReplicaOf` link entre os bancos de dados de origem e de destino. Para obter mais informações, consulte a Documentação do Redis.	Arquiteto de soluções de migração, arquiteto de soluções Redis

Tarefa	Descrição	Habilidades necessárias
Opção 3: usar o AWS DMS.	1. Configure uma instância de replicação do AWS DMS: essa instância executa todos os processos de migração. Para obter instruções: Trabalhar com uma instância de replicação do AWS DMS na documentação do AWS DMS. 2. Defina o banco de dados de origem: defina o endpoint de origem. Teste a conectividade entre o endpoint de origem e o servidor de replicação do AWS DMS. Para obter instruções: Criação de endpoints de origem e destino na documentação do AWS DMS. 3. Configure o banco de dados de destino: configure o Redis Enterprise Cloud na AWS e configure o banco de dados para o qual migrar. 4. Defina o banco de dados de destino: defina o endpoint de destino. Certifique-se de que o emparelhamento de VPC seja estabelecido entre a VPC em que o AWS DMS está sendo executado	Arquiteto de soluções de migração, arquiteto de soluções Redis

Tarefa	Descrição	Habilidades necessárias
	e a VPC que hospeda o Redis Enterprise Cloud na AWS. Teste a conectividade entre o servidor de replicação do AWS DMS e o banco de dados de destino. 5. Crie uma tarefa do AWS DMS: Crie uma tarefa ou um conjunto de tarefas para definir as tabelas e os processos de replicação que você deseja usar para migrar os dados. Para obter instruções: Trabalhar com tarefas do AWS DMS na documentação do AWS DMS. 6. Migrar: migre os dados executando a tarefa do AWS DMS. 7. Recortar: vá para o banco de dados de destino (por exemplo, conectando seu aplicativo a ele).	

Tarefa	Descrição	Habilidades necessárias
Opção 4: Use a mesclagem lógica do banco de dados.	Essa opção envolve o uso de um script de migração ou ferramenta ETL que pode transformar o modelo de dados físicos do banco de dados de origem e gerar um arquivo RDB. O Redis Professional Services pode ajudar nessa etapa, se necessário.	Arquiteto de soluções de migração, arquiteto de soluções Redis

Migrar seu aplicativo

Tarefa	Descrição	Habilidades necessárias
Alinhe os cronogramas e as metas do gerenciamento de projetos.	Alinhe as metas, os marcos e os cronogramas do projeto de migração da camada de aplicação com os do projeto de migração de dados do Redis.	Gerenciamento de projetos
Alinhe as atividades de teste.	Depois que a camada do aplicativo migrar e moderniza r na Nuvem AWS, aponte a camada do aplicativo para a recém-migrada Redis Enterprise Cloud na AWS para testes.	Teste

Teste

Tarefa	Descrição	Habilidades necessárias
Implemente planos de teste.	Execute as rotinas de migração de dados e os scripts que foram desenvolvidos durante a fase de implementação em um ambiente de teste, de acordo com os requisitos de teste, em seu local.	Teste
Teste a qualidade dos dados.	Teste a qualidade dos dados após migrar os dados.	Teste
Testar funcionalidade	Teste as consultas de dados e a camada do aplicativo para garantir que o aplicativo esteja funcionando no mesmo nível do sistema de origem.	Teste

Substituir

Tarefa	Descrição	Habilidades necessárias
Tome a decisão de substituição.	Depois que todos os testes em nível de aplicativo e banco de dados forem concluídos, a equipe de liderança executiva e as partes interessadas tomam a decisão final sobre migrar para o novo ambiente na AWS com base nos resultados finais confirmados pelas equipes de teste.	Gerenciamento de projetos, campeões de negócios

Tarefa	Descrição	Habilidades necessárias
Vá para a Nuvem AWS.	Quando você confirmar que tudo está pronto, aponte a camada do aplicativo para os dados recém-migrados e direcione os clientes para a nova camada de aplicativo que está sendo executada com base no novo sistema Redis Enterprise Cloud na AWS.	TI ou DevOps engenheiro, arquiteto de dados, arquiteto de soluções de migração, arquiteto de soluções Redis

Recursos relacionados

Recursos do Redis

- Documentação do Redis Enterprise Cloud
- Ferramenta RIOT (GitHub repositório)
- Terraform Provider (baixar)

Recursos da AWS

- Migrações de demonstração
- Soluções de parceiros da AWS
- Documentação
- Publicações no blog
- Livros brancos
- Tutoriais e vídeos
- Migração para a nuvem AWS
- Recomendações da AWS

Mais informações

Para obter os requisitos de segurança padrão para migrar cargas de trabalho do Redis para a nuvem da AWS, consulte as melhores práticas de segurança, identidade e conformidade no site da AWS e o Redis Trust Center no site do Redis.

Migre o SAP ASE na Amazon EC2 para o Amazon Aurora compatível com PostgreSQL usando o AWS SCT e o AWS DMS

Criado por Amit Kumar (AWS) e Ankit Gupta (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados SAP Adaptive Server Enterprise (SAP ASE) hospedado em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para a edição compatível com Amazon Aurora PostgreSQL usando o AWS Schema Conversion Tool (AWS SCT) e o AWS Database Migration Service (AWS DMS). O padrão se concentra nas conversões de linguagem de definição de dados (DDL) para objetos armazenados e na migração de dados.

O Aurora compatível com PostgreSQL oferece suporte a workloads de processamento de transações online (OLTP). Esse serviço gerenciado fornece configurações que escalam automaticamente sob demanda. Ele pode iniciar, desligar, aumentar e reduzir a escala verticalmente e automaticamente do seu banco de dados com base nas necessidades do seu aplicativo. Você pode executar seu banco de dados na nuvem sem gerenciar nenhuma instância de banco de dados. O Aurora compatível com PostgreSQL oferece uma opção econômica para workloads pouco frequentes, intermitentes ou imprevisíveis.

O processo de migração consiste em duas fases principais:

- Converter esquema de bancos de dados usando a AWS SCT
- Migração dos dados usando o AWS DMS

Instruções detalhadas para ambas as fases são fornecidas na seção Épicos. Para obter informações sobre a solução de problemas específicos do uso do AWS DMS com bancos de dados SAP ASE, consulte Solução de problemas com o SAP ASE na documentação do AWS DMS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados SAP ASE de origem em uma EC2 instância com serviços de servidor, banco de dados e ouvinte em execução
- Um banco de dados de destino compatível com o Aurora PostgreSQL

Limitações

- O número da porta para conexões deve ser 5432.
- O atributo huge_pages está ativado por padrão, mas pode ser modificado.
- Point-in-time a granularidade de recuperação (PITR) é de 5 minutos.
- Atualmente, a replicação entre regiões não está disponível.
- O tamanho de armazenamento máximo para um banco de dados do Aurora é de 128 TiB.
- É possível criar até 15 réplicas de leitura.
- O limite de tamanho da tabela é limitado somente pelo tamanho do volume do cluster do Aurora, portanto, o tamanho máximo da tabela para um cluster de banco de dados Aurora compatível com PostgreSQL é de 32 TiB. Recomendamos que você siga as práticas recomendadas do design de tabelas, como o particionamento de tabelas grandes.

Versões do produto

- Banco de dados de origem: o AWS DMS atualmente oferece suporte ao SAP ASE 15, 15.5, 15.7 e 16.x. Consulte o Guia do usuário do AWS DMS para obter as informações mais recentes sobre o suporte à versão SAP ASE.
- Banco de dados de destino: PostgreSQL 9.4 e versões posteriores (para a versão 9.x), 10.x, 11.x, 12.x, 13.x e 14.x. Consulte o Guia do usuário do AWS DMS para ver as versões mais recentes suportadas do PostgreSQL.
- Amazon Aurora 1.x ou superior. Para as informações mais recentes, consulte as versões do Aurora compatível com PostgreSQL e versões de mecanismo na documentação do Aurora.

Arquitetura

Pilha de tecnologia de origem

- Banco de dados SAP ASE em execução na Amazon EC2

Pilha de tecnologias de destino

- Banco de dados Aurora compatível com PostgreSQL

Arquitetura de migração

Ferramentas

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e em conformidade com ACID que ajuda você a configurar, operar e escalar as implantações de PostgreSQL.
- O AWS Schema Conversion Tool (AWS SCT) oferece suporte a migrações heterogêneas de bancos de dados convertendo automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino.
- O AWS DMS oferece suporte a vários bancos de dados de origem e destino diferentes. Para obter mais informações, consulte Origens para migração de dados e Destinos para migração de dados na documentação do AWS DMS. Para obter suporte mais abrangente à versão e aos atributos, recomendamos que você use a versão mais recente do AWS DMS.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Configure o acesso à rede na EC2 instância de origem.	Configure grupos de segurança na EC2 instância que hospeda seu banco de dados SAP ASE de origem. Para obter instruções, consulte Grupos EC2 de segurança da Amazon para instâncias Linux na EC2 documentação da Amazon.	Administrador de sistemas
Crie seu cluster de banco de dados de destino Aurora compatível com PostgreSQL.	Instale, configure e execute um cluster Aurora compatível com PostgreSQL para seu banco de dados de destino.	DBA

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte Criar um cluster de banco de dados do Amazon Aurora na documentação do Aurora.	
Configure a autorização para o cluster de banco de dados de destino.	Configure grupos de segurança e firewalls para o banco de dados de destino. Para obter instruções, consulte Criar um cluster de banco de dados do Amazon Aurora na documentação do Aurora.	DBA, administrador de sistemas

Converta seu esquema do banco de dados com a AWS SCT

Tarefa	Descrição	Habilidades necessárias
Inicie a AWS SCT.	Inicie a AWS SCT seguindo as instruções na documentação da AWS SCT. A AWS SCT oferece uma interface de usuário baseada em projeto que permite converter automaticamente o esquema do banco de dados de origem do SAP ASE em um formato que seja compatível com a instância do banco de dados Aurora de destino compatível com PostgreSQL.	DBA

Tarefa	Descrição	Habilidades necessárias
Crie endpoints da AWS SCT.	Crie endpoints para os bancos de dados de origem do SAP ASE e destino do PostgreSQL. Para obter instruções, consulte a documentação da AWS SCT.	DBA
Crie um relatório de avaliação.	Crie um relatório de avaliação da migração do banco de dados para avaliar a migração e detectar quaisquer objetos e funções incompatíveis. Para obter instruções, consulte a documentação da AWS SCT.	DBA
Converta o esquema.	Converta o esquema do banco de dados seguindo as instruções na documentação da AWS SCT.	DBA

Tarefa	Descrição	Habilidades necessárias
Valide objetos do banco de dados.	Se a AWS SCT não puder converter um objeto de banco de dados, ela identificará seu nome e outros detalhes. Você deve converter esses objetos manualmente. Para identificar essas incompatibilidades, siga as instruções na postagem do blog da AWS Validar objetos de banco de dados após migrar do SAP ASE para o Amazon RDS para PostgreSQL ou Amazon Aurora PostgreSQL.	DBA

Analise a migração do AWS DMS

Tarefa	Descrição	Habilidades necessárias
Valide as versões dos bancos de dados de origem e de destino.	Verifique as versões do banco de dados SAP ASE para verificar a compatibilidade com o AWS DMS. Para obter mais informações, consulte Fontes do AWS DMS e Destinos do AWS DMS na documentação do AWS DMS.	DBA
Identifique os requisitos para o tipo e capacidade de armazenamento.	Escolha a capacidade de armazenamento apropriad a para o banco de dados de destino com base no tamanho	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	do seu banco de dados de origem.	
Escolha o tipo de instância, a capacidade e outros atributos da instância de replicação.	Escolha o tipo de instância, a capacidade, os atributos de armazenamento e os atributos de rede que atendem às suas necessidades. Para obter orientação, consulte Escolher a instância de replicação do AWS DMS correta para sua migração na documentação do AWS DMS.	DBA, administrador de sistemas
Identifique os requisitos de segurança de acesso à rede.	Identifique os requisitos de segurança de acesso à rede para os bancos de dados de origem e de destino. Siga as orientações em Como configurar uma rede para uma instância de replicação na documentação do AWS DMS.	DBA, administrador de sistemas

Migrar os dados

Tarefa	Descrição	Habilidades necessárias
Migre os dados criando uma tarefa de migração no AWS DMS.	Para migrar os dados, crie uma tarefa e siga as instruções na documentação do AWS DMS. Recomendamos que você use a versão mais recente	DBA

Tarefa	Descrição	Habilidades necessárias
	do AWS DMS para obter o suporte mais abrangente de versões e atributos.	
Valide os dados.	Para validar se seus dados foram migrados com precisão do banco de dados de origem para o banco de dados de destino, siga as diretrizes de validação de dados fornecidas na documentação do AWS DMS.	DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Identifique a estratégia de migração de aplicativos.	Escolha uma das sete estratégias (7Rs) para migrar aplicativos para a nuvem.	DBA, proprietário do aplicativo, administrador de sistemas
Siga a estratégia de migração de aplicativos.	Conclua as tarefas do banco de dados identificadas pela equipe do aplicativo, incluindo a atualização dos detalhes da conexão DNS do banco de dados de destino e a atualização das consultas dinâmicas.	DBA, proprietário do aplicativo, administrador de sistemas

Vá para o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.	Mude a conexão do banco de dados de origem ao banco de dados de destino. Para obter mais informações, consulte a seção Substituição da estratégia de migração para bancos de dados relacionais.	DBA, proprietário do aplicativo, administrador de sistemas

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.	Encerre todas as tarefas de migração, instâncias de replicação, endpoints e outros recursos da AWS SCT e do AWS DMS. Para obter mais informações, consulte a documentação do AWS DMS.	DBA, administrador de sistemas
Revise e valide os documentos do projeto.	Valide todas as etapas na documentação do projeto para garantir que todas as tarefas tenham sido concluídas com êxito.	DBA, proprietário do aplicativo, administrador de sistemas
Fechar o projeto.	Feche o projeto de migração e forneça qualquer feedback.	DBA, proprietário do aplicativo, administrador de sistemas

Recursos relacionados

Referências

- Habilite conexões criptografadas para instâncias de banco de dados PostgreSQL no Amazon RDS (Recomendações da AWS)
- Transporte bancos de dados PostgreSQL entre duas instâncias de banco de dados Amazon RDS usando pg_transport (Recomendações da AWS)
- Preço do Amazon Aurora
- Práticas recomendadas com o Amazon Aurora Edição Compatível com PostgreSQL (documentação do Amazon Aurora)
- Documentação do AWS SCT
- Documentação do AWS DMS
- Uso de um banco de dados SAP ASE como fonte para AWS DMS

Tutoriais e vídeos

- Introdução ao AWS Database Migration Service
- AWS Database Migration Service (vídeo)

Migrar certificados SSL do Windows para um Application Load Balancer usando o ACM

Criado por Chandra Sekhar Yaratha (AWS) e Igor Kovalchuk (AWS)

Resumo

O padrão fornece orientação para o uso do AWS Certificate Manager (ACM) para migrar certificados Secure Sockets Layer (SSL) existentes de sites hospedados em servidores locais ou instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no Microsoft Internet Information Services (IIS). Os certificados SSL podem, então, ser usados com o Elastic Load Balancing na AWS.

O SSL protege seus dados, confirma sua identidade, fornece melhores classificações nos mecanismos de pesquisa, ajuda a atender aos requisitos do Padrão de segurança de dados do Setor de cartões de pagamento (PCI DSS) e aumenta a confiança do cliente. Os desenvolvedores e as equipes de TI que gerenciam essas workloads querem que seus aplicativos e infraestrutura web, incluindo o servidor IIS e o Windows Server, permaneçam em conformidade com suas políticas de referência.

Esse padrão abrange a exportação manual de certificados SSL existentes do Microsoft IIS, convertendo-os do formato Personal Information Exchange (PFX) para o formato Private Enhanced Mail (PEM) compatível com o ACM e, em seguida, importando-os para o ACM em sua conta da AWS. Também descreve como criar um Application Load Balancer para seu aplicativo e configurar o Application Load Balancer para usar seus certificados importados. Em seguida, as conexões HTTPS são encerradas no Application Load Balancer e você não precisa de mais sobrecarga de configuração no servidor web. Para obter mais informações, consulte Criar um receptor HTTPS para seu Application Load Balancer.

Os servidores Windows usam arquivos .pfx ou .p12 para conter o arquivo de chave pública (certificado SSL) e seu arquivo de chave privada exclusivo. A Autoridade de certificação (CA) fornece seu arquivo de chave pública. Você usa seu servidor para gerar o arquivo de chave privada associado em que a solicitação de assinatura de certificado (CSR) foi criada.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) na AWS com pelo menos uma sub-rede privada e uma pública em cada zona de disponibilidade usada por seus destinos

- IIS versão 8.0 ou superior, em execução no Windows Server 2012 ou superior
- Um aplicativo web em execução no IIS
- Acesso de administrador ao servidor IIS

Arquitetura

Pilha de tecnologia de origem

- Implementação do servidor web IIS com SSL para garantir que os dados sejam transmitidos com segurança em uma conexão criptografada (HTTPS)

Arquitetura de origem

Pilha de tecnologias de destino

- Certificados do ACM em sua conta da AWS
- Um Application Load Balancer configurado para usar certificados importados
- Instâncias do Windows Server nas sub-redes privadas

Arquitetura de destino

Ferramentas

- O AWS Certificate Manager (ACM) ajuda você a criar, armazenar e renovar chaves e certificados SSL/TLS X.509 públicos e privados que protegem seus sites e aplicativos da AWS.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre EC2 instâncias, contêineres e endereços IP em uma ou mais zonas de disponibilidade.

Práticas recomendadas

- Imponha redirecionamentos de tráfego de HTTP para HTTPS.
- Configure grupos de segurança para seu Application Load Balancer adequadamente a fim de permitir tráfego de entrada somente para portas específicas.

- Execute suas EC2 instâncias em diferentes zonas de disponibilidade para garantir a alta disponibilidade.
- Configure o domínio do seu aplicativo para apontar para o nome DNS do Application Load Balancer em vez de seu endereço IP.
- Certifique-se de que o Application Load Balancer tenha verificações de integridade da camada de aplicativo configuradas.
- Configure o limite para verificações de integridade.
- Use CloudWatch a Amazon para monitorar o Application Load Balancer.

Épicos

Exportar um arquivo .pfx

Tarefa	Descrição	Habilidades necessárias
Exporte o arquivo .pfx do Windows Server.	Para exportar o certificado SSL como um arquivo .pfx do gerenciador de IIS on-premises no Windows Server: 1. Escolha Iniciar, Administrativo, Gerenciador de Internet Information Services (IIS). 2. Selecione o nome do servidor e, em Segurança, clique duas vezes em Certificados de servidor. 3. Selecione o certificado que deseja exportar e escolha Exportar. 4. Na caixa Exportar certificado, escolha um local, um caminho e um nome para seu arquivo .pfx.	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	5. Especifique e confirme uma senha para seu arquivo .pfx. **Note** Você precisa dessa senha ao instalar o arquivo.pfx. 6. Escolha OK. Seu arquivo .pfx agora deve ser salvo no local e no caminho que você especificou.	

Converter o certificado codificado em PFX para o formato PEM

Tarefa	Descrição	Habilidades necessárias
Baixe e instale o kit de ferramentas do OpenSSL.	1. Baixe Win32/Win64 OpenSSL do site da Shining Light Productions e instale-o. 2. Adicione a localização dos binários do OpenSSL à sua variável PATH do sistema para que os binários possam estar disponíveis para uso na linha de comando.	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Converter o certificado codificado em PFX para o formato PEM.	As etapas a seguir convertem o arquivo de certificado assinado e codificado em PFX em três arquivos no formato PEM: • `cert-file.pem` contém o certificado SSL/TLS para o recurso. • `privatekey.pem` contém a chave privada do certificado sem proteção por senha. • `ca-chain.pem` contém o certificado raiz da CA. Converter o certificado codificado em PFX: 1. Execute o Windows PowerShell. 2. Use o comando a seguir para extrair a chave privada do certificado do arquivo PFX. Quando solicitado, digite a senha do certificado. `openssl pkcs12 -in <filename>.pfx -nocerts -out withpw-privatekey.pem` O comando gera um arquivo de chave privada codificado em PEM	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias

	chamado `privateke y.pem` . Quando solicitad o, insira uma frase secreta para proteger o arquivo de chave privada.
	3. Execute o seguinte comando para definir a senha da frase secreta. Quando solicitado, forneça a frase secreta que você criou na etapa 2.
	`openssl rsa -in withpw-privatekey. pem -out privateke y.pem`
	Se o comando for bem-sucedido, ele exibirá a mensagem “escrevendo a chave RSA”.
	4. Use o comando a seguir para transferir o certificado do arquivo PFX para um arquivo PEM.
	`openssl pkcs12 -in <file_name>.pfx - clcerts -nokeys -out cert-file.pem`
	Este comando cria um arquivo de certificado codificado em PEM chamado `cert-file`	

Tarefa	Descrição	Habilidades necessárias
	`.pem` . Se o comando for bem-sucedido, ele exibirá a mensagem “MAC verificado OK”. 5. Crie um arquivo de cadeias de CA a partir do arquivo PFX. Execute o seguinte comando para criar um arquivo de cadeia de CA chamado `ca-chain.pem` . `openssl pkcs12 -in <file_name>.pfx -cacerts -nokeys -chain -out ca-chain.pem` Se o comando for bem-sucedido, ele exibirá a mensagem “MAC verificado OK”.	

Importar um certificado para o ACM

Tarefa	Descrição	Habilidades necessárias
Prepare-se para importar o certificado.	No Console do ACM, escolha Importar um certificado.	Administrador de nuvem
Forneça o corpo do certifica do.	Para Corpo do certificado, cole o certificado codificado PEM que deseja importar. Para obter mais informaçõ es sobre os comandos e as etapas descritos nesta e em	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	outras tarefas deste tópico, consulte Importação de um certificado na documentação do ACM.	
Forneça a chave privada do certificado.	Para o Certificado de chave privada, cole a chave privada não criptografada e codificada PEM correspondente à chave pública do certificado.	Administrador de nuvem
Forneça a cadeia do certifica do.	Em Cadeia de certificados, cole a cadeia de certifica dos codificada em PEM, que é armazenada no arquivo `CertificateChain.pem` .	Administrador de nuvem
Importar o certificado.	Selecione Revisar e importar. Confirme se as informações sobre seu certificado estão corretas e escolha Importar.	Administrador de nuvem

Criar um Application Load Balancer

Tarefa	Descrição	Habilidades necessárias
Crie e configure o balanceador de carga e os receptores.	Siga as instruções na documentação do Elastic Load Balancing para configurar um grupo de destino e registrar destinos, além de criar um Application Load Balancer e um receptor. Adicione um segundo receptor (HTTPS) para a porta 443.	Administrador de nuvem

Solução de problemas

Problema	Solução
O Windows PowerShell não reconhece o comando OpenSSL mesmo depois de você adicioná-lo ao caminho do sistema.	Verifique `$env:path` para assegurar que ele inclui a localização dos binários do OpenSSL. Se isso não acontecer, execute o seguinte comando em PowerShell: `$env:path = $env:path + ";C:\OpenSSL-Win64\bin"`

Recursos relacionados

Importar um certificado para ACM

- Console do ACM
- Formato de chaves e certificados para importação
- Importar um certificado
- Guia do usuário do AWS Certificate Manager

Criar um Application Load Balancer

- Criar um Application Load Balancer
- Guia do usuário para Application Load Balancer

Migrar uma fila de mensagens do Microsoft Azure Service Bus para o Amazon SQS

Criado por Nisha Gambhir (AWS)

Resumo

Este padrão descreve como migrar um aplicativo web ou de console do .NET Framework ou .NET Core usando a plataforma de mensagens de fila Microsoft Azure Service Bus para o Amazon Simple Queue Service (Amazon SQS).

Os aplicativos usam serviços de mensagens para enviar e receber dados de outros aplicativos. Esses serviços ajudam a criar microsserviços desacoplados e altamente escaláveis, sistemas distribuídos e aplicativos de tecnologia sem servidor na nuvem.

As filas do Azure Service Bus fazem parte de uma infraestrutura mais ampla de mensagens do Azure que oferece suporte ao enfileiramento e ao sistema de publicação e assinatura de mensagens.

O Amazon SQS é um serviço de filas de mensagens totalmente gerenciado que facilita o desacoplamento e a escala de microsserviços, sistemas distribuídos e aplicativos com tecnologia sem servidor. O Amazon SQS elimina a complexidade e a sobrecarga associadas ao gerenciamento e à operação de middleware orientado a mensagens, além de permitir que os desenvolvedores se concentrem em outros trabalhos. Usando o Amazon SQS, você pode enviar, armazenar e receber mensagens entre componentes de software em qualquer volume, sem perder mensagens ou exigir que outros serviços estejam disponíveis.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo web ou de console do .NET Framework ou .NET Core que usa filas do Azure Service Bus (exemplo de código anexo)

Versões do produto

- .NET Framework 3.5 ou superior ou .NET Core 1.0.1, 2.0.0 ou superior

Arquitetura

Pilha de tecnologia de origem

- Um aplicativo web ou de console do .NET (Core ou Framework) que usa uma fila do Azure Service Bus para enviar mensagens

Pilha de tecnologias de destino

- Amazon SQS

Ferramentas

Ferramentas

- Microsoft Visual Studio

Código

Criar uma política de AWS Identity and Access Management (IAM) para o Amazon SQS:

1. Faça login no Console de Gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/.

2. No painel de navegação à esquerda, escolha Policies (Políticas) e Create policy (Criar política).

3. Escolha a guia JSON e cole o código a seguir:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sqs:DeleteMessage",
            "sqs:GetQueueUrl",
            "sqs:ChangeMessageVisibility",
            "sqs:SendMessageBatch",
            "sqs:ReceiveMessage",
            "sqs:SendMessage",
            "sqs:GetQueueAttributes",
            "sqs:ListQueueTags",
            "sqs:ListDeadLetterSourceQueues",
            "sqs:DeleteMessageBatch",
```

```
            "sqs:PurgeQueue",
            "sqs:DeleteQueue",
            "sqs:CreateQueue",
            "sqs:ChangeMessageVisibilityBatch",
            "sqs:SetQueueAttributes"
         ],
         "Resource": "arn:aws:sqs:*:<AccountId>:*"
      },
      {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "sqs:ListQueues",
         "Resource": "*"
      }
   ]
}
```

4. Escolha Revisar política, digite um nome e, em seguida, selecione Criar política.

5. Vincule a política recém-criada ao seu perfil do IAM ou crie um novo perfil.

Épicos

Configuração do Amazon SQS na AWS

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM para o Amazon SQS.	Crie a política do IAM que fornecerá acesso ao Amazon SQS. Consulte a seção Código para obter um exemplo de política.	Engenheiro de sistemas
Crie um perfil da AWS.	Crie um novo perfil executando as ferramentas da AWS para o PowerShell comando Set-AWSCredential. Isso armazena sua chave de acesso e a chave secreta no seu arquivo de credenciais padrão sob o nome de perfil	Engenheiro de sistemas

Tarefa	Descrição	Habilidades necessárias
	que você especificar. Vincule a política do Amazon SQS que você criou anteriormente a esta conta. Guarde o ID de chave de acesso e a chave de acesso secreta da AWS. Eles serão necessários nas próximas etapas.	
Crie uma fila do SQS.	Você pode criar uma fila padrão ou uma fila de primeiro a entrar, primeiro a sair (FIFO). Para obter instruçõe s, consulte os links na seção Referências.	Engenheiro de sistemas

Revise seu código do aplicativo .NET

Tarefa	Descrição	Habilidades necessárias
Instalar o AWS Toolkit for Visual Studio.	Esse kit de ferramentas é uma extensão do Microsoft Visual Studio e facilita a criação e a implantação de aplicativ os .NET na AWS. Para obter instruções de uso e instalaçã o, consulte o link na seção Referências.	Desenvolvedor de aplicações
Instale o AWSSDK pacote.SQ S. NuGet	Você pode instalar AWSSDK o.SQS escolhendo “Manage NuGet Package” no Visual Studio ou executando o comando “ AWSSDKInstall-Package .SQS”.	Desenvolvedor de aplicações

Tarefa	Descrição	Habilidades necessárias
Crie um AWSCredentials objeto em seu aplicativo.NET.	O aplicativo de exemplo no anexo mostra como criar um AWSCredentials objeto básico, que herda de AWSCredentials. Você pode usar o ID da chave de acesso e a chave de acesso secreta anteriores ou permitir que o objeto escolha-os na pasta .aws como parte do perfil do usuário no runtime.	Desenvolvimento de aplicativos
Crie um objeto cliente SQS.	Crie um objeto cliente SQS (AmazonSQSClient) para o.NET Framework. Isso faz parte do namespace Amazon.SQS. Esse objeto é necessário em vez do IQueue Client, que faz parte do Microsoft.Azure. ServiceBus namespace.	Desenvolvedor de aplicações
Chame o SendMessageAsync método para enviar mensagens para a fila SQS.	Altere o código que envia a mensagem para a fila para usar o. amazonSqsClient SendMessageAsync método. Para obter detalhes, consulte o modelo de código anexo.	Desenvolvimento de aplicativos

Tarefa	Descrição	Habilidades necessárias
Chame o ReceiveMessageAsync método para receber mensagens da fila SQS.	Altere o código que recebe a mensagem para usar amazonSqsClient o. ReceiveMessageAsync método. Para obter detalhes, consulte o modelo de código anexo.	Desenvolvimento de aplicativos
Chame o DeleteMessageAsync método para excluir mensagens da fila SQS.	Para excluir mensagens, altere o código do QueueClient. CompleteAsync método para amazonSqsClient o. DeleteMessageAsync método. Para obter detalhes, consulte o modelo de código anexo.	Desenvolvimento de aplicativos

Recursos relacionados

- Guia do desenvolvedor do AWS SDK para .NET
- Envio de mensagens usando o Amazon SQS
- Criação e uso de uma fila do Amazon SQS com o AWS SDK para .NET
- Enviar uma mensagem do Amazon SQS
- Receber uma mensagem de uma fila do Amazon SQS
- Excluir uma mensagem de uma fila do Amazon SQS Queue
- AWS Toolkit for Visual Studio

Mais informações

Este padrão inclui dois exemplos de aplicativos (consulte a seção de anexos):

- AzureSbTestAppinclui código que usa a fila do Azure Service Bus.
- AmazonSqsTestAppusa o Amazon SQS. Este é um aplicativo de console que usa o .NET Core 2.2 e inclui exemplos para enviar e receber mensagens.

Observações:

- QueueClient é um objeto do IQueue Client, que faz parte do Microsoft.Azure. ServiceBus namespace (incluído no Microsoft.Azure. ServiceBus NuGet pacote).
- amazonSqsClient é um objeto da AmazonSQSClient, que faz parte do namespace Amazon.sqs (incluído no pacote .SQS). AWSSDK NuGet
- Dependendo de onde o código está sendo executado, digamos, se está sendo executado EC2, a função precisa ter permissão para gravar na fila SQS.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre um banco de dados relacional para o MongoDB Atlas em AWS

Criado por Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) e Igor Alekseev (AWS)

Resumo

Esse padrão descreve as etapas para migrar de um banco de dados relacional, como SQL Server, MySQL ou PostgreSQL, para o MongoDB Atlas no. Nuvem AWS Ele usa o MongoDB Relational Migrator para ajudar a acelerar a migração de dados de bancos de dados relacionais para o MongoDB Atlas.

O padrão acompanha o guia Migrating to MongoDB Atlas no site Prescriptive Guidance. AWS AWS Ele fornece as etapas de implementação de um dos cenários de migração discutidos nesse guia. Para cenários adicionais de migração, consulte os seguintes padrões no site da Orientação AWS Prescritiva:

- Migre um ambiente MongoDB auto-hospedado para o MongoDB Atlas em AWS
- Transmita dados do IBM Db2, SAP, Sybase e outros bancos de dados para o MongoDB Atlas em AWS

O padrão é destinado aos parceiros e AWS usuários do AWS System Integrator (SI).

Pré-requisitos e limitações

Pré-requisitos

- Um banco de dados relacional de origem (Oracle Database, SQL Server, PostgreSQL, MySQL, SAP/Sybase ASE e outros) para migrar para o MongoDB Atlas.
- Familiaridade com bancos de dados relacionais, MongoDB Atlas e. Serviços da AWS Esse padrão explica algumas das etapas de migração em alto nível. Detalhes adicionais serão adicionados em versões futuras.

Versões do produto

- MongoDB versão 5.0 ou posterior

Arquitetura

O diagrama a seguir mostra a migração de um banco de dados do sistema de gerenciamento de banco de dados relacional (RDBMS) para o MongoDB Atlas em. AWS

Para arquiteturas de referência do MongoDB Atlas que oferecem suporte a diferentes cenários de uso, consulte Migração para o MongoDB Atlas no site Prescriptive Guidance. AWS AWS

Ferramentas

- O MongoDB Atlas é um banco de dados como serviço DBaa (S) totalmente gerenciado para implantar e gerenciar bancos de dados MongoDB na nuvem.
- O MongoDB Relational Migrator fornece uma transição suave dos dados dos bancos de dados relacionais tradicionais para o MongoDB. Ele ajuda a automatizar o processo de conversão e transforma o modelo de dados estruturados dos bancos de dados relacionais no formato de documento flexível fornecido pelo MongoDB. O Relational Migrator preserva a integridade e os relacionamentos dos dados para simplificar a migração. As organizações podem aproveitar os benefícios de escalabilidade, desempenho e versatilidade que o MongoDB oferece, mantendo a familiaridade de seus dados existentes.

Práticas recomendadas

Para obter as melhores práticas para usar o MongoDB AWS no, consulte as postagens no AWS blog do Partner Network.

Épicos

Descoberta e avaliação

Tarefa	Descrição	Habilidades necessárias
Determine os parâmetros e o tamanho do banco de dados relacional.	Estime o tamanho do conjunto de trabalho usando as recomendações e as informações do Relationa l Migrator `db.stats()` para o espaço total do índice. Suponha que uma porcentag	Proprietário do aplicativo, DBA

Tarefa	Descrição	Habilidades necessárias
	em do seu espaço de dados seja acessada com frequênci a. Essa tarefa deve levar aproximadamente uma semana. Para obter mais informações e exemplos dessa e de outras histórias deste épico, consulte a seção Recursos relacionados.	

Tarefa	Descrição	Habilidades necessárias
Estime os requisitos de largura de banda da rede.	Para estimar seus requisitos de largura de banda da rede, multiplique o tamanho médio dos documentos pelo número de documentos processados por segundo. Considere o tráfego máximo que qualquer nó do seu cluster suportará como base. Para calcular as taxas de transferência de dados downstream do seu cluster para os aplicativos cliente, use a soma do total de documentos retornados em determinado período. Se seus aplicativos fizerem a leitura a partir de nós secundários, divida esse número total de documentos pelo número de nós que podem processar operações de leitura. Para encontrar o tamanho médio do documento para um banco de dados, use o `db.stats().avgObjSize` comando. Essa tarefa normalmente leva um dia.	DBA
Selecione a camada do Atlas.	Siga as instruções na documentação do MongoDB para selecionar a camada correta do cluster Atlas.	DBA
Planeje a transição.	Planeje a substituição do aplicativo.	DBA, proprietário do aplicativo

Configure um novo ambiente MongoDB Atlas em AWS

Tarefa	Descrição	Habilidades necessárias
Crie um novo cluster MongoDB Atlas em. AWS	No MongoDB Atlas, escolha Criar um cluster. Na caixa de diálogo Criar novo cluster, selecione AWS como provedor de nuvem.	DBA
Selecione Regiões da AWS uma configuração global do cluster.	Selecione na lista de disponíveis Regiões da AWS para seu cluster Atlas. Configure clusters globais, se necessário.	DBA
Selecione o nível cluster.	Selecione o nível de cluster de sua preferência. Sua seleção de camadas determina fatores como memória, armazenam ento e especificação de IOPS.	DBA
Configurar definições adicionais de cluster.	Definir configurações adicionais de cluster, como opções de versão, backup e criptografia do MongoDB. Para obter mais informações sobre essas opções, consulte a seção Recursos relacionados.	DBA

Configure a segurança e a conformidade

Tarefa	Descrição	Habilidades necessárias
Configure a lista de acesso.	Para se conectar ao cluster Atlas, você deve adicionar uma entrada à lista de acesso	DBA

Tarefa	Descrição	Habilidades necessárias
	do projeto. O Atlas usa TLS/SSL para criptografar as conexões com a nuvem privada virtual (VPC) do seu banco de dados. Para configurar a lista de acesso do projeto e obter mais informaçõ es sobre as histórias desse épico, consulte a seção Recursos relacionados.	
Autentique e autorize usuários.	Você deve criar e autentica r os usuários do banco de dados que acessarão os clusters MongoDB Atlas. Para acessar clusters em um projeto, os usuários devem pertencer a esse projeto e podem pertencer a vários projetos.	DBA
Criar funções personalizadas.	(Opcional) O Atlas oferece suporte à criação de funções personalizadas nos casos em que as permissões de usuário do banco de dados Atlas incorporadas não abrangem o conjunto de permissões que você deseja.	DBA
Configurar o emparelhamento de VPC.	(Opcional) O Atlas oferece suporte ao emparelhamento de VPC com outros. VPCs AWS	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Configure um AWS PrivateLink endpoint.	(Opcional) Você pode configurar endpoints privados AWS usando AWS PrivateLink. Para obter mais informações, consulte a documentação da Amazon VPC.	Administrador da AWS
Ative a autenticação de dois fatores.	(Opcional) O Atlas fornece suporte à autenticação de dois fatores (2FA) para ajudar os usuários a controlar o acesso às suas contas do Atlas.	Administrador da AWS
Configure a autenticação e autorização do usuário com o LDAP.	(Opcional) O Atlas fornece suporte à autenticação e autorização do usuário com o Lightweight Directory Access Protocol (LDAP).	DBA
Configure o AWS acesso unificado.	(Opcional) Alguns recursos do Atlas, incluindo o Atlas Data Lake e a criptografia em repouso usando o gerenciamento de chaves do cliente, usam funções AWS Identity and Access Management (IAM) para autenticação.	Administrador da AWS
Configure a criptografia em repouso usando AWS KMS.	(Opcional) O Atlas suporta o uso de AWS Key Management Service (AWS KMS) para criptografar mecanismos de armazenamento e backups de provedores de nuvem.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Configurar criptografia em nível de campo do lado do cliente.	(Opcional) O Atlas fornece suporte à criptografia em nível de campo do lado do cliente, incluindo criptografia automática de campos.	Administrador da AWS

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Adicione o MongoDB Relational Migrator à lista de acesso.	Adicione o Relational Migrator à lista de acesso do seu banco de dados de origem. Isso ajuda a preparar o ambiente de origem para se conectar ao cluster Atlas de destino.	DBA
Avalie os objetos do banco de dados relacional.	Inicie o MongoDB Relational Migrator e conecte-se ao seu banco de dados relacional. Inicie a avaliação.	DBA
Aceite os padrões de migração ou opte por alterá-los com base nas necessidades da sua empresa.	Aceite os padrões de banco de dados recomendados pelo Relational Migrator com base na avaliação inicial e nos parâmetros de desempenho, ou opte por alterá-los com base nas necessidades de seus negócios.	DBA
Execute seu conjunto de réplicas de destino no MongoDB Atlas.	Execute seu conjunto de réplicas de destino no MongoDB Atlas. No Relational	DBA

Tarefa	Descrição	Habilidades necessárias
	Migrator, escolha Estou pronto para migrar.	

Configurar integração operacional

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao cluster MongoDB Atlas.	Certifique-se de que a conectividade do cluster MongoDB Atlas funcione conforme o esperado.	Proprietário do App
Interaja com os dados do cluster.	Verifique os dados do cluster.	DBA
Monitore seus clusters.	Verifique se seus clusters estão configurados corretame nte.	DBA
Faça backup e restaure os dados do cluster.	Agende backups com uma cadência regular para dados de cluster.	DBA

Recursos relacionados

Todos os links a seguir, salvo indicação em contrário, vão para páginas da web na documentação do MongoDB.

Guia de migração

- Migrando para o MongoDB AWS Atlas em (orientação prescritiva)AWS

Descoberta e avaliação

- Memória
- Exemplo de dimensionamento com conjuntos de dados de amostra do Atlas

- Exemplo de dimensionamento para aplicativos móveis
- Tráfego de rede
- Ajuste de escala automático de cluster
- Modelo de dimensionamento do Atlas

Configurar a segurança e a conformidade

- Configurar entradas da lista de acesso via IP
- Configurar usuários do banco de dados
- Configurar o acesso à interface do usuário do Atlas
- Configurar funções personalizadas do banco de dados
- Configurar usuários do banco de dados
- Configurar uma conexão de emparelhamento de rede
- Saiba mais sobre endpoints privados no Atlas
- Gerencie suas opções de autenticação multifatorial
- Configurar a autenticação e autorização do usuário com o LDAP
- Atlas Data Lake
- Criptografia em repouso usando o gerenciamento de chaves do cliente
- Métodos para assumir uma função (documentação do IAM)
- Criptografia em nível de campo do lado do cliente
- Criptografia automática
- Controles de segurança do MongoDB Atlas
- Central de confiabilidade do MongoDB
- Configurar recursos de segurança para clusters

Configurando um novo ambiente MongoDB Atlas em AWS

- Provedores de nuvem e regiões
- Gerencie clusters globais
- Selecione o nível do cluster
- Definir configurações adicionais
- Comece a usar o Atlas

- Configurar o acesso à interface do usuário do Atlas
- Gerenciar clusters

Migração de dados

- Migrar ou importar dados

Clusters de monitoramento

- Monitore seus clusters

Integração de operações

- Conectar-se a um cluster
- Interaja com seus dados
- Monitore seus clusters
- Faça backup, restaure e arquive dados

Publicações no blog

- Modernizando esquemas RDBMS com um modelo de documento MongoDB

Migre um ambiente MongoDB auto-hospedado para o MongoDB Atlas em AWS

Criado por Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) e Igor Alekseev (AWS)

Resumo

Esse padrão descreve as etapas para migrar de um ambiente MongoDB autogerenciado (incluindo MongoDB Community Server, Enterprise Server, Enterprise Advanced, MLab ou qualquer cluster MongoDB gerenciado) para o MongoDB Atlas no. Nuvem AWS Ele usa o Atlas Live Migration Service para ajudar a acelerar a migração de dados do MongoDB para o MongoDB Atlas.

O padrão acompanha o guia Migrating to MongoDB Atlas no site Prescriptive Guidance. AWS AWS Ele fornece as etapas de implementação de um dos cenários de migração discutidos nesse guia. Para cenários adicionais de migração, consulte os seguintes padrões no site da Orientação AWS Prescritiva:

- Migre um banco de dados relacional para o MongoDB Atlas em AWS
- Transmita dados do IBM Db2, SAP, Sybase e outros bancos de dados para o MongoDB Atlas em AWS

O padrão é destinado a parceiros e AWS usuários do AWS Systems Integrator (SI).

Pré-requisitos e limitações

Pré-requisitos

- Um MongoDB Enterprise Advanced, Community Server ou outro ambiente MongoDB autogerenciado para migrar para o MongoDB Atlas.
- Familiaridade com MongoDB, MongoDB Atlas e. Serviços da AWS Esse padrão explica algumas das etapas de migração em alto nível. Detalhes adicionais serão adicionados em versões futuras.

Versões do produto

- MongoDB versão 6.0.13 ou posterior

Arquitetura

O diagrama a seguir mostra o Atlas Live Migration Service que é usado para migrar dados de um banco de dados MongoDB Enterprise Advanced e de um banco de dados MongoDB Community

para o MongoDB Atlas on. AWS Use esse serviço quando precisar migrar bancos de dados grandes e complexos para o MongoDB Atlas com o mínimo de tempo de inatividade e sincronização contínua de dados. Esse padrão usa o Atlas Live Migration Service.

O diagrama a seguir mostra o serviço de espelho do MongoDB `mongomirror` () que você também pode usar para migrar dados de um banco de dados MongoDB Enterprise Advanced e de um banco de dados MongoDB Community para o MongoDB Atlas por meio de uma conexão segura. AWS AWS PrivateLink Use `mongomirror` para replicação contínua de dados entre o MongoDB local e o MongoDB Atlas. Essa ferramenta é ideal para recuperação de desastres ou migrações em fases, mas está fora do escopo desse padrão.

Para obter mais arquiteturas de referência do MongoDB Atlas que oferecem suporte a diferentes cenários de uso, consulte Migração para o MongoDB Atlas no site Prescriptive Guidance. AWS AWS

Ferramentas

- O MongoDB Atlas é um banco de dados como serviço (DBaaS) totalmente gerenciado para implantar e gerenciar bancos de dados MongoDB na nuvem.
- O Atlas Live Migration Service é um utilitário gratuito do MongoDB que ajuda a migrar bancos de dados para o Atlas. Este serviço mantém o banco de dados de origem sincronizado com o banco de dados de destino até a substituição. Quando for o momento de realizar a substituição, você irá interromper as instâncias do aplicativo, direcioná-las para o cluster Atlas de destino e reinicializá-las. Para acessar esse serviço, escolha as opções de banco de dados do seu cluster MongoDB Atlas.
- O mongomirror é uma ferramenta para migrar manualmente dados de um conjunto de réplicas existente do MongoDB para um conjunto de réplicas do MongoDB Atlas. `mongomirror`não exige que você encerre seu conjunto de réplicas ou aplicativos existentes, não importa dados do usuário ou da função nem copia o banco de dados de configuração. Você pode fazer o download `mongomirror` da documentação do MongoDB.

Práticas recomendadas

Para obter as melhores práticas para usar o MongoDB AWS no, consulte as postagens no AWS blog do Partner Network.

Épicos

Descoberta e avaliação

Tarefa	Descrição	Habilidades necessárias
Determine o tamanho do cluster.	Estime o tamanho do conjunto de trabalho usando as informações do `db.stats( )` espaço total do índice. Suponha que uma porcentag em do seu espaço de dados seja acessada com frequênci a. Ou você pode estimar seus requisitos de memória com base em suas próprias suposições. Essa tarefa deve levar aproximadamente uma semana. Para obter mais informações e exemplos dessa e de outras histórias deste épico, consulte a seção Recursos relacionados.	DBA, proprietário do aplicativo
Estime os requisitos de largura de banda da rede.	Para estimar seus requisitos de largura de banda da rede, multiplique o tamanho médio dos documentos pelo número de documentos processad os por segundo. Considere o tráfego máximo que qualquer nó do seu cluster suportará como base. Para calcular as taxas de transferência de dados downstream do seu cluster para os aplicativos cliente, use a soma do total de	DBA

Tarefa	Descrição	Habilidades necessárias
	documentos retornados em determinado período. Se seus aplicativos fizerem a leitura a partir de nós secundários, divida esse número total de documentos pelo número de nós que podem processar operações de leitura. Para encontrar o tamanho médio do documento para um banco de dados, use o `db.stats( ).avgObjSize` comando. Essa tarefa normalmente leva um dia.	
Selecione a camada do Atlas.	Siga as instruções na documentação do MongoDB para selecionar a camada correta do cluster Atlas.	DBA
Planeje a transição.	Planeje a substituição do aplicativo.	DBA, proprietário do aplicativo

Configure um novo ambiente MongoDB Atlas na AWS

Tarefa	Descrição	Habilidades necessárias
Crie um novo cluster MongoDB Atlas em. AWS	Faça login no Atlas e abra a página de visão geral do seu projeto. Escolha o botão Criar para criar um cluster. Para obter mais informações, consulte a documentação do MongoDB.	DBA

Tarefa	Descrição	Habilidades necessárias
Selecione Regiões da AWS uma configuração global do cluster.	Selecione na lista de disponíveis Regiões da AWS para seu cluster Atlas. Configure clusters globais, se necessário. Para obter mais informações, consulte a documentação do MongoDB.	DBA
Selecione o nível cluster.	Selecione o nível de cluster de sua preferência. Sua seleção de camadas determina fatores como memória, armazenam ento e especificação de IOPS.	DBA
Configurar definições adicionai s de cluster.	Definir configurações adicionai s de cluster, como opções de versão, backup e criptogra fia do MongoDB. Para obter mais informações sobre essas opções, consulte a seção Recursos relacionados.	DBA

Configure a segurança e a conformidade

Tarefa	Descrição	Habilidades necessárias
Autentique e autorize usuários.	Você deve criar e autentica r os usuários do banco de dados que acessarão os clusters MongoDB Atlas. Para acessar clusters em um projeto, os usuários devem pertencer a esse projeto e podem pertencer a vários projetos. O Atlas também	DBA

Tarefa	Descrição	Habilidades necessárias
	oferece suporte à autentica ção baseada em AWS Identity and Access Managemen t (IAM). Para obter mais informações, consulte a documentação do MongoDB.	
Criar funções personalizadas.	(Opcional) O Atlas oferece suporte à criação de funções personalizadas nos casos em que as permissões de usuário do banco de dados Atlas incorporadas não abrangem o conjunto de permissões que você deseja.	DBA
Configurar o emparelhamento de VPC.	(Opcional) O Atlas oferece suporte ao emparelhamento de nuvem privada virtual (VPC) com outras. VPCs AWS	Administrador da AWS
Configure um AWS PrivateLi nk endpoint.	(Opcional) Você pode configurar endpoints privados AWS usando AWS PrivateLi nk. Para obter mais informaçõ es, consulte a documentação da Amazon VPC.	Administrador da AWS
Ative a autenticação de dois fatores.	(Opcional) O Atlas fornece suporte à autenticação de dois fatores (2FA) para ajudar os usuários a controlar o acesso às suas contas do Atlas.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Configure a autenticação e autorização do usuário com o LDAP.	(Opcional) O Atlas fornece suporte à autenticação e autorização do usuário com o Lightweight Directory Access Protocol (LDAP).	Administrador da AWS
Configure o AWS acesso unificado.	(Opcional) Alguns recursos do Atlas, incluindo o Atlas Data Lake e a criptografia em repouso usando o gerenciam ento de chaves do cliente, usam funções do IAM para autenticação.	Administrador da AWS
Configure a criptografia em repouso usando AWS KMS.	(Opcional) O Atlas suporta o uso de AWS Key Managemen t Service (AWS KMS) para criptografar mecanismos de armazenamento e backups de provedores de nuvem.	Administrador da AWS
Configurar criptografia em nível de campo do lado do cliente.	(Opcional) O Atlas fornece suporte à criptografia em nível de campo do lado do cliente, incluindo criptografia automática de campos.	Administrador da AWS

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Selecione seu conjunto de réplicas de destino no MongoDB Atlas.	Navegue até o cluster Atlas de destino e escolha o botão de elipse (...). Na lista de clusters, esse botão aparece abaixo do	DBA

Tarefa	Descrição	Habilidades necessárias
	nome do cluster. Nos detalhes do cluster, o botão aparece à direita, ao lado dos botões Connect e Configuration. Para obter mais informações, consulte a documentação do MongoDB.	
Adicione o Atlas Live Migration Service à lista de acesso.	Adicione o Atlas Live Migration Service à lista de acesso em seu cluster de AWS origem. Isso ajuda a preparar o ambiente de origem para se conectar ao cluster Atlas de destino.	DBA
Execute a migração com o Atlas Live Migration Service.	Escolha Iniciar migração. Quando o botão Preparar para transferência ficar verde, execute a substitui ção. Analise as métricas de desempenho do cluster Atlas. Considere atualizar a conexão do banco de dados em todas as camadas do aplicativo para apontar para o novo banco de dados.	DBA

Configurar integração operacional

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao cluster MongoDB Atlas.	Certifique-se de que a conectividade do cluster	Proprietário do App

Tarefa	Descrição	Habilidades necessárias
	MongoDB Atlas funcione conforme o esperado.	
Interaja com os dados do cluster.	Teste os dados do cluster.	DBA
Monitore seus clusters.	Verifique se seus clusters estão configurados corretame nte.	DBA
Faça backup e restaure os dados do cluster.	Agende backups com uma cadência regular para dados de cluster.	DBA

Solução de problemas

Problema	Solução

Erro: Não foi possível acessar a fonte especific ada	• Certifique-se de ter adicionado os intervalos de sub-rede corretos à lista de acesso IP no cluster de origem. Você pode encontrar os quatro intervalos de sub-rede necessários na janela modal do Live Migration.
	• Confirme se o nome do host que você especificou foi resolvido para um endereço IP público. Em um prompt de comando, use um dos seguintes comandos:
	`nslookup <hostname>`
	`ping <hostname>`
	• Verifique se você não está usando uma conexão de emparelhamento de VPC, que não é compatível com o pull live migration . Se uma conexão de emparelhamento de

Problema	Solução
	VPC for sua única opção, use em vez disso. `mongomirror`
Erro: Não foi possível resolver o nome do host	Nenhum endereço IP foi encontrado para o nome de host fornecido. Confirme se o nome do host fornecido está correto e acessível ao público.
Qualquer outro erro	Se você encontrar outros erros, consulte Solucionar problemas de migração ao vivo (Pull) na documentação do MongoDB.

Recursos relacionados

Todos os links a seguir, salvo indicação em contrário, vão para páginas da web na documentação do MongoDB.

Guia de migração

- Migrando para o MongoDB AWS Atlas em (orientação prescritiva)AWS

Migração legada

- Migração de versões mais antigas do MongoDB

Descoberta e avaliação

- Memória
- Exemplo de dimensionamento com conjuntos de dados de amostra do Atlas
- Exemplo de dimensionamento para aplicativos móveis
- Tráfego de rede
- Ajuste de escala automático de cluster
- Modelo de dimensionamento do Atlas

Configurar a segurança e a conformidade

- Configurar entradas da lista de acesso via IP
- Configurar usuários do banco de dados
- Configurar o acesso à interface do usuário do Atlas
- Configurar funções personalizadas do banco de dados
- Configurar usuários do banco de dados
- Configurar uma conexão de emparelhamento de rede
- Saiba mais sobre endpoints privados no Atlas
- Gerencie suas opções de autenticação multifatorial
- Configurar a autenticação e autorização do usuário com o LDAP
- Atlas Data Lake
- Criptografia em repouso usando o gerenciamento de chaves do cliente
- Métodos para assumir uma função (documentação do IAM)
- Criptografia em nível de campo do lado do cliente
- Criptografia automática
- Controles de segurança do MongoDB Atlas
- Central de confiabilidade do MongoDB
- Configurar recursos de segurança para clusters

Configurando um novo ambiente MongoDB Atlas em AWS

- Provedores de nuvem e regiões
- Gerencie clusters globais
- Selecione o nível do cluster
- Definir configurações adicionais
- Comece a usar o Atlas
- Configurar o acesso à interface do usuário do Atlas
- Gerenciar clusters

Migração de dados

- Migrar ou importar dados

Clusters de monitoramento

- Monitore seus clusters

Integração de operações

- Conectar-se a um cluster
- Interaja com seus dados
- Monitore seus clusters
- Faça backup, restaure e arquive dados

Treinamento

- Migração ao vivo com o MongoDB Atlas

Mais informações

Para obter informações adicionais, consulte os seguintes tópicos na documentação do MongoDB:

- Para mover dados para uma instância sem servidor, use o Compass para exportar e importar dados, ou migre dados com ferramentas autogerenciadas. Para saber mais, consulte Limitações de instâncias sem servidor.
- Para carregar dados em um novo cluster no Atlas, consulte Carregar dados no Atlas.
- Para fazer uma cópia do seu cluster para fins de teste, consulte Métodos de backup para uma implantação autogerenciada.
- Se o aplicativo que você deseja migrar exigir um tempo de atividade quase contínuo, entre em contato com o Suporte do MongoDB e compartilhe seus requisitos de tempo de atividade e a configuração do cluster.
- Para obter informações adicionais, consulte Migrar ou importar dados.

Migre um banco de dados Oracle JD Edwards EnterpriseOne para a AWS usando o Oracle Data Pump e o AWS DMS

Criado por Thanigaivel Thirumalai (AWS)

Resumo

Você pode migrar e executar seu banco de dados do JD Edwards no Amazon EnterpriseOne Relational Database Service (Amazon RDS). Quando você migra seu banco de dados para o Amazon RDS, a AWS pode cuidar das tarefas de backup e da configuração de alta disponibilidade, para que você possa se concentrar em manter seu EnterpriseOne aplicativo e sua funcionalidade. Para obter uma lista abrangente dos principais fatores a serem considerados durante o processo de migração, consulte as estratégias de migração do banco de dados Oracle nas Recomendações da AWS.

Há várias maneiras de migrar um EnterpriseOne banco de dados, incluindo:

- Usando o Oracle Universal Batch Engine (UBE) R98403 para criação de esquemas e tabelas e usando o AWS Database Migration Service (AWS DMS) para migração
- Usando ferramentas nativas de banco de dados para criação de esquemas e tabelas e usando o AWS DMS para migração
- Usando ferramentas nativas de banco de dados para a migração de dados existentes (carga total) e usando o AWS DMS para tarefas de captura de dados de alteração (CDC - change data capture)

Esse padrão cobre a terceira opção. Ele explica como migrar seus EnterpriseOne bancos de dados locais para o Amazon RDS for Oracle usando o Oracle Data Pump com o AWS DMS e seu recurso CDC.

O Oracle JD Edwards EnterpriseOne é uma solução de planejamento de recursos corporativos (ERP) para organizações que fabricam, constroem, distribuem, atendem ou gerenciam produtos ou ativos físicos. O JD Edwards EnterpriseOne oferece suporte a vários hardwares, sistemas operacionais e plataformas de banco de dados.

Quando você migra aplicativos essenciais de ERP, como o JD Edwards EnterpriseOne, minimizar o tempo de inatividade é fundamental. O AWS DMS minimiza o tempo de inatividade ao oferecer suporte à carga total e à replicação contínua do banco de dados de origem para o banco de dados de destino. O AWS DMS também fornece monitoramento e registro em tempo real para a migração, o que pode ajudá-lo a identificar e resolver quaisquer problemas que possam causar tempo de inatividade.

Ao replicar alterações com o AWS DMS, você deve especificar uma hora ou um número de alteração do sistema (SCN) como ponto de partida para ler as alterações dos logs do banco de dados. É fundamental manter esses registros acessíveis no servidor por um determinado período de tempo (recomendamos 15 dias) para garantir que o AWS DMS tenha acesso a essas alterações.

Pré-requisitos e limitações

Pré-requisitos

- Um banco de dados Amazon RDS para Oracle provisionado em seu ambiente de Nuvem AWS como o banco de dados de destino. Para obter instruções, consulte a documentação do Amazon RDS.
- Um EnterpriseOne banco de dados executado no local ou em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) na AWS.

> **Note**
>
> Esse padrão foi projetado para migrar do local para a AWS, mas foi testado usando um EnterpriseOne banco de dados em uma EC2 instância. Se você planeja migrar do seu ambiente on-premises, deverá configurar a conectividade de rede apropriada.

- Detalhes do esquema. Identifique para qual esquema de banco de dados Oracle (por exemplo, DV92 0) você planeja migrar. EnterpriseOne Antes de iniciar o processo de migração, reúna os seguintes detalhes sobre o esquema:
  - Tamanho do esquema
  - O número de objetos por tipo de objeto
  - O número de objetos inválidos

Limitações

- Você precisa criar os esquemas que quiser no banco de dados Amazon RDS para Oracle de destino: o AWS DMS não os cria para você. (A seção Épicos descreve como usar o Data Pump para exportar e importar esquemas). O nome do esquema já deve existir para o banco de dados Oracle de destino. As tabelas do esquema de origem são importadas para o usuário ou esquema e o AWS DMS usa a conta do administrador ou do sistema para se conectar à instância de destino. Para migrar vários esquemas, você pode criar várias tarefas de replicação. Você também pode

migrar dados para esquemas diferentes em uma instância de destino. Para fazer isso, use regras de transformação de esquema nos mapeamentos de tabelas do AWS DMS.

- Esse padrão foi testado com um conjunto de dados de demonstração. Recomendamos que você valide a compatibilidade do seu conjunto de dados e da personalização.
- Esse padrão usa um EnterpriseOne banco de dados que está sendo executado no Microsoft Windows. No entanto, você pode usar o mesmo processo com outros sistemas operacionais compatíveis com o AWS DMS.

Arquitetura

O diagrama a seguir mostra um sistema que está sendo executado EnterpriseOne em um banco de dados Oracle como banco de dados de origem e um banco de dados Amazon RDS for Oracle como banco de dados de destino. Os dados são exportados do banco de dados Oracle de origem e importados para o banco de dados Amazon RDS para Oracle de destino usando o Oracle Data Pump e replicados para atualizações do CDC usando o AWS DMS.

1. O Oracle Data Pump extrai dados do banco de dados de origem e os dados são enviados para o destino do banco de dados Amazon RDS para Oracle.
2. Os dados do CDC são enviados do banco de dados de origem para um endpoint de origem no AWS DMS.
3. Do endpoint de origem, os dados são enviados para a instância de replicação do AWS DMS, onde a tarefa de replicação é executada.
4. Após a conclusão da tarefa de replicação, os dados são enviados para o endpoint de destino no AWS DMS.
5. Do endpoint de destino, os dados são enviados para a instância do banco de dados do Amazon RDS para Oracle.

Ferramentas

Serviços da AWS

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O Amazon Relational Database Service (Amazon RDS) para Oracle ajuda você a configurar, operar e escalar um banco de dados relacional Oracle na Nuvem AWS.

Outros serviços

- O Oracle Data Pump ajuda você a mover dados e metadados de um banco de dados para outro em alta velocidade.

Práticas recomendadas

Migrating LOBs

Se seu banco de dados de origem contiver objetos binários grandes (LOBs) que precisam ser migrados para o banco de dados de destino, o AWS DMS fornece as seguintes opções:

- Modo LOB completo — O AWS DMS migra tudo do banco de dados LOBs de origem para o de destino, independentemente do tamanho. Embora a migração seja mais lenta do que os outros modos, a vantagem é que os dados não são truncados. Para melhorar o desempenho, você pode criar uma tarefa separada na nova instância de replicação para migrar as tabelas maiores do LOBs que alguns megabytes.
- Modo LOB limitado — Você especifica o tamanho máximo dos dados da coluna LOB, o que permite que o AWS DMS pré-aloque recursos e os aplique em massa. LOBs Se o tamanho das colunas LOB exceder o tamanho especificado na tarefa, o AWS DMS truncará os dados e enviará avisos para o arquivo de log do AWS DMS. Você pode melhorar o desempenho usando o modo LOB limitado se o tamanho dos dados do LOB estiver dentro do tamanho do LOB limitado.
- Modo LOB embutido — você pode migrar LOBs sem truncar os dados ou diminuir o desempenho de sua tarefa replicando tanto pequenos quanto grandes. LOBs Primeiro, especifique um valor para o parâmetro `InlineLobMaxSize`, que está disponível somente quando o modo LOB completo está definido como `true`. A tarefa do AWS DMS transfere o pequeno LOBs em linha, o que é mais eficiente. Em seguida, o AWS DMS migra os grandes LOBs executando uma pesquisa na tabela de origem. No entanto, o modo LOB em linha funciona somente durante a fase de carga total.

Gerando valores de sequência

Durante o processo de CDC do AWS DMS, os números de sequência incrementais não são replicados do banco de dados de origem. Para evitar discrepâncias nos valores de sequência, você deve gerar o valor de sequência mais recente da origem para todas as sequências e aplicá-lo ao banco de dados de destino do Amazon RDS para Oracle.

AWS Secrets Manager

Para ajudar a gerenciar suas credenciais, recomendamos que você siga as instruções na postagem do blog Gerencie suas credenciais de endpoint do AWS DMS com o AWS Secrets Manager.

Desempenho

- Instâncias de replicação – Para obter orientação sobre como escolher o melhor tamanho de instância, consulte Seleção do melhor tamanho para uma instância de replicação na documentação do AWS DMS.
- Opções de conectividade – Para evitar problemas de latência, recomendamos que você escolha a opção de conectividade correta. O AWS Direct Connect fornece o caminho mais curto para os recursos da AWS, porque é uma conexão dedicada entre seus datacenters corporativos e a AWS. Em trânsito, o tráfego de rede permanece na rede global da AWS e nunca passa pela Internet. Isso reduz a chance de ocorrer gargalos ou aumentos inesperados na latência em comparação com o uso de VPN ou de internet pública.
- Largura de banda da rede – Para otimizar o desempenho, verifique se a throughput de sua rede é rápida. Se você estiver usando um túnel VPN entre seu banco de dados de origem on-premises e o AWS DMS, garanta que a largura de banda seja suficiente para seu workload.
- Paralelismo de tarefas – Você pode acelerar a replicação de dados carregando várias tabelas em paralelo durante a carga total. Esse padrão usa endpoints RDBMS, portanto, essa opção se aplica somente ao processo de carregamento completo. O paralelismo de tarefas é controlado pelo parâmetro `MaxFullLoadSubTasks`, que determina quantas subtarefas de carga total são executadas em paralelo. Por padrão, esse parâmetro é definido como 8, o que significa que oito tabelas (se selecionadas no mapeamento de tabelas) são carregadas juntas durante o modo completo. Você pode ajustar esse parâmetro na seção de configurações de tarefa de carga total do script JSON para a tarefa.
- Paralelismo de tabelas – O AWS DMS também permite que você carregue uma única tabela grande usando vários threads paralelos. Isso é particularmente útil para tabelas de origem Oracle que têm bilhões de registros, bem como várias partições e subpartições. Se a tabela de origem não estiver particionada, você poderá usar limites de coluna para cargas paralelas.
- Divida as cargas – Ao dividir as cargas em várias tarefas ou instâncias do AWS DMS, lembre-se dos limites da transação ao capturar as alterações.

Épicos

Use o Oracle Data Pump para exportar o EnterpriseOne esquema

Tarefa	Descrição	Habilidades necessárias

Gere o SCN.	Quando o banco de dados de origem estiver ativo e em uso pelo EnterpriseOne aplicativo, inicie a exportaçã o de dados com o Oracle Data Pump. Primeiro, você deve gerar um número de alteração do sistema (SCN) do banco de dados de origem para manter a consistência de dados durante a exportação com o Oracle Data Pump e como ponto de partida para o CDC no AWS DMS.
	
	Para gerar o SCN atual do banco de dados de origem, use a instrução SQL a seguir:
	
	`SQL> select current_scn from v$database;`
	
	`CURRENT_SCN`
	`-----------`
	`30009727`
	
	Salve o SCN gerado. Você usará o SCN ao exportar os dados e criar a tarefa de replicação do AWS DMS.
		DBA

Crie o arquivo de parâmetro.	Para criar um arquivo de parâmetros para exportar o	DBA

Tarefa	Descrição	Habilidades necessárias

	esquema, você pode usar o código a seguir.
	
	`directory=DMS_DATA_PUMP_DIR logfile=export_dms.log dumpfile=export_dms_data.dmp schemas=<schema name> flashback_scn=<SCN from previous command>`
	
	Note
	Você também pode definir seus próprios comandos DATA_PUMP_DIR usando os comandos a seguir, com base em seus requisitos.
	
	`SQL> CREATE OR REPLACE DIRECTORY DMS_DATA_PUMP_DIR AS '<Directory for dump>'; Directory created.`
	
	`SQL> GRANT READ, WRITE ON DIRECTORY DMS_DATA_PUMP_DIR TO SYSTEM; Grant succeeded.`	

Tarefa	Descrição	Habilidades necessárias

Exporte o esquema.	Para realizar a exportação, use o utilitário expdp da seguinte forma:
	
	`C:\Users\Administrator>expdp system/********@<DB Name> PARFILE='<Path to PAR file create above>'`
	
	`Export: Release 19.0.0.0.0 - Production on *** *** ** **:**:** **** Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production Starting "SYSTEM"."SYS_EXPORT_SCHEMA_02": system/******@<DB Name>PARFILE='E:\exp_dms_datapump.par' Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA Processing object type SCHEMA_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS Processing object type SCHEMA_EXPORT/TABL`
		DBA

Tarefa	Descrição	Habilidades necessárias
	E/STATISTICS/TABLE _STATISTICS Processing object type SCHEMA_EXPORT/STAT ISTICS/MARKER Processing object type SCHEMA_EXPORT/USER Processing object type SCHEMA_EXPORT/ROLE _GRANT Processing object type SCHEMA_EXPORT/DEFA ULT_ROLE Processing object type SCHEMA_EXPORT/TABL ESPACE_QUOTA Processing object type SCHEMA_EXPORT/PRE_ SCHEMA/PROCACT_SCHEMA Processing object type SCHEMA_EXPORT/TABLE/ TABLE Processing object type SCHEMA_EXPORT/TABL E/GRANT/OWNER_GRANT/ OBJECT_GRANT Processing object type SCHEMA_EXPORT/TABLE/ INDEX/INDEX Processing object type SCHEMA_EXPORT/TABLE/ CONSTRAINT/CONSTRAINT . . exported "<Schema Name>"."<Table Name>" 228.9 MB 496397 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _02" successfully loaded/unloaded	

Tarefa	Descrição	Habilidades necessárias
	``` ********** ********** ********** ********** **** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_02 is: E:\DMSDUMP\EXPORT_ DMS_DATA.DMP Job "SYSTEM"."SYS_EXPO RT_SCHEMA_02" successfully completed at *** *** ** **:**:** **** elapsed 0 00:01:57 ```	

Use o Oracle Data Pump para importar o EnterpriseOne esquema

Tarefa	Descrição	Habilidades necessárias
Transfira o arquivo de dump para a instância de destino.	Para transferir seus arquivos usando o utilitário `DBMS_FILE_TRANSFER`, você precisa criar um link de banco de dados do banco de dados de origem para a instância do Amazon RDS para Oracle. Depois que o link for estabelecido, você poderá usar o utilitário para transferir os arquivos do Data Pump diretamente para a instância do Amazon RDS. Como alternativa, você pode transferir os arquivos do Data Pump para o Amazon Simple	DBA

Tarefa	Descrição	Habilidades necessárias

	Storage Service (Amazon S3) e depois importá-los para a instância do Amazon RDS para Oracle. Para obter mais informações sobre essa opção, consulte a seção Informações adicionais.
	
	Para criar um link `ORARDSDB` que se conecte ao usuário mestre do Amazon RDS na instância de banco de dados de destino, execute os comandos a seguir no banco de dados de origem:
	
	`sqlplus / as sysdba`
	
	`SQL*Plus: Release 19.0.0.0.0 on *** *** ** **:**:** **** Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle. All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 Version 19.3.0.0.0`
	
	`SQL> create database link orardsdb connect to admin identifie d by "******" using '(DESCRIPTION = (ADDRESS = (PROTOCOL =`	

Tarefa	Descrição	Habilidades necessárias
	TCP)(HOST = orcl.**** **.us-east-1.rds.a mazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))'; Database link created. SQL>	
Teste o link do banco de dados.	Teste o link do banco de dados para garantir que você possa se conectar ao banco de dados de destino do Amazon RDS para Oracle usando `sqlplus`. SQL> select name from v $database@orardsdb; NAME --------- ORCL	DBA

Tarefa	Descrição	Habilidades necessárias

Transfira o arquivo dump para o banco de dados de destino.	Para copiar o arquivo de despejo para o banco de dados Amazon RDS para Oracle, você pode usar o diretório DATA_PUMP_DIR padrão ou criar seu próprio diretório usando o código a seguir, que deve ser executado na instância de destino do Amazon RDS:
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'DMS_TARGET_PUMP_DIR');`
	`PL/SQL procedure successfully completed.`
	O script a seguir copia um arquivo de despejo chamado EXPORT_DMS_DATA.DMP da instância de origem para um banco de dados de destino do Amazon RDS para Oracle usando o link de banco de dados chamado orardsdb. Você deve executar o script na instância do banco de dados de origem.
	`BEGIN DBMS_FILE_TRANSFER.PUT_FILE(`
		DBA

Tarefa	Descrição	Habilidades necessárias

	`source_directory_object => 'DMS_DATA_PUMP_DIR', source_file_name => 'EXPORT_DMS_DATA.DMP', destination_directory_object => 'DMS_TARGET_PUMP_DIR', destination_file_name => 'EXPORT_DMS_DATA.DMP', destination_database => 'orardsdb'); END;`
	
	`PL/SQL procedure successfully completed.`	

Liste o arquivo dump no banco de dados de destino.	Depois que o procedimento PL/SQL for concluído, você poderá listar o arquivo de despejo de dados no banco de dados Amazon RDS para Oracle usando o seguinte código: `select * from table (rdsadmin.rds_file_util.listdir(p_directory => 'DMS_TARGET_PUMP_DIR'));`	DBA

Tarefa	Descrição	Habilidades necessárias

Crie usuários específicos do JDE na instância de destino.	Crie um perfil e uma função do JD Edwards usando esses comandos na instância de destino:
	
	`SQL> CREATE PROFILE "JDEPROFILE" LIMIT IDLE_TIME 15;`
	`Profile created.`
	
	`SQL> CREATE ROLE "JDE_ROLE";`
	`Role created.`
	
	`SQL> CREATE ROLE "JDEADMIN";`
	`CREATE ROLE "JDEUSER";`
	`Role created.`
	`Role created.`
	
	Conceda as permissões necessárias à função:
	
	`SQL> GRANT CREATE ANY SEQUENCE TO JDE_ROLE;`
	`GRANT DROP ANY SEQUENCE TO JDE_ROLE;`
	`GRANT CREATE ANY TRIGGER TO JDE_ROLE;`
	`GRANT DROP ANY TRIGGER TO JDE_ROLE;`
		DBA, JDE CNC

Tarefa	Descrição	Habilidades necessárias

Crie espaços de tabela na instância de destino.	Crie os espaços de tabela necessários na instância de destino usando os seguintes comandos para os esquemas envolvidos nessa migração:
	`SQL> CREATE TABLESPACE <Tablespace Name for Tables>;`
	`Tablespace created.`
	
	`SQL> CREATE TABLESPACE <Tablespace Name for Indexes>;`
	`Tablespace created.`
		DBA, JDE CNC

Tarefa	Descrição	Habilidades necessárias
Inicie a importação no banco de dados de destino.	Antes de iniciar o processo de importação, configure as funções, os esquemas e os espaços de tabela no banco de dados de destino do Amazon RDS para Oracle usando o arquivo de dump de dados. Para realizar a importação, acesse o banco de dados de destino com a conta de usuário principal do Amazon RDS e use o nome da cadeia de conexão no arquivo `tnsnames.ora` , que inclui o Amazon RDS para Oracle Database `tns-entry` . Se necessário, você pode incluir uma opção de remapeamento para importar o arquivo de dump de dados em um espaço de tabela diferente ou com um nome de esquema diferente. Para iniciar a importação, use o seguinte código: `impdp admin@orardsdb directory=DMS_TARGET_PUMP_DIR logfile=import.log dumpfile=EXPORT_DMS_DATA.DMP`	DBA

Tarefa	Descrição	Habilidades necessárias
	Para garantir uma importação bem-sucedida, verifique se há erros no arquivo de log de importação e revise os detalhes, como contagem de objetos, contagem de linhas e objetos inválidos. Se houver algum objeto inválido, recompile-o. Além disso, compare os objetos do banco de dados de origem e de destino para confirmar se eles coincidem.	

Provisione uma instância de replicação do AWS DMS com os endpoints de origem e de destino

Tarefa	Descrição	Habilidades necessárias
Faça download do modelo.	Faça o download do modelo AWS CloudFormation DMS_Instance.yaml para provisionar a instância de replicação do AWS DMS e seus endpoints de origem e destino.	Administrador de nuvem, DBA
Inicie a criação da pilha.	1. Faça login no AWS Management Console e abra o CloudFormation console da AWS em https://console.aws.amazon.com/cloudformation. 2. Selecione Criar pilha.	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
	3. Em Specify template (Especificar modelo), escolha Upload a template file (Fazer upload de um arquivo de modelo). 4. Escolha Escolher arquivo. 5. Escolha o arquivo `DMS_instance.yaml` . 6. Escolha Próximo.	

Tarefa	Descrição	Habilidades necessárias
Especifique os parâmetros.	1. Em Nome da pilha, insira o nome da pilha. 2. Para parâmetros de instância do AWS DMS, insira os seguintes parâmetros: • DMSInstanceTipo — Escolha a instância necessária para a instância de replicação do AWS DMS, com base nas necessidades da sua empresa. • DMSStorageTamanho — Insira o tamanho do armazenamento para a instância do AWS DMS, com base no tamanho da sua migração. 3. Para Configuração do banco de dados Oracle de origem, insira os seguintes parâmetros: • SourceOracleEndpointID — O nome do servidor do banco de dados Oracle de origem • SourceOracleDatabaseName— O nome do serviço do banco de dados de origem ou o ID da sessão (SID), conforme aplicável	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
	• SourceOracleUserName— O nome de usuário do banco de dados de origem (o padrão é `system`) • SourceOracleDBPassword— A senha do nome de usuário do banco de dados de origem • SourceOracleDBPort— A porta do banco de dados de origem 4. Para Configuração do banco de dados Oracle de destino, insira os seguintes parâmetros: • Target RDSOracle EndpointID — O endpoint do banco de dados RDS de destino • Destino RDSOracle DatabaseName — O nome do banco de dados RDS de destino • Target RSOracle UserName — O nome de usuário do RDS de destino • Alvo RDSOracle DBPassword — A senha do RDS de destino	

Tarefa	Descrição	Habilidades necessárias
	• TargetOracleDBPort— A porta do banco de dados RDS de destino 5. Para configuração de VPC, sub-rede e grupo de segurança, insira os seguintes parâmetros: • VPCID: a VPC para a instância de replicação • VPCSecurityGroupId— O grupo de segurança VPC para a instância de replicação • DMSSubnet1— A sub-rede da Zona de Disponibilidade 1 • DMSSubnet2— A sub-rede da Zona de Disponibilidade 2 6. Escolha Próximo.	

Tarefa	Descrição	Habilidades necessárias
Crie a pilha.	1. Na página Configurar opções de pilha, em Tags, insira quaisquer valores opcionais. 2. Escolha Próximo. 3. Na página Revisar, verifique os detalhes e escolha Enviar. O provisionamento deve ser concluído em aproximad amente cinco a dez minutos. Ele estará completo quando a página AWS CloudFormation Stacks mostrar CREATE_CO MPLETE.	Administrador de nuvem, DBA
Configure os endpoints.	1. Abra o console do AWS DMS em https://console.aws.amazon.com/dms/v2/. 2. Para gerenciamento de recursos, escolha Instância s de replicação e, em seguida, revise as instância s de replicação. 3. Para Gerenciamento de recursos, escolha Endpoints e, em seguida, revise os endpoints.	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
Teste de conectividade.	Depois que os endpoints de origem e destino mostrarem o status como Ativo, teste a conectividade. Escolha Executar teste para cada endpoint (origem e destino) para garantir que o status seja exibido como bem-sucedido.	Administrador de nuvem, DBA

Crie uma tarefa de replicação do AWS DMS para replicação ao vivo

Tarefa	Descrição	Habilidades necessárias
Crie a tarefa de replicação.	Crie a tarefa de replicação do AWS DMS usando as seguintes etapas: 1. Abra o console do AWS DMS em https://console.aws.amazon.com/dms/v2/. 2. No painel de navegação, em Migrar dados, escolha Tarefa de migração de banco de dados. 3. Na caixa Configuração da tarefa, em Identificador da tarefa, insira o identificador da tarefa. 4. Em Instância de replicação, escolha a instância de replicação DMS que você criou.	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
	5. Para Endpoint do banco de dados de origem, escolha seu endpoint de origem. 6. Para o endpoint do banco de dados de destino, escolha seu banco de dados Amazon RDS para Oracle de destino. 7. Em Tipo de migração, escolha Replicar somente alterações de dados. Se você receber uma mensagem informando que o registro complementar precisa ser ativado, siga as instruções na seção Solução de problemas. 8. Na caixa Configurações da tarefa, escolha Especificar número de sequência de log. 9. Em Número de alteração do sistema, insira o SCN do banco de dados do Oracle que você gerou do banco de dados do Oracle de origem. 10 Escolha Ativar validação. 11 Escolha Ativar CloudWatch registros. Ao ativar esse recurso, você pode validar os dados e os registros da Amazon	

Tarefa	Descrição	Habilidades necessárias
	para revisar CloudWatch os registros da instância de replicação do AWS DMS. 12 Em Regras de seleção, preencha o seguinte: • Em Esquema, escolha Insira um esquema. • Em Nome do esquema, insira o nome do esquema JDE (por exemplo: DV92 0). • Em Nome da tabela, insira %. • Em Ação, escolha Incluir. 13 Escolha Criar tarefa. Depois de criar a tarefa, o AWS DMS migra as alterações contínuas para a instância do banco de dados Amazon RDS para Oracle a partir do SCN que você forneceu no modo de início do CDC. Você também pode verificar a migração revisando os CloudWatch registros.	
Repita a tarefa de replicação.	Repita as etapas anteriores para criar tarefas de replicação para outros esquemas do JD Edwards que fazem parte da migração.	Administrador de nuvem, DBA, administrador CNC do JDE

Valide o esquema de banco de dados no banco de dados de destino do Amazon RDS para Oracle

Tarefa	Descrição	Habilidades necessárias
Validar a transferência de dados.	Após o início da tarefa do AWS DMS, você pode verificar a guia Estatísticas da tabela na página Tarefas para ver as alterações feitas nos dados. Você pode monitorar o status da replicação contínua no console na página Tarefas de migração do banco de dados. Para obter mais informações, consulte Validação de dados do AWS DMS.	Administrador de nuvem, DBA

Substituir

Tarefa	Descrição	Habilidades necessárias
Encerrar a replicação.	Interrompa o procedimento de replicação e interrompa os serviços do aplicativo de origem.	Administrador de nuvem, DBA
Inicie o aplicativo JD Edwards.	Inicie a apresentação de destino e o aplicativo de nível lógico do JD Edwards na AWS e direcione-os para o banco de dados Amazon RDS para Oracle.	DBA, administrador do JDE CNC

Tarefa	Descrição	Habilidades necessárias
	Ao acessar o aplicativo, você deve observar que todas as conexões agora estão estabelecidas com o banco de dados Amazon RDS para Oracle.	
Desative o banco de dados de origem.	Depois de confirmar que não há mais conexões, você pode desativar o banco de dados de origem.	DBA

Solução de problemas

Problema	Solução

Você recebe uma mensagem de aviso para ativar o log complementar no banco de dados de origem para replicação contínua	Insira estes comandos para ativar o log complementar:
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`

O AWS DMS fica com o registro suplementar desativado.	O log complementar está desativado por padrão no AWS DMS. Para ativá-lo em um endpoint Oracle de origem:

Problema	Solução
	1. Faça login no AWS Management Console e abra o console do AWS DMS em https://console.aws.amazon.com/dms/v2/. 2. Selecione Endpoints. 3. Selecione o endpoint de origem do Oracle ao qual deseja adicionar o log complementar. 4. Escolha Modificar. 5. Selecione Avançado e adicione o seguinte código à caixa de texto Atributos de conexão extra: `addSupplementalLogging=Y` 6. Escolha Modificar.

O log complementar não está habilitado no nível do CDB.	1. Insira este comando:
	`SQL> alter session set container = CDB$ROOT;`
	`Session altered.`
	2. Repita as etapas para habilitar o log complementar.

Você recebe a mensagem de erro: “Falha no Test Endpoint: Application-Status: 1020912, Application-Message: não LogMiner é suportado no ambiente Oracle PDB A inicialização do Endpoint falhou.”	Se você encontrar essa mensagem de erro, poderá usar o Binary Reader em vez de LogMiner. Em Configurações do Endpoint, adicione essa linha aos atributos extras de conexão do seu banco de dados de origem: `useLogMinerReader=N;useBfile=Y;`

Recursos relacionados

- Introdução ao AWS Database Migration Service
- Práticas recomendadas para o AWS Database Migration Service
- Migrar bancos de dados Oracle para a Nuvem AWS
- Referência de tipo de recurso do AWS Database Migration Service para AWS CloudFormation
- Gerencie suas credenciais de endpoint do AWS DMS com o AWS Secrets Manager
- Solução de problemas de tarefas de migração no AWS Database Migration Service
- Práticas recomendadas para o AWS Database Migration Service

Mais informações

Transferir arquivos usando o Amazon S3

Para transferir os arquivos para o Amazon S3, você pode usar a AWS CLI ou o console do Amazon S3. Depois de transferir os arquivos para o Amazon S3, você pode usar a instância Amazon RDS para Oracle para importar os arquivos do Data Pump do Amazon S3.

Se você optar por transferir o arquivo de dump usando a integração com o Amazon S3 como um método alternativo, execute as seguintes etapas:

1. Criar um bucket do S3.
2. Exporte os dados do banco de dados de origem usando o Oracle Data Pump.
3. Faça upload dos arquivos do Data Pump para o bucket S3.
4. Faça download dos arquivos do Data Pump do bucket do S3 no banco de dados de destino do Amazon RDS para Oracle.
5. Execute a importação usando os arquivos do Data Pump.

> **Note**
>
> Para transferir grandes arquivos de dados entre instâncias do S3 e do RDS, recomendamos que você use o recurso Amazon S3 Transfer Acceleration.

Migre um PeopleSoft banco de dados Oracle para a AWS usando o AWS DMS

Criado por sampath kathirvel (AWS)

Resumo

PeopleSoftO Oracle é uma solução de planejamento de recursos corporativos (ERP) para processos em toda a empresa. PeopleSoft tem uma arquitetura de três camadas: cliente, aplicativo e banco de dados. PeopleSoft pode ser executado no Amazon Relational Database Service (Amazon RDS).

Se você migrar seu banco de dados Oracle para o Amazon RDS, o Amazon Web Services (AWS) poderá cuidar das tarefas de backup e da alta disponibilidade, deixando você livre para se concentrar na manutenção do PeopleSoft aplicativo e de sua funcionalidade. Para obter uma lista abrangente dos principais fatores a serem considerados durante o processo de migração, consulte as estratégias de migração do banco de dados Oracle nas Recomendações da AWS.

Esse padrão fornece uma solução para migrar seus bancos de dados do Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump com o AWS Database Migration Service (AWS DMS) e seu atributo de captura de dados de alteração (CDC).

Ao migrar aplicativos essenciais de ERP, como o Oracle PeopleSoft, minimizar o tempo de inatividade é fundamental. O AWS DMS minimiza o tempo de inatividade ao oferecer suporte à carga total e à replicação contínua do banco de dados de origem para o banco de dados de destino. O AWS DMS também fornece monitoramento e registro em tempo real da migração, o que pode ajudar você a identificar e resolver quaisquer problemas que possam causar tempo de inatividade.

Ao replicar alterações com o AWS DMS, você deve especificar um horário ou um número de alteração do sistema (SCN) como ponto de partida para que o AWS DMS leia as alterações dos registros em log do banco de dados. É fundamental manter esses logs acessíveis no servidor por um determinado período de tempo para garantir que o AWS DMS tenha acesso a essas alterações.

Pré-requisitos e limitações

Pré-requisitos

- Provisionado banco de dados do Amazon RDS para Oracle em seu ambiente de nuvem AWS como banco de dados de destino.
- Um PeopleSoft banco de dados Oracle executado no local ou na Amazon Elastic Compute Cloud (Amazon EC2) na Nuvem AWS.

> **Note**
>
> Esse padrão foi projetado para migrar do local para a AWS, mas foi testado usando o Oracle Database em uma EC2 instância da Amazon. Para migrar do on-premises, você precisará configurar a conectividade de rede apropriada.

- Detalhes do esquema. Ao migrar um PeopleSoft aplicativo Oracle para o Amazon RDS for Oracle, é necessário identificar qual esquema de banco de dados Oracle (por exemplo`SYSADM`,) migrar. Antes de iniciar o processo de migração, reúna os seguintes detalhes sobre o esquema:
  - Tamanho
  - O número de objetos por tipo de objeto
  - O número de objetos inválidos.

  Essas informações ajudarão no processo de migração.

Limitações

- Esse cenário foi testado somente com o banco de dados PeopleSoft DEMO. Ele não foi testado com um grande conjunto de dados.

Arquitetura

O diagrama a seguir mostra uma instância executando um banco de dados do Oracle como banco de dados de origem e um banco de dados do Amazon RDS para Oracle como banco de dados de destino. Os dados são exportados e importados do banco de dados do Oracle de origem para o banco de dados do Amazon RDS para Oracle de destino usando o Oracle Data Pump e replicados para alterações do CDC usando o AWS DMS.

1. A etapa inicial envolve a extração de dados do banco de dados de origem usando o Oracle Data Pump e, em seguida, o envio para o banco de dados de destino do Amazon RDS para Oracle.
2. Os dados são enviados do banco de dados de origem para um endpoint de origem no AWS DMS.
3. Do endpoint de origem, os dados são enviados para a instância de replicação do AWS DMS, onde a tarefa de replicação é executada.
4. Após a conclusão da tarefa de replicação, os dados são enviados para o endpoint de destino no AWS DMS.

5. Do endpoint de destino, os dados são enviados para a instância do banco de dados do Amazon RDS para Oracle.

Ferramentas

Serviços da AWS

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- O Amazon Relational Database Service (Amazon RDS) para Oracle ajuda você a configurar, operar e escalar um banco de dados relacional Oracle na Nuvem AWS.

Outros serviços

- O Oracle Data Pump ajuda você a mover dados e metadados de um banco de dados para outro em alta velocidade.

Práticas recomendadas

Migrating LOBs

Se seu banco de dados de origem contiver objetos binários grandes (LOBs) que precisam ser migrados para o banco de dados de destino, o AWS DMS fornece as seguintes opções:

- Modo LOB completo — O AWS DMS migra tudo do banco de dados LOBs de origem para o de destino, independentemente do tamanho. Embora a migração seja mais lenta, a vantagem é que os dados não são truncados. Para melhorar o desempenho, você pode criar uma tarefa separada na nova instância de replicação para migrar as tabelas com mais de alguns LOBs megabytes.
- Modo LOB limitado — Você especifica o tamanho máximo dos dados da coluna LOB, o que permite que o AWS DMS pré-aloque recursos e os aplique em massa. LOBs Se o tamanho das colunas LOB exceder o tamanho especificado na tarefa, o AWS DMS truncará os dados e enviará avisos para o arquivo de log do AWS DMS. Você pode melhorar o desempenho usando o modo LOB limitado se o tamanho dos dados do LOB estiver dentro do tamanho do LOB limitado.
- Modo LOB embutido — você pode migrar LOBs sem truncar os dados ou diminuir o desempenho de sua tarefa replicando tanto pequenos quanto grandes. LOBs Primeiro, especifique um valor para o InlineLobMaxSize parâmetro, que está disponível somente quando o modo LOB completo está definido como verdadeiro. A tarefa do AWS DMS transfere o pequeno LOBs em linha, o que

é mais eficiente. Em seguida, o AWS DMS migra os grandes LOBs executando uma pesquisa na tabela de origem. No entanto, o modo LOB em linha funciona somente durante a fase de carga total.

Gerando valores de sequência

Lembre-se de que, durante o processo de captura de dados de alterações com o AWS DMS, os números de sequência incrementais não são replicados do banco de dados de origem. Para evitar discrepâncias nos valores de sequência, você deve gerar o valor de sequência mais recente da origem para todas as sequências e aplicá-lo ao banco de dados de destino do Amazon RDS para Oracle.

Gerenciamento de credenciais

Para ajudar a proteger seus recursos da AWS, recomendamos seguir as práticas recomendadas do AWS Identity and Access Management (IAM).

Épicos

Provisione uma instância de replicação do AWS DMS com os endpoints de origem e de destino

Tarefa	Descrição	Habilidades necessárias
Faça download do modelo.	Baixe o CloudFormation modelo da AWS DMS_Instance.yaml para provisionar a instância de replicação do AWS DMS e seus endpoints de origem e destino.	Administrador de nuvem, DBA
Inicie a criação da pilha.	1. No AWS Management Console, escolha CloudFormation. 2. Selecione Criar pilha. 3. Em Specify template (Especificar modelo), escolha Upload a template file (Fazer upload de um arquivo de modelo).	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
	4. Escolha Escolher arquivo. 5. Escolha o arquivo `DMS_instance.yaml` . 6. Escolha Próximo.	

Tarefa	Descrição	Habilidades necessárias
Especifique os parâmetros.	1. Em Nome da pilha, insira o nome da pilha. 2. Em Parâmetros de instância do AWS DMS, insira os seguintes parâmetros: • DMSInstanceTipo — Escolha a instância necessária para a instância de replicação do AWS DMS, com base nas necessidades da sua empresa. • DMSStorageTamanho — Insira o tamanho do armazenamento para a instância do AWS DMS, com base no tamanho da sua migração. 3. Em Configuração do banco de dados do Oracle de origem, insira os seguintes parâmetros: • SourceOracleEndpointID — O nome do servidor do banco de dados Oracle de origem • SourceOracleDatabaseName— O nome do serviço do banco de dados de origem ou o ID da sessão (SID), conforme aplicável	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
	• SourceOracleUserName— O nome de usuário do banco de dados de origem (o padrão é sistema) • SourceOracleDBPassword— A senha do nome de usuário do banco de dados de origem • SourceOracleDBPort— A porta do banco de dados de origem 4. Para Configuração do banco de dados Oracle de destino RDS, insira os seguintes parâmetros: • Target RDSOracle EndpointID — O endpoint do banco de dados RDS de destino • Destino RDSOracle DatabaseName — O nome do banco de dados RDS de destino • Target RSOracle UserName — O nome de usuário do RDS de destino • Alvo RDSOracle DBPassword — A senha do RDS de destino	

Tarefa	Descrição	Habilidades necessárias
	• TargetOracleDBPort— A porta do banco de dados RDS de destino 5. Em Configuração de VPC, sub-rede e grupo de segurança, insira os seguintes parâmetros: • VPCID: a VPC para a instância de replicação • VPCSecurityGroupId— O grupo de segurança VPC para a instância de replicação • DMSSubnet1— A sub-rede da Zona de Disponibilidade 1 • DMSSubnet2— A sub-rede da Zona de Disponibilidade 2 6. Escolha Próximo.	

Tarefa	Descrição	Habilidades necessárias
Crie a pilha.	1. Na página Configurar opções de pilha, em Tags, insira quaisquer valores opcionais. 2. Escolha Próximo. 3. Na página Revisar, verifique os detalhes e escolha Enviar. O provisionamento deve ser concluído em aproximad amente cinco a dez minutos. Ela estará completa quando a página AWS CloudFormation Stacks mostrar CREATE_CO MPLETE.	Administrador de nuvem, DBA
Configure os endpoints.	1. No Console de Gerenciam ento da AWS, selecione Database Migration Services. 2. Em Gerenciamento de recursos, selecione Instâncias de replicação. 3. Em Gerenciamento de recursos, selecione Endpoints.	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
Teste de conectividade.	Depois que os endpoints de origem e destino mostrarem o status como Ativo, teste a conectividade. Escolha Executar teste para cada endpoint (origem e destino) para garantir que o status seja exibido como bem-sucedido.	Administrador de nuvem, DBA

Exporte o PeopleSoft esquema do banco de dados Oracle local usando o Oracle Data Pump

Tarefa	Descrição	Habilidades necessárias
Gere o SCN.	Quando o banco de dados de origem estiver ativo e em uso pelo aplicativo, inicie a exportação de dados com o Oracle Data Pump. Primeiro, você deve gerar um número de alteração do sistema (SCN) do banco de dados de origem para manter a consistência de dados durante a exportação com o Oracle Data Pump e como ponto de partida para a captura de dados de alteraçõe s no AWS DMS. Para gerar o SCN atual a partir do seu banco de dados de origem, insira a seguinte instrução SQL. `SQL> select name from v $database;`	DBA

Tarefa	Descrição	Habilidades necessárias
	``` SQL> select name from v $database; NAME --------- PSFTDMO SQL> SELECT current_s cn FROM v$database; CURRENT_SCN ----------- 23792008 ``` Salve o SCN gerado para usar ao exportar os dados e criar a tarefa de replicação do AWS DMS.	

Tarefa	Descrição	Habilidades necessárias

Crie o arquivo de parâmetro.	Para criar um arquivo de parâmetros para exportar o esquema, você pode usar o código a seguir.
	`$ cat exp_datapmp.par`
	`userid=system/*******`
	`directory=DATA_P`
	`UMP_DIR`
	`logfile=export_dms_`
	`sample_user.log`
	`dumpfile=export_dms_`
	`sample_data_%U.dmp`
	`schemas=SYSADM`
	`flashback_scn=237920`
	`08`
	Note
	Você também pode definir seus próprios comandos `DATA_PUMP_DIR` usando os comandos a seguir, com base em seus requisitos.
	`SQL> CREATE OR REPLACE`
	`DIRECTORY DATA_PUMP`
	`_DIR AS '/opt/oracle/`
	`product/19c/dbhome_1/`
	`dmsdump/';`
	`Directory created.`
	`SQL> GRANT READ, WRITE`
	`ON DIRECTORY DATA_PUMP`
	`_DIR TO system;`
		DBA

Tarefa	Descrição	Habilidades necessárias
	Grant succeeded. SQL> SQL> SELECT owner, directory_name, directory_path FROM dba_directories WHERE directory_name='DA TA_PUMP_DIR'; OWNER DIRECTORY_NAME DIRECTORY_PATH ---------- ---------- ---------- ---------- ---------- ---------- SYS DATA_PUMP_DIR /opt/ oracle/product/19c/dbh ome_1/dmsdump/	

Tarefa	Descrição	Habilidades necessárias
Exporte o esquema.	Para realizar a exportação, use o utilitário `expdp`. `$ expdp parfile=e xp_datapmp.par .... Transferring the dump file with DBMS_FILE _TRANSFER to Target: . . exported "SYSADM". "PS_XML_TEMPLT_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_TEMPLT_LNK" 6.328 KB 0 rows . . exported "SYSADM". "PS_XML_XLATDEF_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_XLATITM_LNG" 7.171 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNCNTL" 7.601 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNPARM" 7.210 KB 0 rows . . exported "SYSADM". "PS_YE_AMOUNTS" 9.351 KB 0 rows . . exported "SYSADM". "PS_YE_DATA" 16.58 KB 0 rows . . exported "SYSADM". "PS_YE_EE" 6.75 KB 0 rows . . exported "SYSADM". "PS_YE_W2CP_AMOUNTS" 9.414 KB 0 rows`	DBA

Tarefa	Descrição	Habilidades necessárias
	. . exported "SYSADM". "PS_YE_W2CP_DATA" 20.94 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_AMOUNTS" 10.27 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_DATA" 20.95 KB 0 rows . . exported "SYSADM". "PS_ZBD_JOBCODE_TBL" 14.60 KB 0 rows . . exported "SYSADM". "PTGRANTTBL" 5.468 KB 0 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _01" successfully loaded/unloaded ** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_01 is: /opt/oracle/pr oduct/19c/dbhome_1 /dmsdump/export_dm s_sample_data_01.dmp Job "SYSTEM"."SYS_EXPO RT_SCHEMA_01" successfully completed at Mon Dec 19 20:13:57 2022 elapsed 0 00:38:22	

Importe o PeopleSoft esquema para o banco de dados Amazon RDS for Oracle usando o Oracle Data Pump

Tarefa	Descrição	Habilidades necessárias
Transfira o arquivo de dump para a instância de destino.	Para transferir seus arquivos usando `DBMS_FILE_TRANSFER`, você precisa criar um link de banco de dados do banco de dados de origem para a instância do Amazon RDS para Oracle. Depois que o link for estabelecido, você poderá usar o utilitário para transferir os arquivos do Data Pump diretamente para a instância do RDS. Como alternativa, você pode transferir os arquivos do Data Pump para o Amazon Simple Storage Service (Amazon S3) e depois importá-los para a instância do Amazon RDS para Oracle. Para obter mais informações sobre essa opção, consulte a seção Informações adicionais. Para criar um link `ORARDSDB` de banco de dados que se conecte ao usuário mestre do Amazon RDS na instância de banco de dados de destino, execute os comandos a seguir no banco de dados de origem.	DBA

Tarefa	Descrição	Habilidades necessárias

	`$sqlplus / as sysdba`
	`$ SQL> create database link orardsdb connect to admin identified by "*****" using '(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = testpsft.*******.us-west-2.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';`
	`Database link created.`	

Teste o link do banco de dados.	Teste o link do banco de dados para garantir que você possa se conectar usando o sqlplus ao banco de dados de destino do Amazon RDS para Oracle.
	`SQL>`
	`SQL> select name from v$database@orardsdb;`
	`NAME`
	`---------`
	`ORCL`
	`SQL>`
		DBA

Tarefa	Descrição	Habilidades necessárias

Transfira o arquivo dump para o banco de dados de destino.	Para copiar o arquivo dump para o banco de dados do Amazon RDS para Oracle, você pode usar o diretório padrão `DATA_PUMP_DIR` ou criar seu próprio diretório usando o código a seguir.
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'TARGET_PUMP_DIR') ;`
	O script a seguir copia um arquivo dump chamado `export_dms_sample_data_01.dmp` da instância de origem para um banco de dados de destino do Amazon RDS para Oracle usando o link de banco de dados de destino chamado `orardsdb`.
	`$ sqlplus / as sysdba SQL> BEGIN DBMS_FILE_TRANSFER .PUT_FILE( source_directory_object => 'DATA_PUMP_DIR', source_file_name => 'export_dms_sample_data_01.dmp',`
		DBA

Tarefa	Descrição	Habilidades necessárias
	`destination_directory _object => 'TARGET_P UMP_DIR'', destination_file_name => 'export_dms_sample _data_01.dmp', destination_database => 'orardsdb' ); END; / PL/SQL procedure successfully completed .`	
Liste o arquivo dump no banco de dados de destino.	Depois que o procedimento PL/SQL for concluído, você poderá listar o arquivo dump de dados no banco de dados do Amazon RDS para Oracle usando o código a seguir. `SQL> select * from table (rdsadmin.rds_file _util.listdir(p_di rectory => 'TARGET_P UMP_DIR'));`	DBA

Tarefa	Descrição	Habilidades necessárias
Inicie a importação no banco de dados de destino.	Antes de iniciar o processo de importação, configure as funções, os esquemas e os espaços de tabela no banco de dados de destino do Amazon RDS para Oracle usando o arquivo de dump de dados. Para realizar a importação, acesse o banco de dados de destino com a conta de usuário principal do Amazon RDS e use o nome da cadeia de conexão no arquivo `tnsnames.ora` , que inclui o Amazon RDS para Oracle Database `tns-entry` . Se necessário, você pode incluir uma opção de remapeamento para importar o arquivo de dump de dados em um espaço de tabela diferente ou com um nome de esquema diferente. Para iniciar a importação, use o código a seguir. `impdp admin@orardsdb directory=TARGET_PUMP_DIR logfile=import.log dumpfile=export_dms_sample_data_01.dmp`	DBA

Tarefa	Descrição	Habilidades necessárias
	Para garantir uma importação bem-sucedida, verifique se há erros no arquivo de log de importação e revise os detalhes, como contagem de objetos, contagem de linhas e objetos inválidos. Se houver algum objeto inválido, recompile-o. Além disso, compare os objetos do banco de dados de origem e de destino para confirmar se eles coincidem.	

Crie uma tarefa de replicação do AWS DMS usando o CDC para realizar a replicação ao vivo

Tarefa	Descrição	Habilidades necessárias
Crie a tarefa de replicação.	Crie a tarefa de replicação do AWS DMS usando as seguintes etapas: 1. No console do AWS DMS, em Conversão e migração, selecione Tarefa de migração de banco de dados. 2. Em Configuração da tarefa, em Identificador da tarefa, insira o identificador da tarefa. 3. Em Instância de replicação, escolha a instância de	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
	replicação DMS que você criou. 4. Para Endpoint do banco de dados de origem, escolha seu endpoint de origem. 5. Para o endpoint do banco de dados de destino, escolha seu banco de dados Amazon RDS para Oracle de destino. 6. Em Tipo de migração, escolha Replicar somente alterações de dados. Se você receber uma mensagem informando que o registro complementar precisa ser ativado, siga as instruções na seção Informações adicionais. 7. Em Configurações de tarefa, selecione Especific ar número de sequência de log. 8. Em Número de alteração do sistema, insira o SCN do banco de dados do Oracle que você gerou do banco de dados do Oracle de origem. 9. Escolha Ativar validação. 10. Escolha Ativar CloudWatch registros.	

Tarefa	Descrição	Habilidades necessárias
	Ao ativar esse recurso, você pode validar os dados e os registros da Amazon para revisar CloudWatch os registros da instância de replicação do AWS DMS. 11. Em Regras de seleção, preencha o seguinte: • Em Esquema, escolha Insira um esquema. • Em Nome do esquema, insira SYSADM. • Em Nome da tabela, insira %. • Em Ação, escolha Incluir. 12. Em Regras de transform ação, preencha o seguinte: • Em Destino, selecione Tabela. • Em Nome do esquema, escolha Insira um esquema. • Em Nome do esquema, insira SYSADM. • Em Ação, selecione Renomear para. 13. Escolha Criar tarefa. Depois de criar a tarefa, ela migra o CDC para a instância do banco de dados do Amazon RDS para Oracle	

Tarefa	Descrição	Habilidades necessárias
	a partir do SCN que você forneceu no modo de início do CDC. Você também pode verificar revisando os CloudWatch registros.	

Valide o esquema de banco de dados no banco de dados de destino do Amazon RDS para Oracle

Tarefa	Descrição	Habilidades necessárias
Validar a transferência de dados.	Após o início da tarefa do AWS DMS, você pode verificar a guia Estatísticas da tabela na página Tarefas para ver as alterações feitas nos dados. Você pode monitorar o status da replicação contínua no console na página Tarefas de migração do banco de dados. Para obter mais informações, consulte Validação de dados do AWS DMS.	Administrador de nuvem, DBA

Substituir

Tarefa	Descrição	Habilidades necessárias
Encerrar a replicação.	Interrompa o procedimento de replicação e interrompa os serviços do aplicativo de origem.	Administrador de nuvem, DBA

Tarefa	Descrição	Habilidades necessárias
Inicie o nível PeopleSoft intermediário.	Inicie o aplicativo de nível PeopleSoft intermediário de destino na AWS e direcione-o para o banco de dados Amazon RDS for Oracle, recentemente migrado. Ao acessar o aplicativo, você deve observar que todas as conexões do aplicativo agora estão estabelecidas com o banco de dados do Amazon RDS para Oracle.	DBA, administrador PeopleSoft
Desative o banco de dados de origem.	Depois de confirmar que não há mais conexões com o banco de dados de origem, ele pode ser desativado.	DBA

Recursos relacionados

- Introdução ao AWS Database Migration Service
- Práticas recomendadas para o AWS Database Migration Service
- Migrar bancos de dados Oracle para a Nuvem AWS

Mais informações

Transferir arquivos usando o Amazon S3

Para transferir os arquivos para o Amazon S3, você pode usar a AWS CLI ou o console do Amazon S3. Depois de transferir os arquivos para o Amazon S3, você pode usar a instância Amazon RDS para Oracle para importar os arquivos do Data Pump do Amazon S3.

Se você optar por transferir o arquivo de dump usando a integração com o Amazon S3 como um método alternativo, execute as seguintes etapas:

1. Criar um bucket do S3.
2. Exporte os dados do banco de dados de origem usando o Oracle Data Pump.
3. Faça upload dos arquivos do Data Pump para o bucket S3.
4. Faça download dos arquivos do Data Pump do bucket do S3 no banco de dados de destino do Amazon RDS para Oracle.
5. Execute a importação usando os arquivos do Data Pump.

> **Note**
>
> Para transferir grandes arquivos de dados entre instâncias do S3 e do RDS, é recomendável usar o recurso Amazon S3 Transfer Acceleration.

Ativar o registro suplementar

Se você receber uma mensagem de aviso para ativar o registro suplementar em log no banco de dados de origem para replicação contínua, use as etapas a seguir.

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
```

Migrar um banco de dados MySQL on-premises para o Amazon RDS para MySQL

Criado por Lorenzo Mota (AWS)

Resumo

Esse padrão fornece orientação para migrar um banco de dados MySQL on-premises para o Amazon Relational Database Service (Amazon RDS) para o MySQL. O padrão discute o uso de AWS Database Migration Service (AWS DMS) ou ferramentas nativas do MySQL, como mysqldump, para uma migração completa do banco de dados. Esse padrão é principalmente para DBAs arquitetos de soluções. Ele pode ser usado em projetos pequenos ou grandes como procedimento de teste (recomendamos pelo menos um ciclo de teste) ou como procedimento final de migração.

Pré-requisitos e limitações

Pré-requisitos

- Uma AWS conta ativa
- Um banco de dados de origem do MySQL em um datacenter on-premises

Limitações

- Limite de tamanho do banco de dados: 64 TB

Versões do produto

- MySQL, versões 5.5, 5.6, 5.7, 8.0 Para obter a lista mais recente de versões compatíveis, consulte MySQL no Amazon RDS na documentação. AWS Se você estiver usando AWS DMS, consulte também Usando um banco de dados compatível com MySQL como destino para as versões do AWS DMS MySQL atualmente suportadas pelo. AWS DMS

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados MySQL on-premises

Pilha de tecnologias de destino

- Uma instância de banco de dados do Amazon RDS executando o MySQL.

Arquitetura de destino

O diagrama a seguir mostra o destino da implementação do Amazon RDS para MySQL após a migração.

AWS arquitetura de migração de dados

Usando AWS DMS:

O diagrama a seguir mostra a arquitetura de migração de dados usada AWS DMS para enviar alterações completas e incrementais até a transição. A conexão de rede do local até o local AWS depende de seus requisitos e está fora do escopo desse padrão.

Usando ferramentas nativas do MySQL:

O diagrama a seguir mostra a arquitetura de migração de dados quando você usa ferramentas nativas do MySQL. Os arquivos de despejo de exportação são copiados para o Amazon Simple Storage Service (Amazon S3) e importados para o banco de dados Amazon RDS for MySQL antes da transição. AWS A conexão de rede do local até o local AWS depende de seus requisitos e está fora do escopo desse padrão.

Observações:

- Dependendo dos requisitos de tempo de inatividade e do tamanho do banco de dados, o uso AWS DMS ou de uma ferramenta de captura de dados de alteração (CDC) minimiza o tempo de transição. AWS DMS pode ajudar a reduzir ao mínimo o tempo de transição para o novo alvo (normalmente minutos). Uma estratégia offline com mysqldump pode ser suficiente se o tamanho do banco de dados e a latência da rede permitirem uma janela curta. (Recomendamos testar para obter um tempo aproximado.)
- Normalmente, uma estratégia do CDC AWS DMS exige mais monitoramento e complexidade do que as opções off-line.

Ferramentas

- AWS services:AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para o Nuvem AWS d ou entre combinações de configurações na nuvem e no local. Para obter informações sobre bancos de dados de origem e destino do MySQL compatíveis com AWS DMS, consulte Migrando bancos de dados compatíveis com MySQL para. AWS Se seu banco de dados de origem não for compatível com AWS DMS, você deverá escolher outro método para migrar seus dados.
- Ferramentas nativas do MySQL: mysqldump
- Ferramentas de terceiros: Percona XtraBackup

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Validar versões do banco de dados.	Valide as versões dos bancos de dados de origem e de destino.	DBA
Identifique os requisitos de hardware.	Identifique os requisitos de hardware para o servidor de destino.	DBA, administrador de sistemas
Identifique os requisitos de armazenamento.	Identifique os requisitos de armazenamento (como tipo e capacidade de armazenamento) para o banco de dados de destino.	DBA, administrador de sistemas
Altere o tipo de instância.	Selecione o tipo de instância de destino com base na capacidade, nos atributos de armazenamento e nos atributos de rede.	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Identifique os requisitos de acesso à rede.	Identifique os requisitos de segurança para acesso à rede para os bancos de dados de origem e de destino.	DBA, administrador de sistemas
Identifique objetos sem suporte.	Identifique objetos sem suporte (se houver) e determine o esforço de migração.	DBA
Identificar dependências.	Identifique todas as dependências em bancos de dados remotos.	DBA
Determine a estratégia de migração do aplicativo.	Determine a estratégia para migrar aplicativos de clientes.	DBA, proprietário do aplicativo, administrador de sistemas

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).	Configure tabelas de rotas, gateway da internet, gateways NAT e sub-redes. Para obter mais informações, consulte VPCs Amazon RDS na documentação do Amazon RDS.	Administrador de sistemas
Criar grupos de segurança.	Configure portas e intervalos CIDR ou específicos, IPs dependendo de seus requisitos. A porta padrão do MySQL é 3306. Para obter mais informações, consulte	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	Controlar o acesso com grupos de segurança no Guia do usuário do Amazon RDS.	
Configure e inicie uma instância de banco de dados do Amazon RDS para MySQL.	Para obter instruções, consulte Criação de uma instância de banco de dados Amazon RDS na documentação do Amazon RDS. Verifique as versões compatíveis.	Administrador de sistemas

Migrar dados – opção 1 (usando ferramentas nativas)

Tarefa	Descrição	Habilidades necessárias
Use ferramentas nativas do MySQL ou terceirizadas para migrar objetos e dados do banco de dados.	Para obter instruções, consulte a documentação das ferramentas do MySQL, como mysqldump e XtraBackupPercona (para migração física). Para obter mais informações sobre opções, consulte a postagem do blog Opções de migração do MySQL para o Amazon RDS para MySQL ou Amazon Aurora MySQL.	DBA

Migrar dados – opção 2 (usando AWS DMS)

Tarefa	Descrição	Habilidades necessárias
Migre dados com AWS DMS.	Para obter instruções, consulte a AWS DMS documentação.	DBA

Execute tarefas preliminares antes da substituição

Tarefa	Descrição	Habilidades necessárias
Corrija discrepâncias na contagem de objetos.	Colete contagens de objetos do banco de dados de origem e do novo banco de dados de destino. Corrija discrepâncias no banco de dados de destino.	DBA
Verifique dependências.	Verifique se as dependênc ias (links) de e para outros bancos de dados são válidas e funcionam conforme o esperado.	DBA
Realize testes.	Se esse for um ciclo de testes, realize testes de consulta, colete métricas e corrija problemas.	DBA

Substituir

Tarefa	Descrição	Habilidades necessárias
Mudar para o banco de dados de destino.	Mude os aplicativos do cliente para a nova infraestrutura.	DBA, proprietário do aplicativ o, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Forneça suporte para testes.	Forneça suporte para testes funcionais de aplicativos.	DBA

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Desligar recursos.	Encerre os AWS recursos temporários que você criou para a migração.	DBA, administrador de sistemas
Valide os documentos do projeto.	Revise e valide os documentos do projeto.	DBA, proprietário do aplicativo, administrador de sistemas
Colete métricas.	Reúna métricas como tempo de migração, porcentagem de tarefas manuais versus esforço automatizado e economia de custos.	DBA, proprietário do aplicativo, administrador de sistemas
Encerre o projeto.	Feche o projeto e forneça feedback.	DBA, proprietário do aplicativo, administrador de sistemas
Descomissionar o banco de dados de origem.	Quando todas as tarefas de migração e substituição estiverem concluídas, desative o banco de dados on-premises.	DBA, administrador de sistemas

Recursos relacionados

Referências

- Estratégia de migração para bancos de dados relacionais
- AWS DMS site

- AWS DMS documentação
- Documentação do Amazon RDS
- Preços do Amazon RDS
- Amazon VPC e Amazon RDS
- Implantações multi-AZ do Amazon RDS
- Migre bancos de dados MySQL locais para o Aurora MySQL usando XtraBackup Percona, Amazon EFS e Amazon S3
- Armazenamento de instâncias de banco de dados do Amazon RDS

Tutoriais

- Começando com AWS DMS
- Conceitos básicos do Amazon RDS

Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server

Criado por Henrique Lobao (AWS), Jonathan Pereira Cruz (AWS) e Vishal Singh (AWS)

Resumo

Esse padrão fornece orientação para migrar de um banco de dados Microsoft SQL Server on-premises para o Amazon Relational Database Service (Amazon RDS) para SQL Server . Ele descreve duas opções de migração: usar o AWS Data Migration Service (AWS DMS) ou usar ferramentas nativas do Microsoft SQL Server, como o Copy Database Wizard.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Microsoft SQL Server de origem em um datacenter on-premises

Limitações

- Limite de tamanho do banco de dados: 16 TB

Versões do produto

- SQL Server 2014-2019, edições Enterprise, Standard, Workgroup e Developer. Para obter a lista mais recente de versões e atributos compatíveis, consulte Microsoft SQL Server no Amazon RDS na documentação da AWS. Se você estiver usando o AWS DMS, consulte também Como usar um banco de dados Microsoft SQL Server como destino para as versões do AWS DMS para versões SQL Server compatíveis com AWS DMS.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Microsoft SQL Server on-premises

Pilha de tecnologias de destino

- Uma instância de banco de dados do Amazon RDS para SQL Server

Arquitetura de origem e destino

Usando o AWS DMS:

Usando ferramentas nativas do SQL Server:

Ferramentas

- O AWS DMS é compatível com vários bancos de dados de origem e destino. Para obter detalhes, consulte as instruções passo a Step-by-Step passo do AWS DMS. Se o AWS DMS não for compatível com o banco de dados de origem, selecione outro método para migrar os dados.
- As ferramentas nativas do Microsoft SQL Server incluem backup e restauração, assistente de cópia de banco de dados, cópia e anexação de banco de dados.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide a versão e o mecanismo dos bancos de dados de origem e de destino.		DBA
Identifique os requisitos de hardware para a instância do servidor de destino.		DBA, administrador de sistemas
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, administrador de sistemas
Escolha o tipo de instância adequado com base na		DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
capacidade, nos atributos de armazenamento e nos atributos de rede.		
Identifique os requisitos de segurança do acesso à rede para os bancos de dados de origem e de destino.		DBA, administrador de sistemas
Identifique a estratégia de migração de aplicativos.		DBA, administrador de sistemas

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).		Administrador de sistemas
Criar grupos de segurança.		Administrador de sistemas
Configurar e inicie uma instância de banco de dados do Amazon RDS.		DBA, administrador de sistemas

Migrar dados - opção 1

Tarefa	Descrição	Habilidades necessárias
Use ferramentas nativas do SQL Server ou ferramentas de terceiros para migrar dados e objetos de banco de dados.		DBA

Migrar dados - opção 2

Tarefa	Descrição	Habilidades necessárias
Migre dados com o AWS DMS.		DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos.		DBA, proprietário do aplicativo, administrador de sistemas

Substituir

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.		DBA, proprietário do aplicativo, administrador de sistemas

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, administrador de sistemas
Revise e valide os documentos do projeto.		DBA, proprietário do aplicativo, administrador de sistemas
Reúna métricas como tempo para migrar, porcentagem de tarefas manuais versus		DBA, proprietário do aplicativo, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
automatizadas e economia de custos.		
Feche o projeto e forneça feedback.		DBA, proprietário do aplicativo, administrador de sistemas

Recursos relacionados

Referências

- Implantação do Microsoft SQL Server na Amazon web Services
- Site do AWS DMS
- Preços do Amazon RDS
- Produtos da Microsoft na AWS
- Licenciamento da Microsoft na AWS
- Microsoft SQL Server na AWS
- Uso da autenticação do Windows com uma instância de banco de dados do Microsoft SQL Server
- Implantações multi-AZ do Amazon RDS

Tutoriais e vídeos

- Conceitos básicos do AWS DMS
- Conceitos básicos do Amazon RDS
- AWS DMS (vídeo)
- Amazon RDS (vídeo)

Migre dados do Microsoft Azure Blob para o Amazon S3 usando o Rclone

Criado por Suhas Basavaraj (AWS), Aidan Keane (AWS) e Corey Lane (AWS)

Resumo

Esse padrão descreve como usar o Rclone para migrar dados do armazenamento de objetos do Microsoft Azure Blob para um bucket do Amazon Simple Storage Service (Amazon S3). Você pode usar esse padrão para realizar uma migração única ou uma sincronização contínua dos dados. O Rclone é um programa de linha de comando escrito em Go e é usado para mover dados em várias tecnologias de armazenamento de provedores de nuvem.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Dados armazenados no serviço de contêiner Azure Blob

Arquitetura

Pilha de tecnologia de origem

- Contêiner de armazenamento Azure Blob

Pilha de tecnologias de destino

- Bucket do Amazon S3
- Instância Linux da Amazon Elastic Compute Cloud (Amazon EC2)

Arquitetura

Ferramentas

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

- O Rclone é um programa de linha de comando de código aberto inspirado no rsync. Ele é usado para gerenciar arquivos em várias plataformas de armazenamento em nuvem.

Práticas recomendadas

Ao migrar dados do Azure para o Amazon S3, lembre-se dessas considerações para evitar custos desnecessários ou velocidades de transferência lentas:

- Crie sua infraestrutura da AWS na mesma região geográfica da conta de armazenamento do Azure e do contêiner Blob — por exemplo, região da AWS `us-east-1` (Norte da Virgínia) e região do Azure. `East US`
- Evite usar o NAT Gateway, se possível, pois ele acumula taxas de transferência de dados para a largura de banda de entrada e saída.
- Use um endpoint de gateway VPC para o Amazon S3 para aumentar o desempenho.
- Considere usar uma EC2 instância baseada no processador AWS Graviton2 (ARM) para obter menor custo e maior desempenho em relação às instâncias Intel x86. O Rclone é altamente compilado de forma cruzada e fornece um binário ARM pré-compilado.

Épicos

Prepare os recursos de nuvem da AWS e do Azure

Tarefa	Descrição	Habilidades necessárias
Prepare um bucket do S3 de destino.	Crie um novo bucket S3 na região da AWS apropriada ou escolha um bucket existente como destino para os dados que você deseja migrar.	Administrador da AWS
Crie uma função de instância do IAM para a Amazon EC2.	Crie uma nova função do AWS Identity and Access Management (IAM) para a Amazon EC2. Essa função dá à sua EC2 instância acesso de gravação ao bucket do S3 de destino.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Anexar uma política do IAM à instância	Use o console do IAM ou a AWS Command Line Interface (AWS CLI) para criar uma política embutida para a função EC2 da instância que permite permissões de acesso de gravação ao bucket S3 de destino. Para ver um exemplo de política, consulte a seção Informações adicionais.	Administrador da AWS
Execute uma EC2 instância.	Execute uma EC2 instância Amazon Linux que esteja configurada para usar a função de serviço IAM recém-criada. Essa instância também precisará acessar os endpoints públicos da API do Azure pela Internet. **Note** Considere usar EC2 instâncias do AWS baseadas em Graviton para reduzir custos. O Rclone fornece binários compilados em ARM.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Crie uma entidade principal de serviço do Azure AD.	Use a CLI do Azure para criar uma entidade principal de serviço do Azure Active Directory (Azure AD) que tenha acesso somente de leitura ao contêiner de armazenamento de Blob do Azure de origem. Para obter instruções, consulte a seção Informações adicionais. Armazene essas credenciais na sua EC2 instância no local `~/azure-principal.json` .	Administrador de nuvem, Azure

Instalar e configurar o Rclone

Tarefa	Descrição	Habilidades necessárias
Faça download e instale o Rclone.	Baixe e instale o programa de linha de comando Rclone. Para obter instruções de instalação, consulte Documentação da instalação do Rclone.	AWS geral, Administrador de nuvem
Configure o Rclone.	Copie o arquivo `rclone.conf` de amostra a seguir. `AZStorageAccount` Substitua pelo nome da sua conta do Azure Storage e `us-east-1` pela região da AWS onde seu bucket do S3 está	AWS geral, Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	localizado. Salve esse arquivo `~/.config/rclone/rclone.conf` no local da sua EC2 instância.
	
	`[AZStorageAccount]`
	`type = azureblob`
	`account = AZStorageAccount`
	`service_principal_file = azure-principal.json`
	
	`[s3]`
	`type = s3`
	`provider = AWS`
	`env_auth = true`
	`region = us-east-1`	

Tarefa	Descrição	Habilidades necessárias

Verifique a configuração do Rclone.	Para confirmar se o Rclone está configurado e se as permissões estão funcionando corretamente, verifique se o Rclone pode analisar seu arquivo de configuração e se os objetos dentro do contêiner do Azure Blob e do bucket do S3 estão acessíveis. Veja a seguir exemplos de comandos de validação.
	• Liste os controles remotos configurados no arquivo de configuração. Isso garantirá que seu arquivo de configuração seja analisado corretamente. Revise a saída para verificar se ela corresponde ao seu `rclone.conf` arquivo.
	`rclone listremotes`
	`AZStorageAccount:`
	`s3:`
	• Liste os contêineres do Azure Blob na conta configurada. `AZStorage Account` Substitua pelo nome da conta de armazenamento que você usou no `rclone.conf` arquivo.
		AWS geral, Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	`rclone lsd AZStorage Account:`
	`2020-04-29 08:29:26 docs`
	• Liste os arquivos no contêiner Azure Blob. Substitua os documento s nesse comando por um nome de contêiner Blob real em sua conta de armazenamento do Azure.
	`rclone ls AZStorage Account:docs`
	`824884 administr ator-en.a4.pdf`
	• Liste os buckets em sua conta da AWS.
	`[root@ip-10-0-20-157 ~]# rclone lsd s3:`
	`2022-03-07 01:44:40 amzn-s3-demo-bucket1`
	`2022-03-07 01:45:16 amzn-s3-demo-bucket2`
	`2022-03-07 02:12:07 amzn-s3-demo-bucket3`
	• Liste os arquivos no bucket do S3.
	`[root@ip-10-0-20-1 57 ~]# rclone ls`	

Tarefa	Descrição	Habilidades necessárias
	`s3:amzn-s3-demo-bucket1 template0.yaml template1.yaml`	

Migre dados usando o Rclone

Tarefa	Descrição	Habilidades necessárias

Migre dados de seus contêineres.	Execute o comando Rclone copiar ou sincronizar.
	
	Exemplo: cópia
	
	Esse comando copia dados do contêiner Azure Blob de origem para o bucket S3 de destino.
	
	`rclone copy AZStorageAccount:blob-container s3:amzn-s3-demo-bucket1`
	
	Exemplo: sincronização
	
	Esse comando sincroniza dados entre o contêiner Azure Blob de origem e o bucket S3 de destino.
	
	`rclone sync AZStorageAccount:blob-container s3:amzn-s3-demo-bucket1`
		AWS geral, Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Important Quando você usa o comando sync, os dados que não estão presentes no contêiner de origem serão excluídos do bucket S3 de destino.	
Sincronize seus contêineres.	Depois que a cópia inicial estiver concluída, execute o comando Rclone sync para a migração contínua, de forma que somente os novos arquivos que estão faltando no bucket S3 de destino sejam copiados.	AWS geral, Administrador de nuvem
Verifique se os dados foram migrados com sucesso.	Para verificar se os dados foram copiados com êxito para o bucket S3 de destino, execute os comandos Rclone lsd e ls.	AWS geral, Administrador de nuvem

Recursos relacionados

- Guia do usuário do Amazon S3 (documentação da AWS)
- Funções do IAM para a Amazon EC2 (documentação da AWS)
- Criação de um contêiner do Microsoft Azure Blob (documentação do Microsoft Azure)
- Comandos Rclone (documentação do Rclone)

Mais informações

Exemplo de política de função para EC2 instâncias

Essa política dá à sua EC2 instância acesso de leitura e gravação a um bucket específico em sua conta. Se o bucket usa uma chave gerenciada pelo cliente para a criptografia no lado do servidor, a política pode precisar de acesso adicional ao AWS Key Management Service (AWS KMS).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
              "arn:aws:s3:::amzn-s3-demo-bucket/*",
              "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Criando uma entidade principal de serviço do Azure AD somente para leitura

Uma entidade principal de serviço do Azure é uma identidade de segurança usada por aplicativos, serviços e ferramentas de automação do cliente para acessar recursos específicos do Azure. Pense nisso como uma identidade de usuário (login e senha ou certificado) com uma função específica e permissões rigorosamente controladas para acessar seus recursos. Para criar uma entidade principal de serviço somente de leitura para seguir as permissões de privilégio mínimo e proteger os dados no Azure contra exclusões acidentais, siga estas etapas:

1. Faça login no portal da sua conta na nuvem do Microsoft Azure e inicie o Cloud Shell PowerShell ou use a Interface de Linha de Comando (CLI) do Azure em sua estação de trabalho.
2. Crie uma entidade principal de serviço e configure-o com acesso somente de leitura à sua conta de armazenamento de Blobs do Azure. Salve a saída JSON desse comando em um arquivo local chamado`azure-principal.json`. O arquivo será enviado para sua EC2 instância. Substitua as variáveis de espaço reservado que são mostradas entre colchetes (`{e}`) por sua ID de assinatura do Azure, nome do grupo de recursos e nome da conta de armazenamento.

```
az ad sp create-for-rbac `
--name AWS-Rclone-Reader `
--role "Storage Blob Data Reader" `
--scopes /subscriptions/{Subscription ID}/resourceGroups/{Resource Group Name}/
providers/Microsoft.Storage/storageAccounts/{Storage Account Name}
```

Migre do Couchbase Server para o Couchbase Capella na AWS

Criado por Battulga Purevragchaa (AWS), Mark Gamble e Saurabh Shanbhag (AWS)

Resumo

O Couchbase Capella é um banco de dados NoSQL totalmente gerenciado como serviço (DBaaS) para aplicativos de missão crítica (por exemplo, perfis de usuário ou catálogos on-line e gerenciamento de inventário). O Couchbase Capella gerencia sua carga de trabalho DBaa S em uma conta da Amazon Web Services (AWS) gerenciada pelo Couchbase. O Capella facilita a execução e o gerenciamento da replicação de vários clusters, várias regiões da AWS, multicloud e nuvem híbrida em uma única interface.

O Couchbase Capella ajuda você a escalar instantaneamente seus aplicativos do Couchbase Server, ajudando você a criar clusters de vários nós em minutos. O Couchbase Capella oferece suporte a todos os recursos do Couchbase Server, incluindo SQL++, Full Text Search, Eventing Service e Analytics Service. Também elimina a necessidade de gerenciar instalações, atualizações, backups e manutenção geral do banco de dados.

Esse padrão descreve as etapas e as melhores práticas para migrar um ambiente autogerenciado do Couchbase Server para a Nuvem AWS. O padrão fornece um processo repetível para migrar dados e índices dos clusters do Couchbase Server, executados on-premises ou na nuvem, para o Couchbase Capella. O uso dessas etapas ajuda a evitar problemas durante a migração e acelera o processo geral de migração.

Esse padrão fornece as duas opções de migração a seguir:

- A opção 1 é apropriada se você tiver menos de 50 índices para migrar.
- A opção 2 é apropriada se você tiver mais de 50 índices para migrar.

Você também pode configurar dados de amostra em seu Couchbase Server autogerenciado para acompanhar o guia de migração.

Se você escolher a opção de migração 2 ou se estiver usando escopos ou coleções diferentes do valor padrão, deverá usar o arquivo de configuração de exemplo, que está na seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta paga existente do Couchbase Capella. Você também pode criar uma conta do Couchbase Capella na AWS e usar o teste gratuito do Couchbase Capella e, em seguida, fazer o upgrade para uma conta paga para configurar seu cluster para a migração. Para começar com a versão de teste, siga as instruções em Introdução ao Couchbase Capella.
- Um ambiente existente do Couchbase Server autogerenciado on-premises ou implantado em um provedor de serviços em nuvem.
- Para a opção de migração 2, Couchbase Shell e um arquivo de configuração. Para criar o arquivo de configuração, você pode usar o arquivo de exemplo que está na seção Informações adicionais.
- Familiaridade com a administração do Couchbase Server e do Couchbase Capella.
- Familiaridade com abrir portas TCP e executar comandos em uma interface de linha de comando (CLI).

O processo de migração também exige as funções e a experiência descritas na tabela a seguir.

Função	Experiência	Responsabilidades
Administrador do Couchbase	• Familiaridade com o Couchbase Server e o Couchbase Capella • O conhecimento básico da linha de comando é útil, mas não obrigatório	• Tarefas específicas do Couchbase Server e do Capella
Administrador de sistemas, administrador de TI	• Familiaridade com o ambiente e a administração autogerenciados do sistema Couchbase Server	• Abrindo portas e determina ndo endereços IP em nós de cluster autogerenciados do Couchbase Server

Limitações

- Esse padrão é usado para migrar dados, índices e índices Couchbase Full Text Search do Couchbase Server para o Couchbase Capella na AWS. O padrão não se aplica à migração do Couchbase Eventing Service ou ao Couchbase Analytics.
- O Couchbase Capella está disponível em várias regiões da AWS. Para up-to-date obter informações sobre as regiões às quais a Capella oferece suporte, consulte Amazon Web Services na documentação do Couchbase.

Versões do produto

- Couchbase Server (Community ou Enterprise) Edition versão 5.x ou superior

Arquitetura

Pilha de tecnologia de origem

- Couchbase Server

Pilha de tecnologias de destino

- Couchbase Capella

Arquitetura de destino

1. Você acessa o Couchbase Capella usando o ambiente de gerenciamento Capella. É possível usar o ambiente de gerenciamento Capella para fazer o seguinte:
   - Controlar e monitorar sua conta.
   - Gerenciar clusters e dados, índices, usuários e grupos, permissões de acesso, monitoramento e eventos.
2. Clusters são criados.
3. O plano de dados Capella está na conta da AWS gerenciada pela Couchbase. Depois de criar um novo cluster, o Couchbase Capella o implanta em várias zonas de disponibilidade na região da AWS selecionada.
4. Você pode desenvolver e implantar aplicativos Couchbase em uma VPC na sua conta da AWS. Normalmente, essa VPC acessa o plano de dados Capella por meio do emparelhamento de VPC.

Ferramentas

- O Couchbase Cross Data Center Replication (XDCR) ajuda a replicar dados em clusters localizados em diferentes provedores de nuvem e datacenters. Ele é usado para migrar dados para o Couchbase Capella a partir de clusters autogerenciados do Couchbase Server.

> **Note**
>
> O XDCR não pode ser usado com o Couchbase Server Community Edition para migrar para o Couchbase Capella. Em vez disso, você pode usar o cbexport. Para obter mais informações, consulte o épico migrar dados da Community Edition.

- O Couchbase Shell é um shell de linha de comando para o Couchbase Server e o Couchbase Capella acessarem clusters locais e remotos do Couchbase. Nesse padrão, o Couchbase Shell é usado para migrar índices.
- cbexport é um utilitário do Couchbase para exportar dados do cluster do Couchbase. Incluído nas ferramentas da CLI do Couchbase Server.

Épicos

Preparar-se para a migração

Tarefa	Descrição	Habilidades necessárias
Avalie o tamanho do cluster autogerenciado do Couchbase Server.	Faça login no Couchbase Web Console para Couchbase Server e avalie os nós e buckets do seu cluster autogerenciado. 1. Para mostrar uma lista dos nós do cluster, escolha a guia Servidores na barra de navegação. 2. Registre o número de nós e escolha cada nó na lista	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	para exibir suas proprieda des. 3. Registre a memória e o armazenamento de cada nó individual. 4. Escolha a guia Buckets na barra de navegação e, em seguida, escolha cada bucket na lista para exibir suas propriedades. Registre a cota de RAM e a configuração de resolução de conflitos para cada bucket. Você usará suas configura ções de cluster autogeren ciadas do Couchbase Server como um guia geral para dimensionar e configura r o cluster de destino no Couchbase Capella. Para obter ajuda com um exercício mais detalhado de dimensionamento do Couchbase Capella, entre em contato com o Couchbase.	

Tarefa	Descrição	Habilidades necessárias
Registre a distribuição do Couchbase Service no cluster autogerenciado do Couchbase Server.	1. No Couchbase Web Console, escolha a guia Servidores para exibir a lista de nós do cluster. 2. Escolha cada nó para exibir suas propriedades e, em seguida, registre a distribuição do Couchbase Service para cada nó (Data Service, Query Service, Index Service, Search Service, Analytics Service e Eventing Service).	Administrador do Couchbase
Registre os endereços IP dos nós do cluster autogerenciado do Couchbase Server.	(Ignore essa etapa se você estiver usando o Community Edition.) Registre o endereço IP de cada nó em seu cluster. Eles serão adicionados à lista de permissões em seu cluster Couchbase Capella posterior mente.	Administrador do Couchbase, administrador de sistemas

Implemente e configure recursos no Couchbase Capella

Tarefa	Descrição	Habilidades necessárias
Escolher um modelo.	1. Faça login no seu ambiente de gerenciam ento Couchbase Capella, escolha a guia Painel ou a guia Clusters na navegação principal e, em seguida, escolha Criar Cluster.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	2. Usando as informações que você registrou na avaliação do seu cluster autogeren ciado do Couchbase Server, escolha o modelo de cluster que atenda aos requisitos da configuração. Se você não encontrar um modelo adequado, escolha Modelo personalizado no editor Dimensionamento de Cluster.	
Escolha e configure os nós.	Escolha e configure os nós para corresponder ao seu ambiente de cluster autogeren ciado do Couchbase Server, incluindo o número de nós, distribuição de serviços, computação ou RAM e armazenamento. O Couchbase Capella usa as melhores práticas de escalabil idade multidimensional. Serviços e nós só podem ser escolhidos de acordo com as melhores práticas de implantação. Isso pode significar que você não pode corresponder exatamente às configurações do cluster autogerenciado do Couchbase Server.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
Implantar o cluster	Escolha uma zona de suporte e um pacote de suporte e, em seguida, implante o cluster. Para obter instruções e etapas detalhadas, consulte Criar um cluster na documentação do Couchbase. **Important** Se você estiver usando o teste gratuito do Couchbase Capella, deverá convertê-lo em uma conta paga antes de iniciar sua migração. Para converter sua conta, abra a seção Faturamento do ambiente de gerenciamento do Couchbase Capella e escolha Adicionar ID de ativação. A ID de ativação é enviada para seu endereço de e-mail de contato de cobrança após você concluir um contrato de compra com a Couchbase Sales ou depois de fazer uma	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	compra por meio do AWS Marketplace.	

Tarefa	Descrição	Habilidades necessárias
Crie um usuário com credencial de banco de dados.	Um usuário de credencial de banco de dados é específico de um cluster e consiste em um nome de usuário, senha e um conjunto de privilégios de bucket. Esse usuário é necessário para criar buckets e acessar os dados do bucket. No ambiente de gerenciamento do Couchbase Capella, crie uma credencial de banco de dados para o novo cluster seguindo as instruções em Configurar credenciais de banco de dados na documentação do Couchbase Capella. **Note** Um usuário da organização precisa de credenciais de função organizacional atribuídas a ele se quiser acessar dados do bucket em um cluster específico, remotamente ou por meio da interface do Couchbase Capella. Isso é separado das credenciais do	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	banco de dados, que normalmente são usadas por aplicativos e integrações. A criação do usuário organizacional permite que você crie e gerencie os buckets de destino em seu cluster Couchbase Capella.	
Se estiver usando a opção de migração 2, instale o Couchbase Shell.	Você pode instalar o Couchbase Shell em qualquer sistema que tenha acesso de rede ao seu Couchbase Server autogerenciado e aos clusters Couchbase Capella. Para obter mais informações, consulte Instalar o Couchbase Shell versão 1.0.0-beta.5 na documentação do Couchbase Shell. Confirme se o Couchbase Shell está instalado testando uma conexão com seu cluster autogerenciado em um terminal de linha de comando.	Administrador do Couchbase, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Permitir endereços IP.	1. No ambiente de gerenciamento do Couchbase Capella escolha Clusters e, em seguida, escolha seu cluster de destino. 2. Escolha a guia Conectar para o cluster e registre o endpoint de conexão do seu cluster que está listado em Gerenciar IPs permitidos. 3. Para adicionar o endereço IP do sistema em que você instalou o Couchbase Shell e o endereço IP de suas instâncias de cluster autogerenciadas do Couchbase Server como endereços IP permitidos, faça o seguinte: a. Em Rede de longa distância, escolha Gerenciar IPs permitidos. b. Escolha Adicionar IP permitido, insira o endereço IP do sistema em que você instalou o Couchbase Shell e escolha Adicionar IP. c. Repita a etapa anterior para adicionar o endereço IP da sua	Administrador do Couchbase, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	instância de cluster autogerenciada do Couchbase Server. Para obter mais informaçõ es sobre endereços IP permitidos, consulte Configura r endereços IP permitidos na documentação do Couchbase.	

Tarefa	Descrição	Habilidades necessárias
Configurar certificados.	1. Para baixar o certificado raiz do seu cluster, em Certificado raiz, escolha Baixar. 2. Salve o certificado raiz usando a extensão de arquivo .pem em uma pasta no sistema que executará o Couchbase Shell. 3. Em seguida, faça login no console web autogeren ciado do Couchbase Server, escolha Segurança na barra de navegação esquerda e escolha a guia Certificados. 4. Copie o certificado raiz do seu cluster autogerenciado do Couchbase Server e salve-o como um arquivo.p em na mesma pasta em que você salvou o arquivo do certificado raiz do seu cluster Couchbase Capella. Para obter mais informaçõ es sobre o certificado raiz, consulte Certificado raiz na documentação do Couchbase Server.	Administrador do Couchbase, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Criar o arquivo de configuração do Couchbase Shell.	Crie um dotfile de configuração no diretório inicial da instalação do Couchbase Shell (por exemplo, `/<HOME_DIRECTORY>/.cbsh/config`). Para obter mais informações, consulte Configurar dotfiles na documentação do Couchbase. Adicione propriedades de conexão dos clusters de origem e de destino ao arquivo de configuração. Você pode usar o arquivo de configuração de exemplo que está na seção Informações adicionais e editar as configurações dos seus clusters. Salve o arquivo de configuração com as configurações atualizadas na pasta `.cbsh` (por exemplo, `/<HOME_DIRECTORY>/.cbsh/config`).	Administrador do Couchbase, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Crie buckets de destino.	Para cada bucket de origem, crie um bucket de destino em seu cluster Couchbase Capella seguindo as instruções em Criar um bucket na documentação do Couchbase. As configurações do bucket de destino devem corresponder aos nomes dos buckets, às configurações de memória e às configurações de resolução de conflitos dos buckets em seu cluster autogerenciado do Couchbase Server.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias

Crie escopos e coleções.	Cada bucket contém um escopo e uma coleção padrão com o espaço-chave `_default._default` . Se você estiver usando qualquer outro espaço-chave para seu escopo e coleção, deverá criar espaços-chave idênticos no cluster Capella de destino.
	1. Abra o terminal da linha de comando no sistema em que você instalou o Couchbase Shell.
	2. Para iniciar o Couchbase Shell, execute o comando a seguir.
	`./cbsh`
	3. Para cada bucket que você deseja migrar, crie escopos e coleções no cluster Capella executand o os comandos a seguir. Lembre-se de substituir <BUCKET_NAME> pelo nome do bucket que você deseja migrar.
	`scopes --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope | where scope != "_default" | each`
		Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	`{ |it| scopes create $it.scope --clusters "Capella-Cluster" } collections --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope collection | where $it.scope != "_default" | where $it.collection != "_default" | each { |it| collections create $it.collection --clusters "Capella-Cluster" --bucket <BUCKET_NAME> --scope $it.scope }`	

Migre os dados da Enterprise Edition

Tarefa	Descrição	Habilidades necessárias
Abra portas TCP nos nós de cluster autogerenciados do Couchbase Server.	Garanta que as portas apropriadas estejam abertas para comunicação XDCR nos nós do cluster autogerenciado do Couchbase Server. Para obter mais informações, consulte a documentação de portas do Couchbase Server.	Administrador do Couchbase, administrador de sistemas
Se você estiver usando o Couchbase Server Enterprise Edition, configure o Couchbase XDCR.	1. Na navegação principal do ambiente de gerenciamento do Couchbase Capella, escolha Clusters e, em seguida, escolha o cluster de destino para migração.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	2. Em Certificado raiz, escolha Copiar. 3. Faça login no console web autogerenciado do Couchbase Server e, na navegação principal, escolha XDCR. Escolha Adicionar registro. 4. Insira as seguintes configurações: • Nome do cluster: um nome para a conexão do cluster Capella • IP/HostName: o endpoint de conexão para seu cluster Couchbase Capella • Nome de usuário do cluster remoto: o usuário do banco de dados do seu cluster Couchbase Capella • Senha: a senha do usuário do banco de dados para seu cluster Couchbase Capella • Ativar conexão segura: selecionado • Completo (senha e dados de criptografia TLS): selecionado 5. Cole o certificado raiz do cluster Capella que você	

Tarefa	Descrição	Habilidades necessárias
	copiou anteriormente e escolha Salvar.	
Inicie o Couchbase XDCR.	1. No console web autogerenciado do Couchbase Server, escolha XDCR na navegação principal e, em seguida, escolha Adicionar replicação. 2. Insira as seguintes configurações: • Replicar do bucket: selecione o bucket de origem para migração. • Bucket remoto: insira o nome do bucket de destino. • Cluster remoto: selecione o cluster de destino que você criou anteriormente. 3. Escolha Salvar Replicação. O processo de replicação deve começar em alguns segundos.	Administrador do Couchbase

Migre os índices usando a opção 1

Tarefa	Descrição	Habilidades necessárias
Migre índices de cluster autogerenciados para o Couchbase Capella.	**Important** Recomendamos esse processo se você tiver menos de 50	Administrador do Couchbase, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	índices para migrar. Se você tiver mais de 50 índices para migrar, recomenda mos usar a opção de migração 2. 1. No console Couchbase Web, escolha Índices. 2. Na lista de índices, escolha o primeiro índice que você deseja migrar. A definição do índice é então exibida. 3. Copie a definição do índice usando a instrução `CREATE`, mas não copie `WITH { "defer_bu ild":true }` . Por exemplo, a partir do exemplo de definição de índice a seguir, você copiaria somente `CREATE INDEX `cityinde x` ON `travel-s ample`(`city`)` . `CREATE INDEX `cityinde x` ON `travel-s ample`(`city`) WITH { "defer_bu ild":true }` 4. No ambiente de gerenciam ento Couchbase Capella,	

Tarefa	Descrição	Habilidades necessárias
	escolha Clusters e, em seguida, escolha o cluster de destino. 5. Na lista suspensa Ferramentas, escolha Query Workbench. Cole a instrução `CREATE` que você copiou anteriormente no Editor de consultas e escolha Executar. Isso cria e constrói o índice. 6. Para confirmar que o índice foi criado, escolha Índices na lista suspensa Ferramentas. A lista mostra que o índice foi criado e construído. 7. Repita esse processo para cada índice que deve ser migrado.	

Migre os índices usando a opção 2

Tarefa	Descrição	Habilidades necessárias
Migre as definições do índice.	**Important** Recomendamos esse processo se você tiver mais de 50 índices para migrar. Se você tiver menos de 50 índices para migrar,	Administrador do Couchbase, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias

	recomendamos usar a opção de migração 1.
	
	1. Abra o terminal da linha de comando no sistema em que você instalou o Couchbase Shell.
	2. Para iniciar o Couchbase Shell, execute o comando a seguir.
	
	`./cbsh`
	
	3. Para se conectar ao cluster autogerenciado do Couchbase Server, execute o comando a seguir.
	
	`cb-env cluster On-Prem-Cluster`
	
	4. Para migrar as definições de índice do cluster autogerenciado do Couchbase Server para o cluster Couchbase Capella, execute o comando a seguir para cada bucket que você deseja migrar. Lembre-se de substituir `<BUCKET_NAME>` pelo nome do bucket que corresponde aos índices que você deseja migrar. Essa opção de migração	

Tarefa	Descrição	Habilidades necessárias
	exige que os nomes dos buckets de destino sejam idênticos aos nomes dos buckets de origem. `query indexes --definitions | where bucket =~ <BUCKET_NAME>| get definition | each { |it| query $it --clusters Capella-Cluster }`	

Tarefa	Descrição	Habilidades necessárias

Crie as definições do índice.	1. Para mudar o contexto do cluster do Couchbase Capella, execute o comando a seguir:
	`cb-env cluster Capella-Cluster`
	2. Para criar as definições de índice que foram migradas para o cluster Couchbase Capella, execute o comando a seguir, substituindo <BUCKET_NAME> pelo nome do bucket que corresponde aos índices que você deseja criar.
	`query 'SELECT RAW CONCAT("BUILD INDEX ON ", k , "(['", CONCAT2 ("','", inames), "']);") FROM system:indexes AS s LET bid = CONCAT("` ",s.bucket_id, "`"), sid = CONCAT("`", s.scope_id, "`"), kid = CONCAT("` ", s.keyspace_id, "`"), k = NVL2(bid, CONCAT2(".", bid, sid, kid), kid) WHERE s.namespa ce_id = "default" AND s.bucket_id = "" GROUP BY k LETTING inames = ARRAY_AGG (s.name) FILTER`
		Administrador do Couchbase, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	(WHERE s.state = 'deferred') HAVING ARRAY_LENGTH(iname s) > 0;' | each { | it| query $it } 3. Repita esse procedimento para cada bucket.	

Migre índices de pesquisa de texto completo

Tarefa	Descrição	Habilidades necessárias
Migre os índices de pesquisa de texto completo do cluster autogerenciado para o Couchbase Capella.	1. No Couchbase Web Console, escolha Pesquisar . 2. Na lista de índices de pesquisa de texto completo (FTS), escolha o primeiro índice FTS que você deseja migrar, escolha Mostrar definição de índice JSON e escolha Copiar para área de transferê ncia. Anote o nome do índice e o bucket ao qual ele pertence. 3. No ambiente de gerenciam ento Couchbase Capella, escolha Clusters e, em seguida, escolha o cluster de destino. 4. Na lista suspensa Ferramentas, escolha Full Text Search.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	5. Escolha Importar índice e cole a definição do índice FTS. 6. Insira o nome do índice, selecione o bucket correto, conforme observado no cluster autogerenciado, e escolha Criar. 7. Repita esse processo para cada índice do FTS que deve ser migrado.	

Migre dados do Couchbase Community Edition

Tarefa	Descrição	Habilidades necessárias

Exporte dados do Couchbase Server Community Edition autogerenciado.	O XDCR criptografado não está disponível no Couchbase Community Edition. Você pode exportar dados do Couchbase Community Edition e depois importar manualmente os dados para o Couchbase Capella.
	
	Para exportar dados do bucket de origem, use `cbexport` na linha de comando.
	
	O comando a seguir é um exemplo.
	
	`cbexport json \`
	`--cluster localhost \`
		Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias

	`--bucket <SOURCE BUCKET NAME> \`
	`--format lines \`
	`--username <USERNAME> \`
	`--password <PASSWORD> \`
	`--include-key cbkey \`
	`--scope-field cbscope \`
	`--collection-field cbcoll \`
	`--output cbexported_data.json`
	
	Observe que `cbkey`, `cbscope`, `cbcoll`, e `cbexported_data.json` são rótulos arbitrários. Eles serão referenciados posteriormente no processo, portanto, se você optar por nomeá-los de forma diferente, anote-os.	

Tarefa	Descrição	Habilidades necessárias
Importe dados para o Couchbase Capella.	1. No ambiente de gerenciamento Couchbase Capella, escolha Clusters e, em seguida, escolha o cluster de destino. 2. Na lista suspensa Ferramentas, escolha Importar. Isso abrirá um assistente com as seis etapas a seguir: a. Bucket: escolha o bucket de destino. b. Arquivo: escolha JSON, escolha Linhas e, em seguida, escolha Usando seu navegador da web. Se você tiver uma grande quantidade de dados, poderá explorar a opção Manualmente. Selecione o arquivo criado por `cbexport`. c. Coleções: escolha Mapeamento de coleção personalizado. Se seu banco de dados do Community Edition não usa escopos ou coleções, ou usa apenas _default, você pode escolher a opção Selecionar coleção única.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	Em Expressão de mapeamento de coleção, insira `%cbscope% .%cbcoll%` . Para verificar se essa expressão funciona corretamente, você pode colar dados de exemplo, como os seguintes. `{ "cbscope" :"inventory", "cbcoll":"landmark", "cbkey":" landmark_3991" }` d. Chave: escolha a geração de clientes. (Se você não se importa em preservar as chaves dos dados que está importando, selecione UUID gerado automaticamente e vá para a etapa 5.) Para Expressão do gerador de nome de chave, insira %cbkey%. Para verificar se essa expressão funciona corretamente, cole alguns dados de exemplo. e. Configurações: escolha Ignorar campos e insira cbscope,cbcoll,cbk	

Tarefa	Descrição	Habilidades necessárias
	ey. Esses campos contêm informações transitórias que não precisam estar no bucket de destino após uma importação. Deixe as outras configurações nos valores padrão. f. Importar: revise e escolha Importar quando estiver pronto. Aguarde o upload e a importação dos dados. Para arquivos grandes, o Couchbase Capella suporta importação de linha de comando usando cURL. Você pode explorar as opções de importação com mais detalhes em Importar dados na documentação do Couchbase Capella.	

Testar e verificar a migração

Tarefa	Descrição	Habilidades necessárias
Verificar a migração de dados.	1. No ambiente de gerenciamento do Couchbase Capella, escolha Clusters e, em seguida, escolha o cluster de destino na sua lista de clusters.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
	2. Escolha a guia Buckets para seu cluster de destino. Verifique se o número de itens (documentos) no bucket de destino corresponde ao número de itens no bucket de origem. 3. No cluster de destino, na lista suspensa Ferrament as, escolha Documento s. Verifique se todos os documentos foram migrados. 4. (Opcional) Depois que todos os dados forem migrados, você poderá encerrar a replicação excluindo-a. Para obter mais informações, consulte Excluir uma replicaçã o na documentação do Couchbase.	
Verifique a migração do índice.	No ambiente de gerenciam ento do Couchbase Capella, na lista suspensa Ferrament as do seu cluster de destino, escolha Índices. Verifique se os índices foram migrados e criados.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
Verificar resultados da consulta.	1. No ambiente de gerenciamento do Couchbase Capella, na lista suspensa Ferramentas do seu cluster de destino, escolha Bancada de consultas. 2. Execute uma consulta N1QL de amostra ou uma consulta usada em seu aplicativo. Lembre-se de receber os mesmos resultados de quando executa a consulta em seu cluster autogerenciado do Couchbase Server.	Administrador do Couchbase

Tarefa	Descrição	Habilidades necessárias
Verifique os resultados da pesquisa em texto completo (aplicável se você migrou os índices do FTS).	1. No ambiente de gerenciamento do Couchbase Capella, na lista suspensa Ferramentas do seu cluster de destino, escolha Full Text Search. 2. Selecione um índice FTS escolhendo seu nome. 3. Selecione a opção Pesquisar. 4. Insira um exemplo de consulta de pesquisa e escolha Pesquisar. 5. Verifique se os resultados são os mesmos de quando você executa a pesquisa em seu cluster autogerenciado.	Administrador do Couchbase

Recursos relacionados

Prepare a migração

- Comece com o teste gratuito do Couchbase Capella
- Requisitos do provedor de nuvem para o Couchbase Capella
- Diretrizes de dimensionamento do Couchbase Capella

Migre os dados e os índices

- Couchbase XDCR
- Documentação do Couchbase Shell

Couchbase SLAs Capella e suporte

- Contratos de nível de serviço do Couchbase Capella () SLAs
- Política de suporte do Couchbase Capella Service

Mais informações

O seguinte código é um exemplo de arquivo de configuração bean para Couchbase Shell.

```
Version = 1

[[clusters]]
identifier = "On-Prem-Cluster"
hostnames = ["<SELF_MANAGED_COUCHBASE_CLUSTER>"]
default-bucket = "travel-sample"
username = "<SELF_MANAGED_ADMIN>"
password = "<SELF_MANAGED_ADMIN_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"

[[clusters]]
identifier = "Capella-Cluster"
hostnames = ["<COUCHBASE_CAPELLA_ENDPOINT>"]
default-bucket = "travel-sample"
username = "<CAPELLA_DATABASE_USER>"
password = "<CAPELLA_DATABASE_USER_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"
```

Antes de salvar o arquivo de configuração, use a tabela a seguir para garantir que você tenha adicionado suas próprias informações do cluster de origem e destino.

<SELF_MANAGED_COUCHBASE_CLUSTER>	Use o endereço IP do seu cluster autogeren ciado do Couchbase Server.
<SELF_MANAGED_ADMIN>	Use o usuário administrador para seu cluster autogerenciado do Couchbase Server.

<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>	Use o caminho absoluto para o arquivo de certificado raiz salvo para seu cluster autogerenciado do Couchbase Server.
<COUCHBASE_CAPELLA_ENDPOINT>	Use o endpoint de conexão para seu cluster Couchbase Capella.
<CAPELLA_DATABASE_USER>	Use o usuário do banco de dados para seu cluster Couchbase Capella.
<CAPELLA_DATABASE_USER_PWD>	Use a senha de usuário do banco de dados para seu cluster Couchbase Capella.
<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>	Use o caminho absoluto para o arquivo de certificado raiz salvo para seu cluster Couchbase Capella.

Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2

Criado por Neal Ardeljan (AWS) e Afroz Khan (AWS)

Resumo

Esse padrão orienta você pelas etapas de migração de um sistema local Red Hat Enterprise Linux (RHEL) 6.9 ou posterior que esteja executando o IBM WebSphere Application Server (WAS) para o RHEL 8 executando o Apache Tomcat em uma instância do Amazon Elastic Compute Cloud (Amazon). EC2

O padrão pode ser aplicado às seguintes versões de origem e destino:

- WebSphere Servidor de aplicativos 7.x para Apache Tomcat 8 (com Java 7 ou posterior)
- WebSphere Servidor de aplicativos 8.x para Apache Tomcat 8 (com Java 7 ou posterior)
- WebSphere Servidor de aplicativos 8.5.5.x para Apache Tomcat 9 (com Java 8 ou posterior)
- WebSphere Servidor de aplicativos 8.5.5.x para Apache Tomcat 10 (com Java 8 ou posterior)

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Código-fonte Java, com as seguintes pressuposições:
  - Usa a versão Java Development Kit (JDK) do Java 7 ou superior
  - Usa a estrutura Spring ou Apache Struts
  - Não usa a estrutura Enterprise Java Beans (EJB) ou qualquer outra funcionalidade de WebSphere servidor que não esteja prontamente disponível para o Tomcat
  - Usa principalmente servlets ou Java Server Pages () JSPs
  - Usa conectores Java Database Connectivity (JDBC) para se conectar a bancos de dados
- Fonte IBM WebSphere Application Server versão 7.x ou superior
- Destino: Apache Tomcat versão 8.5 ou superior

Arquitetura

Pilha de tecnologia de origem

- Um aplicativo web criado usando a estrutura Apache Struts Model-View-Controller (MVC)
- Um aplicativo web executado no IBM WebSphere Application Server versão 7.x ou 8.x
- Um aplicativo web que usa um conector Lightweight Directory Access Protocol (LDAP) para se conectar a um diretório LDAP (iPlanet/eTrust)
- Um aplicativo que usa a conectividade do IBM Tivoli Access Manager (TAM) para atualizar a senha do usuário TAM (na implementação atual, os aplicativos usam PD.jar)

Bancos de dados on-premises

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)
- Oracle Database 12c Versão 2 (12.2.0.1)
- Oracle Database 12c Versão 1 (12.1.0.2)

Pilha de tecnologias de destino

- Apache Tomcat versão 8 (ou posterior) em execução no RHEL em uma instância EC2
- Amazon Relational Database Service (Amazon RDS) para Oracle

Para obter mais informações sobre as versões do Oracle compatíveis do Amazon RDS, consulte o site do Amazon RDS para Oracle.

Arquitetura de destino

Ferramentas

- Nível do aplicativo: reconstruindo o aplicativo Java em um arquivo WAR.
- Nível do banco de dados: backup e restauração nativos do Oracle.
- Ferramenta de migração Apache Tomcat para Jakarta EE. Essa ferramenta pega um aplicativo web escrito para Java EE 8 executado no Apache Tomcat 9 e o converte automaticamente para execução no Apache Tomcat 10, que implementa o Jakarta EE 9.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Conclua a descoberta do aplicativo, o estado atual e a linha de base de desempenho.		BA, líder de migração
Valide as versões dos bancos de dados de origem e de destino.		DBA
Identifique os requisitos de hardware para a EC2 instância do servidor de destino.		DBA, SysAdmin
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, SysAdmin
Escolha o tipo de EC2 instância adequado com base na capacidade, nos recursos de armazenamento e nos recursos de rede.		DBA, SysAdmin
Identifique os requisitos de segurança de acesso à rede para os bancos de dados de origem e de destino.		DBA, SysAdmin
Identifique a estratégia e as ferramentas de migração de aplicativos.		DBA, líder de migração

Tarefa	Descrição	Habilidades necessárias
Concluir o projeto da migração e o guia de migração do aplicativo.		Líder de desenvolvimento, líder de migração
Concluir o runbook de migração do aplicativo.		Líder de construção, líder de substituição, líder de teste, líder de migração

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).		SysAdmin
Criar grupos de segurança.		SysAdmin
Configurar e iniciar o Amazon RDS para Oracle.		DBA, SysAdmin

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Crie ou obtenha acesso aos endpoints para buscar os arquivos de backup do banco de dados.		DBA
Use o mecanismo de banco de dados nativo ou uma ferramenta de terceiros para migrar objetos e dados do banco de dados.	Para obter detalhes, consulte “Migrar objetos e dados do banco de dados” na seção Informações adicionais.	DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Apresentar a change request (CR – solicitação de alteração) para migração.		Líder de substituição
Obtenha a aprovação do CR para migração.		Líder de substituição
Siga a estratégia de migração de aplicativos de acordo com o runbook de migração de aplicativos.	Para obter detalhes, consulte “Como configurar a camada do aplicativo” na seção Informações adicionais.	DBA, engenheiro de migração, proprietário do aplicativo
Atualize o aplicativo (se necessário).		DBA, engenheiro de migração, proprietário do aplicativo
Conclua os testes funcionais e não funcionais de validação de dados, SLA e desempenho.		Líder de teste, proprietário do aplicativo, usuários do aplicativo

Substituir

Tarefa	Descrição	Habilidades necessárias
Obtenha a aprovação do proprietário do aplicativo ou do proprietário da empresa.		Líder de substituição
Mude os clientes do aplicativo para a nova infraestrutura.		DBA, engenheiro de migração, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, engenheiro de migração, SysAdmin
Revise e valide os documentos do projeto.		Líder de migração
Reúna métricas como tempo de migração, porcentagem de tarefas manuais versus automatizadas e economia de custos.		Líder de migração
Feche o projeto e forneça feedback.		Líder de migração, proprietário do aplicativo

Recursos relacionados

Referências

- Documentação do Apache Tomcat 10.0
- Documentação do Apache Tomcat 9.0
- Documentação do Apache Tomcat 8.0
- Guia de instalação do Apache Tomcat 8.0
- Documentação do Apache Tomcat JNDI
- Site do Amazon RDS para Oracle
- Preços do Amazon RDS
- Oracle e Amazon Web Services
- Oracle no Amazon RDS
- Implantações multi-AZ do Amazon RDS

Tutoriais e vídeos

- Conceitos básicos do Amazon RDS

Mais informações

Migração de objetos e dados do banco de dados

Por exemplo, se você estiver usando utilitários nativos de backup/restauração da Oracle:

1. Criar o backup do Amazon Simple Storage Service (Amazon S3) para arquivos de backup do banco de dados (opcional).
2. Faça backup dos dados do Oracle DB na pasta compartilhada da rede.
3. Faça login no servidor de preparação da migração para mapear a pasta de compartilhamento de rede.
4. Copie dados da pasta de compartilhamento de rede para o bucket do S3.
5. Solicite uma implantação do Multi-AZ do Amazon RDS para Oracle.
6. Restaure o backup do banco de dados on-premises no Amazon RDS para Oracle.

Como configurar o nível do aplicativo

1. Instale o Tomcat 8 (ou 9/10) no site do Apache Tomcat.
2. Compacte o aplicativo e as bibliotecas compartilhadas em um arquivo WAR.
3. Implante o arquivo WAR no Tomcat.
4. Monitore o registro inicial de `Linux cat` todas as bibliotecas compartilhadas ausentes do WebSphere.
5. Assista ao registro inicial de `Linux cat` qualquer extensão WebSphere específica do descritor de implantação.
6. Colete todas as bibliotecas Java dependentes ausentes do WebSphere servidor.
7. Altere elementos WebSphere específicos do descritor de implantação com equivalentes compatíveis com Tomcat.
8. Reconstrua o arquivo WAR com as bibliotecas Java dependentes e os descritores de implantação atualizados.
9. Atualize a configuração LDAP, a configuração do banco de dados e as conexões de teste (consulte COMO FAZER a configuração do Realm) e COMO FAZER uma fonte de dados JNDI na documentação do Apache Tomcat).

10. Teste o aplicativo instalado no banco de dados do Amazon RDS para Oracle restaurado.
11. Crie uma Amazon Machine Image (AMI) para Linux a partir da EC2 instância.
12. Inicie a arquitetura completa com o grupo Application Load Balancer e grupo do Auto Scaling (ajuste de escala automático).
13. Atualize o URLs (usando a junção WebSEAL) para apontar para o Application Load Balancer.
14. Atualize o banco de dados de gerenciamento de configuração (CMDB).

Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2 com o Auto Scaling

Criado por Kevin Yung (AWS) e Afroz Khan (AWS)

Resumo

Esse padrão fornece orientação para migrar um aplicativo Java do IBM WebSphere Application Server para o Apache Tomcat em uma EC2 instância do Amazon Elastic Compute Cloud (Amazon) com o Amazon Auto EC2 Scaling ativado.

Ao usar esse padrão, você pode conseguir:

- Uma redução nos custos de licenciamento da IBM
- Alta disponibilidade usando implantação Multi-AZ
- Melhor resiliência de aplicativos com o Amazon EC2 Auto Scaling

Pré-requisitos e limitações

Pré-requisitos

- Aplicações Java (versão 7.x ou 8.x) devem ser desenvolvidas em pilhas LAMP.
- O estado de destino é hospedar aplicativos Java em hosts Linux. Esse padrão foi implementado com sucesso em um ambiente Red Hat Enterprise Linux (RHEL) 7. Outras distribuições Linux podem seguir esse padrão, mas a configuração da distribuição Apache Tomcat deve ser referenciada.
- Você deve entender as dependências do aplicativo Java.
- Você deve ter acesso ao código-fonte do aplicativo Java para fazer alterações.

Limitações e mudanças na redefinição da plataforma

- Você deve compreender os componentes do arquivamento corporativo (EAR) e verificar se todas as bibliotecas estão empacotadas nos arquivos WAR do componente web. Você precisa configurar o plug-in WAR do Apache Maven e produzir artefatos de arquivo WAR.
- Ao usar o Apache Tomcat 8, há um conflito conhecido entre o servlet-api.jar e os arquivos JAR integrados do pacote do aplicativo. Para resolver esse problema, exclua o servlet-api.jar do pacote do aplicativo.

- Você deve configurar WEB-INF/Resources localizados no classpath da configuração do Apache Tomcat. Por padrão, as bibliotecas JAR não são carregadas no diretório. Como alternativa, você pode implantar todos os recursos abaixo src/main/resources.
- Verifique se há raízes de contexto de codificação rígida no aplicativo Java e atualize a nova raiz de contexto do Apache Tomcat.
- Para definir as opções de runtime da JVM, você pode criar o arquivo de configuração setenv.sh na pasta bin do Apache Tomcat; por exemplo, JAVA_OPTS, JAVA_HOME etc.
- A autenticação é configurada no nível do contêiner e configurada como uma região nas configurações do Apache Tomcat. A autenticação é estabelecida para qualquer um dos três domínios a seguir:
  - O JDBC Database Realm pesquisa usuários em um banco de dados relacional acessado pelo driver JDBC.
  - DataSource O Database Realm pesquisa usuários em um banco de dados que é acessado pelo JNDI.
  - O JNDI Directory Realm pesquisa usuários no diretório Lightweight Directory Access Protocol (LDAP) que é acessado pelo provedor JNDI. As pesquisas exigem:
    - Detalhes da conexão LDAP: base de pesquisa de usuário, filtro de pesquisa, base de perfil, filtro de perfil
    - A principal região do diretório JNDI: conecta-se ao LDAP, autentica usuários e recupera todos os grupos dos quais um usuário é membro
- Autorização: no caso de um contêiner com uma autorização baseada em funções que verifica as restrições de autorização em web.xml, os recursos da Web devem ser definidos e comparados às funções definidas nas restrições. Se o LDAP não tiver mapeamento de função de grupo, você deverá definir o atributo < security-role-ref > em web.xml para obter o mapeamento de função de grupo. Para ver um exemplo de um documento de configuração, consulte a documentação da Oracle.
- Conexão de banco de dados: crie uma definição de recurso no Apache Tomcat com um URL de endpoint do Amazon Relational Database Service (Amazon RDS) e detalhes de conexão. Atualize o código do aplicativo para fazer referência a DataSource usando a pesquisa JNDI. Uma conexão de banco de dados existente definida em não WebSphere funcionaria, pois usa os nomes WebSphere JNDI. Você pode adicionar uma <resource-ref>entrada em web.xml com o nome JNDI e a definição do DataSource tipo. Para ver um exemplo de documento de configuração, consulte a documentação do Apache Tomcat.

- Registro: por padrão, o Apache Tomcat faz o registro de logs no console ou em um arquivo de log. Você pode ativar o rastreamento em nível de domínio atualizando logging.properties (consulte Registro em log no Tomcat). Se você estiver usando o Apache Log4j para anexar registros em log a um arquivo, você deve baixar o tomcat-juli e adicioná-lo ao classpath.
- Gerenciamento de sessão: se você estiver mantendo o IBM WebSEAL para Application Load Balancer e gerenciamento de sessões, nenhuma alteração será necessária. Se você estiver usando um Application Load Balancer ou Network Load Balancer na AWS para substituir o componente IBM WebSEAL, deverá configurar o gerenciamento de sessões usando uma instância da ElastiCache Amazon com um cluster Memcached e configurar o Apache Tomcat para usar o gerenciamento de sessões de código aberto.
- Se você estiver usando o proxy de encaminhamento IBM WebSEAL, deverá configurar um novo Network Load Balancer na AWS. Use o IPs fornecido pelo Network Load Balancer para configurações de junção do WebSEAL.
- Configuração SSL: recomendamos que você use o Secure Sockets Layer (SSL) para comunicações. end-to-end Para definir uma configuração de servidor SSL no Apache Tomcat, siga as instruções na documentação do Apache Tomcat.

Arquitetura

Pilha de tecnologia de origem

- Servidor WebSphere de aplicativos IBM

Pilha de tecnologias de destino

- A arquitetura usa o Elastic Load Balancing (versão 2). Se você estiver usando o IBM WebSEAL para gerenciamento e balanceador de carga do Identify, poderá selecionar um Network Load Balancer na AWS para integrar com o proxy reverso IBM WebSEAL.
- Os aplicativos Java são implantados em um servidor de aplicativos Apache Tomcat, que é executado em uma EC2 instância em um grupo do Amazon Auto Scaling. EC2 Você pode configurar uma política de escalabilidade com base nas CloudWatch métricas da Amazon, como a utilização da CPU.
- Se você estiver retirando o uso do IBM WebSEAL para balanceamento de carga, poderá usar o Amazon ElastiCache for Memcached para gerenciamento de sessões.

- Para o banco de dados de backend, você pode implantar a Alta Disponibilidade (Multi-AZ) para o Amazon RDS e selecionar um tipo de mecanismo de banco de dados.

Arquitetura de destino

Ferramentas

- AWS CloudFormation
- AWS Command Line Interface (AWS CLI)
- Apache Tomcat (versão 7.x ou 8.x)
- RHEL 7 ou Centos 7
- Implantação do Multi-AZ do Amazon RDS
- Amazon ElastiCache para Memcached (opcional)

Épicos

Configuração da VPC

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).		
Crie sub-redes.		
Crie tabelas de roteamento, se necessário.		
Crie listas de controle de acesso à rede (ACLs).		
Configure o AWS Direct Connect ou uma conexão VPN corporativa.		

Redefina a plataforma do aplicativo

Tarefa	Descrição	Habilidades necessárias
Refatore a configuração do Maven de compilação do aplicativo para gerar os artefatos WAR.		
Refatore as fontes de dados de dependência do aplicativo no Apache Tomcat.		
Refatore os códigos-fonte do aplicativo para usar nomes JNDI no Apache Tomcat.		
Implante os artefatos WAR no Apache Tomcat.		
Validações e testes completos do aplicativo.		

Configure a rede

Tarefa	Descrição	Habilidades necessárias
Configure o firewall corporativo para permitir a conexão com os serviços de dependência.		
Configure o firewall corporativo para permitir que o usuário final acesse o Elastic Load Balancing na AWS.		

Crie a infraestrutura de aplicativos

Tarefa	Descrição	Habilidades necessárias
Crie e implante o aplicativo em uma EC2 instância.		
Crie um cluster Amazon ElastiCache for Memcached para gerenciamento de sessões.		
Crie uma instância do Multi-AZ do Amazon RDS para o banco de dados de backend.		
Crie certificados SSL e importe-os para o AWS Certificate Manager (ACM).		
Instale certificados SSL em balanceadores de carga.		
Instale certificados SSL para servidores Apache Tomcat.		
Validações e testes completos do aplicativo.		

Substituir

Tarefa	Descrição	Habilidades necessárias
Encerre a infraestrutura existente.		

Tarefa	Descrição	Habilidades necessárias
Restaure o banco de dados da produção para o Amazon RDS.		
Substitua o aplicativo fazendo alterações no DNS.		

Recursos relacionados

Referências

- Documentação do Apache Tomcat 7.0
- Guia de instalação do Apache Tomcat 7.0
- Documentação do Apache Tomcat JNDI
- Implantações multi-AZ do Amazon RDS
- Amazon ElastiCache para Memcached

Tutoriais e vídeos

- Conceitos básicos do Amazon RDS

Migre uma aplicação .NET do Microsoft Azure App Service para o AWS Elastic Beanstalk

Criado por Raghavender Madamshitti (AWS)

Resumo

Esse padrão descreve como migrar um aplicativo web.NET hospedado no Microsoft Azure App Service para o AWS Elastic Beanstalk. Há duas maneiras de migrar aplicativos para o Elastic Beanstalk:

- Use o AWS Toolkit for Visual Studio: Esse plug-in para o IDE do Microsoft Visual Studio fornece a maneira mais fácil e direta de implantar aplicativos.NET personalizados na AWS. Você pode usar essa abordagem para implantar código.NET diretamente na AWS e criar recursos de suporte, como o Amazon Relational Database Service (Amazon RDS) para bancos de dados SQL Server, diretamente do Visual Studio.
- Carregar e implantar no Elastic Beanstalk: cada Serviço de Aplicativo do Azure inclui um serviço em segundo plano chamado Kudu, que é útil para capturar despejos de memória e registros de implantação, visualizar parâmetros de configuração e acessar pacotes de implantação. Você pode usar o console Kudu para acessar o conteúdo do Azure App Service, extrair o pacote de implantação e, em seguida, carregar o pacote no Elastic Beanstalk usando a opção de upload e implantação no console do Elastic Beanstalk.

Esse padrão descreve a segunda abordagem (fazer o upload do seu aplicativo para o Elastic Beanstalk por meio do Kudu). O padrão também usa os seguintes serviços da AWS: AWS Elastic Beanstalk, Amazon Virtual Private Cloud (Amazon VPC), Amazon, Amazon Elastic Compute Cloud (CloudWatchAmazon) Auto Scaling, EC2 Amazon Simple Storage Service (Amazon S3) e Amazon Route 53.

O aplicativo web.NET é implantado no AWS Elastic Beanstalk, que é executado em um grupo Amazon EC2 Auto Scaling. Você pode configurar uma política de escalabilidade com base nas CloudWatch métricas da Amazon, como a utilização da CPU. No caso de banco de dados, você pode usar o Amazon RDS em um ambiente Multi-AZ ou o Amazon DynamoDB, dependendo do seu aplicativo e dos requisitos comerciais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo web.NET em execução no Serviço de Aplicativo do Azure
- Permissão para usar o console Kudu do Serviço de Aplicativo do Azure

Versões do produto

- .NET Core (x64) 1.0.1, 2.0.0 ou superior, ou .NET Framework 4.x, 3.5 (consulte .NET no histórico da plataforma do Windows Server)
- Serviços de Informações da Internet (IIS) versão 8.0 ou superior, em execução no Windows Server 2012 ou superior
- .NET 2.0 ou 4.0 runtime.

Arquitetura

Pilha de tecnologia de origem

- Aplicativo desenvolvido usando o .NET Framework 3.5, ou superior, ou .NET Core 1.0.1, 2.0.0 ou superior e hospedado no Serviço de Aplicativo do Azure (aplicativo web ou aplicativo de API)

Pilha de tecnologias de destino

- AWS Elastic Beanstalk em execução em um grupo do Amazon EC2 Auto Scaling

Arquitetura de migração

Fluxo de trabalho de implantação

Ferramentas

Ferramentas

- .NET Core ou .NET Framework
- C#
- IIS

- Console Kudu

Serviços e atributos da AWS

- AWS Elastic Beanstalk — O Elastic Beanstalk é um serviço para implantar e easy-to-use escalar aplicativos web.NET. O Elastic Beanstalk gerencia automaticamente o provisionamento de capacidade, o balanceamento de carga e o escalonamento automático.
- Grupo Amazon EC2 Auto Scaling — O Elastic Beanstalk inclui um grupo de Auto Scaling que gerencia as instâncias da Amazon no ambiente. EC2 Em um ambiente de instância única, o grupo de Auto Scaling garante que sempre haja uma instância em execução. Em um ambiente com balanceamento de carga, você pode configurar o grupo com uma variedade de instâncias para execução, e o Amazon EC2 Auto Scaling adiciona ou remove instâncias conforme necessário, com base na carga.
- Elastic Load Balancing — Quando você ativa o balanceamento de carga no AWS Elastic Beanstalk, ele cria um balanceador de carga que distribui o tráfego entre as instâncias no ambiente. EC2
- Amazon CloudWatch — O Elastic Beanstalk CloudWatch usa automaticamente a Amazon para fornecer informações sobre seus recursos de aplicativo e ambiente. A Amazon CloudWatch oferece suporte a métricas padrão, métricas personalizadas e alarmes.
- Amazon Route 53: o Amazon Route 53 é um web service de Sistema de Nomes de Domínio (DNS) altamente disponível e dimensionável. Você pode usar os registros de alias do Route 53 para mapear nomes de domínio personalizados para ambientes do AWS Elastic Beanstalk.

Épicos

Configurar uma VPC

Tarefa	Descrição	Habilidades necessárias
Configurar uma nuvem privada virtual (VPC).	Na sua conta da AWS, crie uma VPC com as informações necessárias.	Administrador de sistema
Crie sub-redes.	Crie duas ou mais sub-redes em sua VPC.	Administrador de sistema

Tarefa	Descrição	Habilidades necessárias
Crie uma tabela de rotas.	Crie uma tabela de rotas com base em seus requisitos.	Administrador de sistema

Configurar Elastic Beanstalk

Tarefa	Descrição	Habilidades necessárias
Acessar o console Kudu do Serviço de Aplicativo do Azure.	Acesse o Kudu por meio do portal do Azure navegando até o painel do Serviço de Aplicativo e escolhendo Ferramentas Avançadas, Go. Ou então, você pode modificar a URL do Serviço de Aplicativo do Azure da seguinte forma: `https://<appservicename>.scm.azurewebsites.net` .	Desenvolvedor de aplicativos, administrador do sistema
Baixe o pacote de implantação do Kudu.	Navegue até o Windows PowerShell escolhendo a DebugConsoleopção. Isso abrirá o console do Kudo. Vá até a pasta `wwwroot` e faça o download. Isso baixará o pacote de implantação do Serviço de Aplicativo do Azure como um arquivo zip. Para ver um exemplo, consulte o anexo.	Desenvolvedor de aplicativos, administrador do sistema
Crie um pacote para o Elastic Beanstalk.	Descompacte o pacote de implantação que você baixou do Serviço de Aplicativo	Desenvolvedor de aplicativos, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
	do Azure. Crie um arquivo JSON chamado `aws-windows-deployment-manifest.json` (esse arquivo é necessário somente para aplicativos.NET Core). Crie um arquivo zip que inclua `aws-windows-deployment-manifest.json` e o arquivo do pacote de implantação do Serviço de Aplicativo do Azure. Para ver um exemplo, consulte o anexo.	
Crie um novo aplicativo do Elastic Beanstalk.	Abra o console do Elastic Beanstalk. Escolha um aplicativo existente ou crie um aplicativo novo.	Desenvolvedor de aplicativos, administrador do sistema
Criar o ambiente	No menu Ações do console do Elastic Beanstalk, escolha Criar ambiente. Selecione o ambiente do servidor web e a plataforma .NET/IIS. Em Código do aplicativo, escolha Fazer upload. Faça upload do arquivo zip que você preparou para o Elastic Beanstalk e escolha Create Environment.	Desenvolvedor de aplicativos, administrador do sistema

Tarefa	Descrição	Habilidades necessárias
Configure a Amazon CloudWatch.	Por padrão, o CloudWatch monitoramento básico está ativado. Se você quiser alterar a configuração, no assistente do Elastic Beanstalk, escolha o aplicativo publicado e, em seguida, escolha Monitoram ento.	Administrador de sistema
Verifique se o pacote de implantação está no Amazon S3.	Quando o ambiente do aplicativo for criado, você poderá encontrar o pacote de implantação no bucket do S3.	Desenvolvedor de aplicativos, administrador do sistema
Testar o aplicativo.	Quando o ambiente for criado, use a URL fornecida no console do Elastic Beanstalk para testar a aplicação.	Administrador de sistema

Recursos relacionados

- Conceitos do AWS Elastic Beanstack (Documentação do Elastic Beanstalk)
- Conceitos básicos do .NET no Elastic Beanstalk (Documentação do Elastic Beanstalk)
- Consola Kudu () GitHub
- Usar o “Kudu” para gerenciar aplicativos Web do Azure (artigo do GS Lab)
- Implantações personalizadas do ASP.NET Core Elastic Beanstalk (guia do usuário do AWS Toolkit for Visual Studio)
- Documentação do Elastic Load Balancing
- Plataformas com suporte do AWS Elastic Beanstalk (Documentação do Elastic Beanstalk)
- Implante um aplicativo web na AWS (artigo da C# Corner)
- Dimensionando o tamanho do seu grupo de Auto Scaling (documentação da Amazon EC2)
- Alta disponibilidade (Multi-AZ) para o Amazon RDS (Documentação do Amazon RDS)

Mais informações

Observações

- Se você estiver migrando um banco de dados local ou do Azure SQL Server para o Amazon RDS, também deverá atualizar os detalhes da conexão do banco de dados.
- Para fins de teste, um exemplo de aplicativo de demonstração é anexado.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre do Oracle WebLogic para o Apache Tomcat (TomEE) no Amazon ECS

Criado por Anya Epishcheva (AWS) e Harshad Gohil (AWS)

Resumo

Esse padrão discute as etapas para migrar um sistema Oracle Solaris SPARC local executando Oracle para uma instalação baseada em contêiner Docker executando o Apache TomEE (Apache Tomcat com suporte adicional de contêiner) com o Amazon Elastic Container Service (Amazon ECS). WebLogic

Para obter informações sobre a migração de bancos de dados associados aos aplicativos que você está migrando do Oracle WebLogic para o Tomcat, consulte os padrões de migração de banco de dados neste catálogo.

Práticas recomendadas

As etapas para migrar aplicativos web Java e Java Enterprise Edition (Java EE) variam, dependendo do número de recursos específicos do contêiner usados pelo aplicativo. Os aplicativos baseados em Spring geralmente são mais fáceis de migrar, porque eles têm um pequeno número de dependências no contêiner de implantação. Por outro lado, os aplicativos Java EE que usam Enterprise JavaBeans (EJBs) e recursos gerenciados de contêiner, como pools de threads, Java Authentication and Authorization Service (JAAS) e Container-Managed Persistence (CMP) exigem mais esforço.

Os aplicativos desenvolvidos para o Oracle Application Server frequentemente usam o pacote Oracle Identity Management. Os clientes que migram para servidores de aplicativos de código aberto frequentemente optam por reimplementar o gerenciamento de identidade e acesso usando a federação baseada em SAML. Outros usam o Oracle HTTP Server Webgate para casos em que migrar do pacote Oracle Identity Management não é uma opção.

Os aplicativos web Java e Java EE são ótimos candidatos para implantação em serviços da AWS baseados em Docker, como o AWS Fargate e o Amazon ECS. Os clientes frequentemente escolhem uma imagem do Docker com a versão mais recente do servidor de aplicativos de destino (como o TomEE) e o Java Development Kit (JDK) pré-instalados. Eles instalam seus aplicativos em cima da imagem base do Docker, a publicam no registro do Amazon Elastic Container Registry (Amazon ECR) e a usam para a implantação escalável de seus aplicativos no AWS Fargate ou no Amazon ECS.

Idealmente, a implantação do aplicativo é elástica; ou seja, o número de instâncias do aplicativo aumenta ou diminui, dependendo do tráfego ou da workload. Isso significa que as instâncias do aplicativo precisam ficar on-line ou ser encerradas para ajustar a capacidade à demanda.

Ao migrar um aplicativo Java para a AWS, considere torná-lo sem estado. Esse é um princípio arquitetônico fundamental do AWS Well-Architected Framework que permitirá a escalabilidade horizontal usando a conteinerização. Por exemplo, a maioria dos aplicativos web baseados em Java armazena localmente as informações da sessão do usuário. Para sobreviver ao encerramento da instância do aplicativo devido ao escalonamento automático no Amazon Elastic Compute Cloud EC2 (Amazon) ou por outros motivos, as informações da sessão do usuário devem ser armazenadas globalmente para que os usuários do aplicativo web possam continuar trabalhando de forma contínua e transparente sem se reconectar ou se reconectar a um aplicativo web. Há várias opções de arquitetura para essa abordagem, incluindo Amazon ElastiCache for Redis ou armazenar o estado da sessão em um banco de dados global. Servidores de aplicativos, como o TomEE, têm plug-ins que permitem o armazenamento e o gerenciamento de sessões via Redis, bancos de dados e outros armazenamentos de dados globais.

Use uma ferramenta comum e centralizada de registro e depuração que seja facilmente integrada à Amazon e ao AWS CloudWatch X-Ray. A migração oferece uma oportunidade de melhorar os recursos do ciclo de vida do aplicativo. Por exemplo, talvez você queira automatizar o processo de criação para que as alterações sejam feitas com facilidade usando um pipeline de integração contínua e entrega contínua (CI/CD). Isso pode exigir alterações no aplicativo para que ele possa ser implantado sem qualquer tempo de inatividade.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Código-fonte Java e JDK
- Aplicativo de origem criado com Oracle WebLogic
- Solução definida para gerenciamento de identidade e acesso (SAML ou Oracle Webgate)
- Solução definida para gerenciamento de sessões de aplicativos (migrando like-for-like ou com a Amazon ElastiCache, ou tornando o aplicativo sem estado, se necessário)
- Entendendo se a equipe precisa refatorar bibliotecas específicas do J2EE para portabilidade para o Apache toMEE (consulte Status de implementação do Java EE 7 no site do Apache)
- Imagem TomEE reforçada com base nos seus requisitos de segurança
- Imagem do contêiner com destino pré-instalado TomEE
- Correção de aplicativos acordada e implementada, se necessário (por exemplo, registro em log de debug de criação, autenticação)

Versões do produto

- Oracle WebLogic OC4 J, 9i, 10g
- Tomcat 7 (com Java 1.6 ou superior)

Arquitetura

Pilha de tecnologia de origem

- Aplicativo web criado usando Oracle WebLogic
- Aplicativo Web usando autenticação Oracle Webgate ou SAML
- Aplicativos Web conectados ao Oracle Database versão 10g e posterior

Pilha de tecnologias de destino

- TomEE (Apache Tomcat com suporte adicional a contêineres) em execução no Amazon ECS (consulte também Implantação de aplicativos Web Java e Microsserviços Java no Amazon ECS)
- Amazon Relational Database Service (Amazon RDS) para Oracle; para versões Oracle compatíveis com Amazon RDS, consulte Amazon RDS para Oracle

Arquitetura de destino

Ferramentas

Para operar no TomEE, um aplicativo Java deve ser reconstruído em um arquivo .war. Em alguns casos, podem ser necessárias alterações no aplicativo para operar o aplicativo no TomEE; você deve verificar se as opções de configuração e as propriedades do ambiente necessárias estão definidas corretamente.

Além disso, as pesquisas de Java Naming and Directory Interface (JNDI) e os namespaces JavaServer Pages (JSP) devem ser definidos corretamente. Considere verificar os nomes dos arquivos usados pelo aplicativo para evitar colisões de nomes com bibliotecas T integradas. Por exemplo, persistence.xml é um nome de arquivo usado pela estrutura Apache OpenJPA (que vem com o OpenEJB no TomEE) para fins de configuração. O arquivo persistence.xml na PUI contém declarações de bean do Spring framework.

O TomEE versão 7.0.3 e posterior (Tomcat 8.5.7 e posterior) retorna uma resposta HTTP 400 (solicitação inválida) para raw (não codificada) com caracteres especiais. URLs A resposta do servidor aparece como uma página em branco para o usuário final. As versões anteriores do TomEE e do Tomcat permitiam o uso de certos caracteres especiais não codificados em URLs; no entanto, isso é considerado inseguro, conforme declarado no site CVE-2016-6816. Para resolver o problema de codificação de URL, o URLs passado diretamente para o navegador JavaScript deve ser codificado com o método encodeURI () em vez de ser usado como strings brutas.

Depois de implantar o arquivo.war no TomEE, monitore o log de inicialização no Linux cat em busca de bibliotecas compartilhadas ausentes e extensões específicas do Oracle para adicionar componentes ausentes das bibliotecas Tomcat.

Procedimento geral

- Configure o aplicativo no TomEE.
- Identifique e reconfigure arquivos e recursos de configuração específicos do servidor de aplicativos, do formato de origem ao de destino.
- Identifique e reconfigure os recursos da JNDI.
- Ajuste o namespace EJB e as pesquisas para o formato exigido pelo servidor do aplicativo de destino (se aplicável).
- Reconfigure as funções de segurança e os mapeamentos principais específicos do contêiner do aplicativo JAAS (se aplicável).
- Empacote o aplicativo e as bibliotecas compartilhadas em um arquivo .war.
- Implante o arquivo .war no TomEE usando o contêiner do Docker fornecido.
- Monitore o log de início para identificar qualquer biblioteca compartilhada ausente e extensões de descritor de implantação. Se algum for encontrado, volte para a primeira tarefa.
- Teste o aplicativo instalado em relação ao banco de dados Amazon RDS restaurado.
- Inicie a arquitetura completa com um balanceador de carga e um cluster Amazon ECS seguindo as instruções em Implantar contêineres do Docker.
- Atualize o URLs para apontar para o balanceador de carga.
- Atualize o banco de dados de gerenciamento de configuração (CMDB).

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Executar a descoberta de aplicativos (pegada do estado atual e linha de base de desempenho).		BA, líder de migração
Validar versões e mecanismos do banco de dados de origem e de destino.		DBA
Validar o design do aplicativo de origem e de destino (gerenciamento de identidade e sessão).		DBA, engenheiro de migração, proprietário do aplicativo
Identificar os requisitos de hardware e armazenamento para a instância do servidor de destino.		DBA, SysAdmin
Escolher o tipo de instância adequado com base na capacidade, nos atributos de armazenamento e nos atributos de rede.		DBA, SysAdmin
Identifique os requisitos de segurança do acesso à rede para os bancos de dados de origem e de destino.		DBA, SysAdmin
Identificar a estratégia e as ferramentas de migração de aplicativos.		DBA, líder de migração

Tarefa	Descrição	Habilidades necessárias
Concluir o projeto da migração e o guia de migração do aplicativo.		Líder de desenvolvimento, líder de migração
Concluir o runbook de migração do aplicativo.		Líder de construção, líder de substituição, líder de teste, líder de migração

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).		SysAdmin
Criar grupos de segurança.		SysAdmin
Configurar e iniciar a instância de banco de dados do Amazon RDS.		DBA, SysAdmin
Configurar a implantação do Amazon ECS.		SysAdmin
Empacotar seu aplicativo como uma imagem do Docker.		SysAdmin
Enviar a imagem para o registro do Amazon ECR (ou pule esta etapa e envie-a para o cluster do Amazon ECS).		SysAdmin
Configurar a definição da tarefa para o aplicativo e as opções de serviço do Amazon ECS.		SysAdmin

Tarefa	Descrição	Habilidades necessárias
Configurar seu cluster, revise configurações de segurança e defina perfis do AWS Identity and Access Management (IAM).		SysAdmin
Iniciar sua configuração e execute testes de acordo com o runbook de migração do aplicativo.		SysAdmin

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Obter a permissão da sua equipe de garantia de segurança para mover dados de produção para a AWS.		DBA, engenheiro de migração, proprietário do aplicativo
Criar e obter acesso aos endpoints para buscar arquivos de backup do banco de dados.		DBA
Usar o mecanismo de banco de dados nativo ou ferrament as de terceiros para migrar objetos e dados do banco de dados.		DBA
Executar os testes necessári os no runbook de migração de aplicativos para confirmar		DBA, engenheiro de migração, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
a migração de dados bem-sucedida.		

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Criar uma solicitação de alteração (CR) para migração.		Líder de substituição
Obter a aprovação de CR para migração.		Líder de substituição
Seguir a estratégia de migração de aplicativos no runbook de migração de aplicativos.		DBA, engenheiro de migração, proprietário do aplicativo
Atualizar o aplicativo (se necessário).		DBA, engenheiro de migração, proprietário do aplicativo
Completar testes funcionais e não funcionais de validação de dados, SLA e desempenho.		Líder de teste, proprietário do aplicativo, usuários do aplicativo

Substituir

Tarefa	Descrição	Habilidades necessárias
Obter a aprovação do aplicativo ou do proprietário da empresa.		Líder de substituição

Tarefa	Descrição	Habilidades necessárias
Fazer um exercício com tópicos de tabela para percorrer todas as etapas do runbook de substituição.		DBA, engenheiro de migração, proprietário do aplicativo
Mudar os clientes do aplicativo para a nova infraestrutura.		DBA, engenheiro de migração, proprietário do aplicativo

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		DBA, engenheiro de migração, SysAdmin
Revise e valide os documentos do projeto.		Líder de migração
Reunir métricas sobre o tempo de migração, porcentagem de manual versus ferramenta, economia de custos, etc.		Líder de migração
Feche o projeto e forneça feedback.		Líder de migração, proprietário do aplicativo

Recursos relacionados

Referências

- Documentação do Apache Tomcat 7.0
- Guia de instalação do Apache Tomcat 7.0
- Documentação do Apache Tomcat JNDI
- Documentação do Apache ToMEE

- Amazon RDS para Oracle
- Preços do Amazon RDS
- Oracle e AWS
- Documentação da Oracle no Amazon RDS
- Implantações multi-AZ do Amazon RDS
- Conceitos básicos do Amazon ECS
- Conceitos básicos do Amazon RDS

Tutoriais e vídeos

- Práticas recomendadas para a execução de bancos de dados Oracle no Amazon RDS (ref.: apresentação Invent 2018)

Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for Oracle usando o AWS DMS

Criado por Chethan Gangadharaiah (AWS) e Brian motzer (AWS)

Resumo

Esse padrão descreve as etapas para migrar um banco de dados Oracle no Amazon Elastic Compute Cloud (Amazon EC2) para o Amazon Relational Database Service (Amazon RDS) for Oracle usando o AWS Database Migration Service (AWS DMS). O padrão também usa o Oracle SQL Developer ou o SQL *Plus para se conectar à sua instância de banco de dados Oracle e inclui um CloudFormation modelo da AWS que automatiza algumas das tarefas.

A migração para o Amazon RDS para Oracle permite que você se concentre em seus negócios e aplicativos, enquanto o Amazon RDS cuida das tarefas de administração do banco de dados, como provisionamento de bancos de dados, backup e recuperação, patches de segurança, atualizações de versão e gerenciamento de armazenamento.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma imagem de máquina da Amazon (AMI) para banco de dados Oracle na Amazon EC2

Versões do produto

- O AWS DMS é compatível com versões do Oracle 11g (versões 11.2.0.3.v1 e superior), 12c e 18c para bancos de dados de instâncias do Amazon RDS para as edições Enterprise, Standard, Standard One e Standard Two. Para obter as informações mais recentes sobre as versões compatíveis, consulte Uso de um banco de dados Oracle como destino para o AWS DMS na documentação da AWS. (Os CloudFormation modelos anexados da AWS usam o Oracle versão 12c como banco de dados de origem.)
- Oracle SQL Developer 4.0.3

Arquitetura

Arquitetura de origem

- Banco de dados Oracle na Amazon EC2

Arquitetura de destino

- Amazon RDS para Oracle

Arquitetura de migração

Ferramentas

- AWS DMS: o AWS Database Migration Service (AWS DMS) ajuda a migrar bancos de dados para a AWS de forma rápida e segura. Ele suporta migrações homogêneas e heterogêneas. Para obter informações sobre as versões e edições do banco de dados Oracle compatíveis, consulte Usando um banco de dados Oracle como origem para o AWS DMS e Usando um banco de dados Oracle como destino para o AWS DMS na documentação da AWS.
- Oracle SQL Developer ou SQL *Plus: essas ferramentas permitem que você se conecte à instância de banco de dados do Amazon RDS para Oracle.

Épicos

Configurar o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de banco de dados do Amazon RDS para Oracle.	Faça login no AWS Management Console e abra o console do Amazon RDS em https://console.aws.amazon.com/rds/. Crie uma instância de banco de dados Oracle selecionando o mecanismo, o modelo, a configuração de credenciais do banco de dados, o tipo de instância, o armazenamento, as configurações Multi-AZ, a	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	nuvem privada virtual (VPC) e a configuração, as credencia is de login e outras configura ções para o banco de dados Oracle. Para obter instruçõe s, consulte os links na seção “Recursos relacionados”. Ou use o CloudFormation modelo da AWS (Create_RDS.yaml) no anexo para criar a instância de banco de dados Amazon RDS for Oracle.	
Conecte-se ao Amazon RDS e conceda privilégios ao usuário Oracle.	Modifique o grupo de segurança para abrir as portas apropriadas para se conectar a partir da máquina local e da instância de replicação do AWS DMS. Ao configurar a conectividade, certifique-se de que a opção “Acessível ao público” esteja seleciona da para que você possa se conectar ao banco de dados fora da VPC. Conecte-se ao Amazon RDS com o Oracle SQL Developer ou o SQL *Plus usando as credencia is de login, crie um usuário do AWS DMS e forneça os privilégios necessários ao usuário do AWS DMS para modificar o banco de dados.	Desenvolvedor

Configurar o grupo de segurança da EC2 instância de origem

Tarefa	Descrição	Habilidades necessárias
Verifique se o banco de dados Oracle está funcionando.	Use o Secure Shell (SSH) para se conectar à EC2 instância e tente se conectar ao banco de dados Oracle usando o SQL *Plus.	Desenvolvedor
Modificação do grupo de segurança.	Modifique o grupo de segurança da EC2 instância para abrir as portas apropriadas, para que você possa se conectar a partir da sua máquina local e da instância de replicação do AWS DMS.	Desenvolvedor

Configurar o AWS DMS

Tarefa	Descrição	Habilidades necessárias
Criar uma instância de replicação do AWS DMS.	No AWS DMS, crie uma instância de replicação na mesma VPC da sua instância de banco de dados Amazon RDS para Oracle. Especifique o nome e a descrição da instância de replicação, escolha a classe da instância e a versão do mecanismo de replicação (use o padrão), escolha a VPC na qual você criou a instância de banco de dados Amazon RDS, defina configurações Multi-	DBA

Tarefa	Descrição	Habilidades necessárias
	AZ, se necessário, aloque armazenamento, especifique a zona de disponibilidade e defina configurações adicionais. Como alternativa, você pode usar o CloudFormation modelo da AWS (DMS.yaml) no anexo para implementar essa etapa.	
Conecte-se aos endpoints dos bancos de dados de origem e de destino.	Crie os endpoints do banco de dados de origem e de destino especificando o identificador do endpoint, o mecanismo, o servidor, a porta, as credenciais de login e os atributos extras de conexão. Para o servidor de origem, use o DNS público da EC2 instância que está hospedando o banco de dados Oracle. Para o servidor de destino, use o endpoint do Amazon RDS para Oracle. Execute um teste para verificar se as conexões de origem e destino estão funcionando. Como alternativa, você pode usar o CloudFormation modelo da AWS (DMS.yaml) no anexo para implementar essa etapa.	DBA

Tarefa	Descrição	Habilidades necessárias
Crie uma tarefa do AWS DMS.	Crie uma tarefa do AWS DMS para migrar dados do endpoint de origem para o endpoint de destino, para configurar a replicação entre o endpoint de origem e de destino, ou ambos. Ao criar a tarefa do AWS DMS, especifiq ue a instância de replicaçã o, o endpoint de origem, o endpoint de destino, o tipo de migração (somente dados, somente replicação ou ambos), o mapeamento da tabela e o filtro. Execute a tarefa do AWS DMS, monitore a tarefa, verifique as estatísticas da tabela e verifique os registros na Amazon CloudWatch. Como alternativa, você pode usar o CloudFormation modelo da AWS (DMS.yaml) no anexo para implementar essa etapa.	DBA

Recursos relacionados

- Criação de uma instância de banco de dados do Amazon RDS
- Conectar-se a uma instância de banco de dados executando o mecanismo de banco de dados Oracle
- Documentação do AWS DMS
- Instruções passo a passo do AWS DMS Step-by-Step
- Migrar bancos de dados Oracle para a Nuvem AWS

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre um banco de dados Oracle local para o Amazon OpenSearch Service usando o Logstash

Criado por Aditya Goteti (AWS)

Resumo

Esse padrão descreve como mover dados de um banco de dados Oracle local para o Amazon OpenSearch Service usando o Logstash. Ele inclui considerações arquitetônicas e alguns conjuntos de habilidades e recomendações necessários. Os dados podem ser de uma única tabela ou de várias tabelas nas quais uma pesquisa de texto completo precisará ser realizada.

OpenSearch O serviço pode ser configurado em uma nuvem privada virtual (VPC) ou pode ser colocado publicamente com restrições baseadas em IP. Esse padrão descreve um cenário em que o OpenSearch serviço é configurado em uma VPC. O Logstash é usado para coletar os dados do banco de dados Oracle, analisá-los no formato JSON e, em seguida, alimentar os dados no Service. OpenSearch

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Java 8 (exigido pelo Logstash 6.4.3)
- Conectividade entre os servidores de banco de dados locais e as instâncias do Amazon Elastic Compute Cloud EC2 (Amazon) em uma VPC, estabelecida usando a Rede Privada Virtual da AWS (AWS VPN)
- Uma consulta para recuperar os dados necessários para serem enviados ao OpenSearch Serviço a partir do banco de dados
- Drivers do Java Database Connectivity (JDBC) da Oracle

Limitações

- O Logstash não consegue identificar registros que foram excluídos permanentemente do banco de dados

Versões do produto

- Banco de Dados Oracle 12c
- OpenSearch Serviço 6.3
- Logstash 6.4.3

Arquitetura

Pilha de tecnologia de origem

- Banco de dados on-premises da Oracle
- VPN AWS on-premises

Pilha de tecnologias de destino

- VPC
- EC2 instância
- OpenSearch Serviço
- Logstash
- NAT Gateway (para atualizações do sistema operacional em EC2 instâncias e para instalar Java 8, Logstash e plug-ins)

Arquitetura de migração de dados

Ferramentas

- Logstash 6.4.3
- Plugin de entrada JDBC (download e mais informações)
- Plugin de saída do Logstash (logstash-output-amazon_es)
- Driver JDBC da Oracle

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Identifique o tamanho do banco de dados de origem	O tamanho dos dados de origem é um dos parâmetros que você usa para determina r o número de fragmentos a serem configurados em um índice.	DBA, desenvolvedor do banco de dados
Analise os tipos de dados de cada coluna e os dados correspondentes.	OpenSearch O serviço mapeia dinamicamente o tipo de dados quando um campo inédito é encontrado no documento. Se houver algum tipo ou formato de dados específico (por exemplo, campos de data) que precise ser declarado explicitamente, identifique os campos e defina o mapeamento desses campos durante a criação do índice.	Proprietário do aplicativo, desenvolvedor, desenvolvedor de banco de dados
Determine se há alguma coluna com chaves primárias ou exclusivas.	Para evitar a duplicação de registros no Amazon OpenSearch Service durante atualizações ou inserções , você precisa `document_ id` definir a configura ção na seção de saída do `amazon_es` plug-in (por exemplo, `document_id => "%{customer_id}"` onde	Proprietário do aplicativo, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`customer_id` está uma chave primária).	
Analise o número e a frequência dos novos registros adicionados; verifique com que frequência os registros são excluídos.	Essa tarefa é necessária para entender a taxa de crescimento dos dados de origem. Se os dados forem lidos intensivamente e as inserções forem raras, você poderá ter um único índice. Se novos registros forem inseridos com frequência e não houver exclusões, o tamanho do fragmento pode facilmente exceder o tamanho máximo recomendado de 50 GB. Nesse caso, você pode criar dinamicamente um índice configurando padrões de índice no Logstash e no código em que você pode acessá-lo usando um alias.	Proprietário do aplicativo, desenvolvedor
Determine quantas réplicas são necessárias.		Proprietário do aplicativo, desenvolvedor
Determine o número de fragmentos a serem configura dos no índice.		Proprietário do aplicativo, desenvolvedor
Identifique os tipos de instância para nós mestres dedicados, nós de dados e a EC2 instância.	Para obter mais informações, consulte a seção Recursos relacionados.	Proprietário do aplicativo, desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Determine o número de nós principais dedicados e nós de dados necessários.	Para obter mais informações, consulte a seção Recursos relacionados.	

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Execute uma EC2 instância.	Execute uma EC2 instância dentro da VPC à qual o AWS VPN está conectado.	Construções do Amazon VPC, AWS VPN
Instale o Logstash na EC2 instância.		Desenvolvedor
Instale os plug-ins do Logstash.	Instale os plug-ins necessários do Logstash `jdbc-input` e `logstash-output-amazon_es` .	Desenvolvedor
Configure o Logstash.	Crie o armazenamento de chaves do Logstash para armazenar informações confidenciais, como chaves do AWS Secrets Manager e credenciais do banco de dados, e depois coloque as referências em um arquivo de configuração do Logstash.	Desenvolvedor
Configure fila de mensagens não entregues e a fila persistente.	Por padrão, quando o Logstash encontra um evento que não pode ser processado porque os dados contêm um erro de mapeamento ou algum	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	outro problema, o pipeline do Logstash trava ou descarta o evento malsucedido. Para se proteger contra perda de dados nessa situação, você pode configurar o Logstash para gravar eventos malsucedidos em uma fila de mensagens não entregues em vez de descartá-los. Para se proteger contra perda de dados durante o encerrame nto anormal, o Logstash tem um atributo de fila persisten te que armazenará a fila de mensagens no disco. As filas persistentes fornecem a durabilidade dos dados no Logstash.	
Crie o domínio do Amazon OpenSearch Service.	Crie o domínio do Amazon OpenSearch Service com uma política de acesso que não exija a assinatur a de solicitações com as credenciais do AWS Identity and Access Management (IAM). O domínio do Amazon OpenSearch Service deve ser criado dentro da mesma VPC. Você também deve seleciona r os tipos de instância e definir o número de nós principais e dedicados com base na sua análise.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Configure os registros necessários OpenSearch do Amazon Service.	Para obter mais informações, consulte a documentação do OpenSearch serviço.	
Crie o índice.		Desenvolvedor
Inicie o Logstash.	Execute o Logstash como um serviço em segundo plano. O Logstash executa a consulta SQL configurada, extrai os dados, os converte no formato JSON e os envia para o Service. OpenSearch Para o carregamento inicial, não configure o agendador no arquivo de configuração do Logstash.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Verifique os documentos.	Verifique o número de documentos no índice e se todos os documentos estão presentes no banco de dados de origem. Durante o carregamento inicial, eles são adicionados ao índice e usados para interromper o Logstash. Altere a configuração do Logstash para adicionar um agendador que seja executado em um intervalo fixo, dependendo dos requisitos do cliente, e reinicie o Logstash. O Logstash selecionará somente os registros que foram atualizados ou adicionados após a última execução, e a data e hora da última execução será armazenada no arquivo configurado com a propriedade de `last_run_metadata_path => “/usr/share/logstash/.logstash_jdbc_last_run”` no arquivo de configuração do Logstash.	Desenvolvedor

Recursos relacionados

- CloudWatch Alarmes recomendados

- Amazon OpenSearch Service Master Nodes dedicados
- Dimensionamento de domínios de OpenSearch serviços da Amazon
- Logstash documentation (Documentação do Logstash)
- Plugin de entrada JDBC
- Plugin de saída do Logstash
- Site da Amazon OpenSearch Service

Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle

Criado por Baji Shaik (AWS) e Pavan Pusuluri (AWS)

Resumo

Esse padrão descreve as etapas para migrar bancos de dados Oracle on-premises para um Amazon Relational Database Service (Amazon RDS) para Oracle. Como parte do processo de migração, você cria um plano de migração e considera fatores importantes sobre sua infraestrutura de banco de dados de destino com base no seu banco de dados de origem. Você pode escolher uma das duas opções de migração com base nos requisitos comerciais e no caso de uso:

- AWS Database Migration Service (AWS DMS): você pode usar o AWS DMS para migrar bancos de dados para a Nuvem AWS de forma rápida e segura. Seu banco de dados de origem permanece totalmente operacional durante a migração, o que minimiza o tempo de inatividade de aplicativos que dependem dele. Você pode reduzir o tempo de migração usando o AWS DMS para criar uma tarefa que captura as mudanças em andamento após a conclusão de uma migração inicial de carga completa por meio de um processo chamado captura de dados de alteração (change data capture, CDC).
- Ferramentas nativas da Oracle — Você pode migrar bancos de dados usando ferramentas nativas da Oracle, como Oracle e Data Pump Export e Data Pump Import com Oracle GoldenGate para CDC. Você também pode usar ferramentas nativas da Oracle, como o Export utility original e o Import utility original para reduzir o tempo de carregamento total.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados Oracle on-premises
- Uma instância de banco de dados Oracle do Amazon RDS

Limitações

- Limite de tamanho do banco de dados: 64 TB

Versões do produto

- Versões do Oracle 11g (versões 11.2.0.3.v1 e mais recentes) até 12.2 e 18c. Para obter uma lista de versionamentos e edições compatíveis, consulte Amazon RDS para Oracle na documentação da AWS. Para obter a lista mais recente de versões Oracle compatíveis com AWS DMS, consulte Uso de um banco de dados Oracle como origem para o AWS DMS na documentação da AWS.

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Oracle on-premises.

Pilha de tecnologias de destino

- Amazon RDS para Oracle

Arquitetura de origem e destino

O diagrama a seguir mostra como migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o AWS DMS.

O diagrama mostra o seguinte fluxo de trabalho:

1. Crie ou use um usuário de banco de dados existente, conceda as permissões do AWS DMS necessárias a esse usuário, ative o modo ARCHIVELOG e, em seguida, configure o registro suplementar.
2. Configure o gateway da Internet entre a rede on-premises e a rede da AWS.
3. Configure endpoints de origem e destino para o AWS DMS.
4. Configure as tarefas de replicação do AWS DMS para migrar os dados do banco de dados de origem para o banco de dados de destino.
5. Conclua as atividades de pós-migração no banco de dados de destino.

O diagrama a seguir mostra como migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando ferramentas Oracle nativas.

O diagrama mostra o seguinte fluxo de trabalho:

1. Crie ou use um usuário de banco de dados existente e conceda as permissões necessárias para fazer backup do banco de dados Oracle usando os utilitários Oracle Export (`exp`) e Import (`imp`).
2. Configure o gateway da Internet entre a rede on-premises e a rede da AWS.
3. Configure o cliente Oracle no Bastion host para usar o banco de dados de backup.
4. Faça upload do backup do banco de dados para um bucket do Amazon Simple Storage Service (Amazon S3)
5. Restaure o backup do banco de dados do Amazon S3 para um banco de dados do Amazon RDS para Oracle.
6. Configure o Oracle GoldenGate para CDC.
7. Conclua as atividades de pós-migração no banco de dados de destino.

Ferramentas

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a Nuvem AWS ou entre combinações de configurações na nuvem e on-premises.
- As ferramentas nativas da Oracle ajudam você a realizar uma migração homogênea. Você pode usar o Oracle Data Pump para migrar dados entre seus bancos de dados de origem e de destino. Esse padrão usa o Oracle Data Pump para realizar a carga completa do banco de dados de origem para o banco de dados de destino.
- GoldenGateA Oracle ajuda você a realizar a replicação lógica entre dois ou mais bancos de dados. Esse padrão é usado GoldenGate para replicar as alterações delta após o carregamento inicial usando o Oracle Data Pump.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Crie documentos do projeto e registre os detalhes do banco de dados.	1. Documente suas metas de migração, requisitos de migração, principais partes interessadas do projeto, marcos do projeto, prazos do projeto,	DBA

Tarefa	Descrição	Habilidades necessárias
	principais métricas, riscos de migração e planos de mitigação de riscos. 2. Documente informações críticas sobre seu banco de dados de origem, incluindo RAM, IOPS e. CPUs Posteriormente, você usará essas informações para determinar a instância de banco de dados de destino apropriada. 3. Valide as versões dos bancos de dados de origem e de destino.	

Tarefa	Descrição	Habilidades necessárias
Identifique os requisitos de armazenamento.	Identifique e documente seus requisitos de armazenamento, incluindo o seguinte: 1. Calcular o armazenamento alocado para a instância do banco de dados de origem. 2. Reunir as métricas históricas de crescimento da instância do banco de dados de origem. 3. Prever o crescimento futuro para a instância de banco de dados de destino. **Note** Para volumes SSD de uso geral (gp2), você obtém três IOPS por 1 GB de armazenamento. Aloque o armazenamento calculando o número total de IOPS de leitura e gravação no banco de dados de origem.	DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
Escolha o tipo de instância adequado com base nos requisitos de computação.	1. Determine os requisitos de computação da instância do banco de dados de destino. 2. Identifique problemas de desempenho. 3. Considere os seguintes fatores para determinar o tipo de instância apropriad o: • Utilização da CPU da instância do banco de dados de origem • IOPS (operações de leitura e gravação) para a instância do banco de dados de origem • Espaço de memória na instância do banco de dados de origem	SysAdmin
Identifique os requisitos de segurança de acesso à rede.	1. Identifique e documente os requisitos de segurança de acesso à rede para os bancos de dados de origem e de destino. 2. Configure os grupos de segurança apropriados para permitir que o aplicativo se comunique com o banco de dados.	DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
Identifique a estratégia de migração de aplicativos.	1. Determine e documente a estratégia de substituição da migração. 2. Determine e documente o objetivo de tempo de recuperação (RTO) e o objetivo de ponto de recuperação (RPO) do seu aplicativo e, em seguida, planeje a transição adequadamente.	DBA SysAdmin, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Identifique os riscos da migração.	Avalie os riscos e mitigações específicos da migração de documentos e bancos de dados. Por exemplo: • Identifique tabelas sem registro e destaque o risco de perda de dados em caso de recuperação. • Extraia os usuários e privilégios do banco de dados de origem e destaque os conflitos com os privilégios do Amazon RDS. • Revise o registro de alertas para ver se há erros e avisos específicos do Oracle. • Identifique os atributos compatíveis e não compatíveis da instância de banco de dados de destino. • Analise os atributos obsoletos do mecanismo de versão do banco de dados de destino.	DBA

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	Crie uma nova Amazon Virtual Private Cloud (Amazon VPC)	SysAdmin

Tarefa	Descrição	Habilidades necessárias
	para a instância do banco de dados de destino.	
Criar grupos de segurança.	Crie um grupo de segurança em sua nova VPC para permitir conexões de entrada com a instância de banco de dados.	SysAdmin
Crie uma instância de banco de dados do Amazon RDS para Oracle.	Crie a instância de banco de dados de destino com a nova VPC e o grupo de segurança e, em seguida, inicie a instância.	SysAdmin

Opção 1 - Use ferramentas nativas da Oracle ou de terceiros para migrar dados

Tarefa	Descrição	Habilidades necessárias
Prepare o banco de dados de origem.	1. Crie um diretório Data Pump ou use um existente. 2. Crie um usuário de migração e conceda permissões para realizar a extração do Data Pump. 3. Extraia perfis, usuários e espaços de tabela do banco de dados de origem como um script SQL. 4. Transfira o dump extraído do Data Pump para o diretório da instância `data pump` de banco de dados de destino.	DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
Preparar o banco de dados de destino.	1. Confirme se todas as opções de banco de dados (por exemplo, text e Java) estão instaladas ou habilitadas na instância de banco de dados Amazon RDS para Oracle de destino. 2. Crie um diretório Data Pump ou use um existente. 3. Crie um usuário de migração e conceda permissões para realizar a importação do Data Pump. 4. Crie os espaços de tabela, os usuários e os perfis necessários na instância de banco de dados de destino. 5. Importe o despejo de exportação do Data Pump transferido para o banco de dados de destino. 6. Crie todos os índices excluídos durante a importação ou a criação do objeto. 7. Crie quaisquer restriçõe s excluídas durante a importação. 8. Valide ou recompile objetos inválidos. 9. Recompile os índices inválidos.	DBA, SysAdmin

Tarefa	Descrição	Habilidades necessárias
	10. Valide as contagens de objetos do banco de dados entre os bancos de dados de origem e de destino. 11. Solucione todas as discrepâncias encontradas entre as contagens de objetos.	

Opção 2 - Use o AWS DMS para migrar dados

Tarefa	Descrição	Habilidades necessárias
Preparar os dados.	1. Limpe os dados no banco de dados de origem. 2. Crie de uma instância de replicação. 3. Crie um endpoint de origem e um endpoint de destino. 4. Identifique o número de tabelas e objetos a serem migrados.	DBA
Migre os dados.	1. Elimine restrições de chave externa e triggers no banco de dados de destino. 2. Elimine índices secundários no banco de dados de destino. 3. Defina as configurações de tarefas de carga total do AWS DMS do banco de	DBA

Tarefa	Descrição	Habilidades necessárias
	dados de origem para o banco de dados de destino. 4. Habilite chaves externas. 5. Permita que o AWS DMS CDC replique as mudanças em andamento. 6. Habilite triggers. 7. Atualize as sequências. 8. Valide os dados de origem e de destino.	

Vá para o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.	1. Interrompa todos os serviços de aplicativos e conexões de clientes que apontam para a Oracle. 2. Execute as tarefas do AWS DMS. 3. Configure uma tarefa de reversão (por exemplo, reverta o CDC do banco de dados Amazon RDS para o banco de dados Oracle on-premises). 4. Valide os dados. 5. Inicie os serviços do aplicativo no novo banco de dados de destino configura ndo o Amazon Route 53	DBA SysAdmin, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	para a nova instância de banco de dados Amazon RDS para Oracle. 6. Adicione o CloudWatch monitoramento da Amazon à sua nova instância de banco de dados Amazon RDS for Oracle.	
Implemente seu plano de reversão.	1. Interrompa todos os serviços de aplicativos que apontam para a instância de banco de dados do Amazon RDS para Oracle. 2. Reverta as alterações no banco de dados Oracle on-premises de origem usando uma tarefa do AWS DMS. 3. Interrompa a execução das tarefas do AWS DMS do banco de dados Oracle on-premises para o banco de dados Amazon RDS para Oracle. 4. Configure os aplicativos de volta no banco de dados Oracle de origem. 5. Confirme se a implantação de reversão foi concluída.	DBA, proprietário do aplicativo

Encerre o projeto de migração

Tarefa	Descrição	Habilidades necessárias
Limpar os recursos	Encerre ou remova os recursos temporários da AWS, como a instância de replicaçã o do AWS DMS e o bucket S3.	DBA, SysAdmin
Revise os documentos do projeto.	Revise seus documentos e metas de planejamento de migração e confirme se você concluiu todas as etapas de migração necessárias.	DBA SysAdmin, proprietário do aplicativo
Colete métricas.	Registre as principais métricas de migração, incluindo o tempo necessário para concluir a migração, a porcentagem de tarefas manuais versus tarefas baseadas em ferramentas, economia de custos e outras métricas relevantes.	DBA SysAdmin, proprietário do aplicativo
Encerre o projeto.	Encerre o projeto de migração e obtenha feedback sobre o empenho.	DBA SysAdmin, proprietário do aplicativo

Recursos relacionados

Referências

- Migração de bancos de dados Oracle para a nuvem da AWS (AWS Prescriptive Guidance)
- AWS Database Migration Service (documentação do AWS DMS)
- Preços do Amazon RDS (documentação do Amazon RDS)

Tutoriais e vídeos

- Introdução ao AWS Database Migration Service (documentação do AWS DMS)
- Amazon RDS resources (documentação do Amazon RDS)
- AWS Database Migration Service (DMS) (YouTube)

Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump

Criado por Mohan Annam (AWS) e Brian motzer (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados Oracle de um datacenter on-premises para um Amazon Relational Database Service (Amazon RDS) para instância de banco de dados Oracle usando o Oracle Data Pump.

O padrão envolve criar um arquivo de despejo de dados do banco de dados de origem, armazenar o arquivo em um bucket do Amazon Simple Storage Service (Amazon S3) e restaurar os dados em uma instância de banco de dados do Amazon RDS para Oracle. Esse padrão é útil quando você encontra limitações ao usar o AWS Database Migration Service (AWS DMS) para a migração.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- As permissões necessárias para criar perfis no AWS Identity and Access Management (IAM) e para um upload de várias partes do Amazon S3
- As permissões necessárias para exportar dados do banco de dados de origem
- AWS Command Line Interface (AWS CLI), instalado e configurado

Versões do produto

- O Oracle Data Pump está disponível somente para o banco de dados Oracle 10g Release 1 (10.1) e versões posteriores.

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Oracle on-premises.

Pilha de tecnologias de destino

- Amazon RDS para Oracle
- Cliente SQL (desenvolvedor Oracle SQL)
- Um bucket do S3

Arquitetura de origem e destino

Ferramentas

Serviços da AWS

- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los. Nesse padrão, o IAM é usado para criar os perfis e as políticas necessárias para migrar dados do Amazon S3 para o Amazon RDS para Oracle.
- O Amazon Relational Database Service (Amazon RDS) para Oracle ajuda você a configurar, operar e escalar um banco de dados relacional Oracle na Nuvem AWS.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- O Oracle Data Pump ajuda você a mover dados e metadados de um banco de dados para outro em alta velocidade. Nesse padrão, o Oracle Data Pump é usado para exportar o arquivo de despejo de dados (.dmp) para o servidor Oracle e importá-lo para o Amazon RDS para Oracle. Para obter mais informações, consulte Como importar dados no Amazon RDS na documentação do Amazon RDS.
- O Oracle SQL Developer é um ambiente de desenvolvimento integrado que simplifica o desenvolvimento e o gerenciamento de bancos de dados Oracle em implantações tradicionais e baseadas em nuvem. Ele interage com o banco de dados Oracle on-premises e com o Amazon RDS para Oracle para executar os comandos SQL necessários para exportar e importar dados.

Épicos

Criar um bucket do S3.

Tarefa	Descrição	Habilidades necessárias
Crie o bucket.	Para criar um bucket do S3, siga as instruções na documentação da AWS.	Administrador de sistemas AWS

Criar o perfil do IAM e atribuir políticas

Tarefa	Descrição	Habilidades necessárias
Configurar permissões do IAM	Para configurar as permissões, siga as instruções na documentação da AWS.	Administrador de sistemas AWS

Criar a instância de destino do banco de dados do Amazon RDS para Oracle e associar o perfil de integração do Amazon S3

Tarefa	Descrição	Habilidades necessárias
Crie a instância de destino do banco de dados do Amazon RDS para Oracle.	Para criar a instância do Amazon RDS para Oracle, siga as instruções na documentação da AWS.	Administrador de sistemas AWS
Associe o perfil à instância de banco de dados.	Para associar o perfil à instância, siga as instruções na documentação da AWS.	DBA

Criar o usuário do banco de dados no banco de dados de destino

Tarefa	Descrição	Habilidades necessárias

Crie o usuário.	Conecte-se ao banco de dados Amazon RDS para Oracle de destino a partir do Oracle SQL Developer ou SQL*Plus e execute o seguinte comando SQL para criar o usuário para o qual importar o esquema.
	`create user SAMPLE_SCHEMA identified by <PASSWORD>;`
	`grant create session, resource to <USER NAME>;`
	`alter user <USER NAME> quota 100M on users;`
		DBA

Criar o arquivo de exportação do banco de dados Oracle de origem

Tarefa	Descrição	Habilidades necessárias

Criar um arquivo de despejo de dados.	Para criar um arquivo de despejo nomeado `sample.dmp` no diretório `DATA_PUMP_DIR` para exportar o usuário `SAMPLE_SCHEMA`, use o script a seguir.
	`DECLARE`
	`  hdnl NUMBER;`
	`BEGIN`
		DBA

Tarefa	Descrição	Habilidades necessárias

	<pre> hdnl := dbms_data
	pump.open(operation
	 => 'EXPORT',
	
	          job_mode =>
	 'SCHEMA',
	
	          job_name =>
	 NULL);
	
	    dbms_datapump.add_
	file(handle => hdnl,
	
	         filename =>
	 'sample.dmp',
	
	       directory =>
	 'DATA_PUMP_DIR',
	
	         filetype =>
	 dbms_datapump.ku$_
	file_type_dump_file);
	
	    dbms_datapump.add_
	file(handle => hdnl,
	
	         filename =>
	 'export.log',
	
	       directory =>
	 'DATA_PUMP_DIR',
	
	         filetype =>
	 dbms_datapump.ku$_
	file_type_log_file);
	
	    dbms_datapump.meta
	data_filter(hdnl,
	 'SCHEMA_EXPR', 'IN
	 (''SAMPLE_SCHEMA''
	)');</pre>	

Tarefa	Descrição	Habilidades necessárias

	`dbms_datapump.start_job(hdnl);`
	`END;`
	`/`
	
	Revise os detalhes da exportação revisando o arquivo `export.log` em seu diretório local `DATA_PUMP_DIR` .	

Faça upload do arquivo de despejo no bucket do S3.

Tarefa	Descrição	Habilidades necessárias
Carregue o arquivo de despejo de dados da origem para o bucket do S3.	Quando usar a AWS CLI, execute o comando a seguir. `aws s3 cp sample.dmp s3://<bucket_created_epic_1>/`	DBA

Baixe o arquivo de exportação do bucket do S3 para a instância do RDS

Tarefa	Descrição	Habilidades necessárias
Baixe o arquivo de despejo de dados para o Amazon RDS	Para copiar o arquivo de despejo `sample.dmp` do bucket do S3 no banco de dados do Amazon RDS para Oracle, execute o seguinte comando SQL. Neste exemplo, o arquivo `sample.dmp` é baixado	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	do bucket do S3 `my-s3-integration1` para o diretório Oracle `DATA_PUMP_DIR`. Verifique se você tem espaço em disco suficiente alocado para sua instância do RDS para acomodar o banco de dados e o arquivo de exportação.
	
	`-- If you want to download all the files in the S3 bucket remove the p_s3_prefix line.`
	
	`SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3( p_bucket_name => 'my-s3-integration', p_s3_prefix => 'sample.dmp', p_directory_name => 'DATA_PUMP_DIR') AS TASK_ID FROM DUAL;`
	
	O comando anterior gera um ID da tarefa. Para revisar o status do download analisando os dados no ID da tarefa, execute o comando a seguir.
	
	`SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','d`	

Tarefa	Descrição	Habilidades necessárias

	`btask-<task_id>.log'));`
	
	Para ver os arquivos no diretório `DATA_PUMP_DIR` , execute o seguinte comando.
	
	`SELECT filename, type,filesize/1024 /1024 size_megs ,to_char(mtime,'DD -MON-YY HH24:MI:SS') timestamp FROM TABLE(rdsadmin.rds_file_util.listdir (p_directory => upper('DATA_PUMP_DIR'))) order by 4;`	

Importe o arquivo de despejo para o banco de dados de destino.

Tarefa	Descrição	Habilidades necessárias
Restaure o esquema e os dados no Amazon RDS.	Para importar o arquivo de despejo para o esquema do banco de dados `sample_schema` , execute o seguinte comando SQL do SQL Developer ou do SQL*Plus. `DECLARE hdnl NUMBER; BEGIN hdnl := DBMS_DATAPUMP.OPEN( operation`	DBA

Tarefa	Descrição	Habilidades necessárias
	=> 'IMPORT', job_mode => 'SCHEMA', job_name=>null); DBMS_DATAPUMP.ADD_FILE(handle => hdnl, filename => 'sample.dmp', directory => 'DATA_PUMP_DIR', filetype => dbms_datapump.ku$_file_type_dump_file); DBMS_DATAPUMP.ADD_FILE(handle => hdnl, filename => 'import.log', directory => 'DATA_PUMP_DIR', filetype => dbms_datapump.ku$_file_type_log_file); DBMS_DATAPUMP.METADATA_FILTER(hdnl,'SCHEMA_EXPR','IN (''SAMPLE_SCHEMA'')'); DBMS_DATAPUMP.START_JOB(hdnl); END; / Para ver o arquivo de log da importação, execute o comando a seguir. SELECT text FROM table(rdsadmin.rds_file_util.read_te	

Tarefa	Descrição	Habilidades necessárias
	xt_file('DATA_PUMP _DIR','import.log'));	

Remova o arquivo de despejo do diretório DATA_PUMP_DIR

Tarefa	Descrição	Habilidades necessárias

Listar e limpar os arquivos de exportação.	Para listar e remover os arquivos de exportação no diretório `DATA_PUMP_DIR` , execute os comandos a seguir.
	`-- List the files SELECT filename, type,filesize/1024 /1024 size_megs ,to_char(mtime,'DD -MON-YY HH24:MI:S S') timestamp FROM TABLE(rdsadmin.rds _file_util.listdir (p_directory => upper('DATA_PUMP_D IR'))) order by 4;`
	`-- Remove the files EXEC UTL_FILE. FREMOVE('DATA_PUMP _DIR','sample.dmp'); EXEC UTL_FILE.FREMOVE(' DATA_PUMP_DIR','im port.log');`
		Administrador de sistemas AWS

Recursos relacionados

- Integração do Amazon S3
- Criar uma instância de banco de dados
- Importar dados para o Oracle no Amazon RDS
- Documentação do Amazon S3
- Documentação do IAM
- Documentação do Amazon RDS
- Documentação do Oracle Data Pump
- Oracle SQL Developer

Migre do PostgreSQL na Amazon para o EC2 Amazon RDS for PostgreSQL usando pglogical

Criado por Rajesh Madiwale (AWS)

Resumo

Esse padrão descreve as etapas para migrar um banco de dados PostgreSQL (versão 9.5 e posterior) do Amazon Elastic Compute Cloud (Amazon) para o Amazon EC2 Relational Database Service (Amazon RDS) para PostgreSQL usando a extensão pglógica do PostgreSQL. O Amazon RDS agora tem suporte para a extensão pglogical nas versões 10 e posteriores do PostgreSQL.

Pré-requisitos e limitações

Pré-requisitos

- Escolher o tipo certo de instância do Amazon RDS. Para obter mais informações, consulte Tipos de instância do Amazon RDS.
- Certifique-se de que as versões de origem e destino do PostgreSQL sejam as mesmas.
- Instale e integre a extensão pglogical com o PostgreSQL na Amazon. EC2

Versões do produto

- PostgreSQL versão 10 e posterior no Amazon RDS, com os recursos suportados no Amazon RDS (consulte PostgreSQL no Amazon RDS na documentação da AWS). Esse padrão foi testado com a migração do PostgreSQL 9.5 para o PostgreSQL versão 10 no Amazon RDS, mas também se aplica às versões posteriores do PostgreSQL no Amazon RDS.

Arquitetura

Arquitetura de migração de dados

Ferramentas

- Extensão pglogical
- Utilitários nativos do PostgreSQL: pg_dump e pg_restore

Épicos

Migrar dados usando a extensão pglogical

Tarefa	Descrição	Habilidades necessárias
Criar uma instância de banco de dados do Amazon RDS PostgreSQL	Atualizar uma instância de banco de dados PostgreSQL no Amazon RDS. Para obter instruções, consulte a documentação do Amazon RDS para PostgreSQL.	DBA
Obter um despejo de esquema do banco de dados PostgreSQL de origem e restaurar no banco de dados PostgreSQL de destino.	1. Use o utilitário pg_dump com a opção `-s` de gerar um arquivo de esquema do banco de dados de origem. 2. Use o utilitário psql com a opção `-f` de carregar o esquema no banco de dados de destino.	DBA
Habilitar decodificação lógica.	No grupo de parâmetros de banco de dados do Amazon RDS, defina o parâmetro estático `rds.logical_replication` como 1. Para obter instruções, consulte a documentação do Amazon RDS.	DBA
Criar a extensão pglogical nos bancos de dados de origem e de destino.	1. Criar a extensão `pglogical` no banco de dados PostgreSQL de origem: `psql -h <amazon-ec2-endpoint> -d target-`	DBA

Tarefa	Descrição	Habilidades necessárias
	dbname -U target-dbuser -c "create extension pglogical ;" 2. Criar a extensão `pglogical` no banco de dados PostgreSQL de destino: `psql -h <amazon-rds-endpoint> -d source-dbname -U source-dbuser -c "create extension pglogical ;"`	
Criar um publicador no banco de dados PostgreSQL de origem.	Para criar um publicador, execute: `psql -d dbname -p 5432 <<EOF SELECT pglogical .create_node( node_name := 'provider1', dsn := 'host=<ec2-endpoint> port=5432 dbname=source-dbname user=source-dbuser' ); EOF`	DBA

Tarefa	Descrição	Habilidades necessárias

Criar um conjunto de replicação, adicionar tabelas e sequências.	Para criar um conjunto de replicação no banco de dados PostgreSQL de origem e adicionar tabelas e sequências ao conjunto de replicação, execute:
	`psql -d dbname -p 5432 <<EOF`
	`SELECT pglogical.replication_set_add_all_tables('default', '{public}'::text[],synchronize_data := true);`
	`EOF`
		DBA

Criar um assinante.	Para criar um assinante no banco de dados PostgreSQL de destino, execute:
	`psql -h <rds-endpoint> -d target-dbname -U target-dbuser <<EOF`
	`SELECT pglogical.create_node(`
	`node_name := 'subscriber1',`
	`dsn := 'host=<rds-endpoint> port=5432 dbname=target-dbname password=postgres user=target-dbuser'`
	`);`
	`EOF`
		DBA

Tarefa	Descrição	Habilidades necessárias
Criar uma assinatura.	Para criar uma assinatura no banco de dados PostgreSQL de destino, execute: `psql -h <rds-endpoint> -d target -U postgres <<EOF SELECT pglogical .create_subscription( subscription_name := 'subscription1', replication_sets := array['default'], provider_dsn := 'host=<ec2-endpoint> port=5432 dbname=<source-dbname> password=<password> user=source-dbuser' );`	DBA

Validar os dados

Tarefa	Descrição	Habilidades necessárias
Verificar os bancos de dados de origem e de destino.	Verifique os bancos de dados de origem e destino para confirmar se os dados estão sendo replicados com sucesso. Você pode realizar validação básica usando `select count(1)` da origem e tabelas de destino.	DBA

Recursos relacionados

- Amazon RDS
- Replicação lógica para o PostgreSQL no Amazon RDS (documentação do Amazon RDS)
- pglogical (repositório) GitHub
- Limitações do pglogical (arquivo README GitHub do repositório)
- Migração do PostgreSQL do local ou da Amazon EC2 para o Amazon RDS usando replicação lógica (blog do banco de dados da AWS)

Migrar um banco de dados PostgreSQL on-premises para o Aurora PostgreSQL

Criado por Baji Shaik (AWS) e Jitender Kumar (AWS)

Resumo

O Amazon Aurora Edição Compatível com PostgreSQL combina o desempenho e a disponibilidade dos bancos de dados comerciais de ponta com a simplicidade e a economia dos bancos de dados de código aberto. O Aurora fornece esses benefícios escalando o armazenamento em três zonas de disponibilidade na mesma região da AWS e oferece suporte a até 15 instâncias de réplica de leitura para aumentar a escala horizontalmente de workloads de leitura e fornecer alta disponibilidade em uma única região. Ao usar um banco de dados global Aurora, você pode replicar bancos de dados PostgreSQL em até cinco regiões para acesso remoto de leitura e recuperação de desastres no caso de uma falha na região. Esse padrão descreve as etapas para migrar um banco de dados de origem PostgreSQL on-premises para um banco de dados compatível com o Aurora PostgreSQL. O padrão inclui duas opções de migração: usar o AWS Data Migration Service (AWS DMS) ou usar ferramentas nativas do PostgreSQL (como pg_dump, pg_restore e psql) ou ferramentas de terceiros.

As etapas descritas nesse padrão também se aplicam aos bancos de dados PostgreSQL de destino nas instâncias do Amazon Relational Database Service (Amazon RDS) e do Amazon Elastic Compute Cloud (Amazon). EC2

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem PostgreSQL em um datacenter no on-premise
- Uma instância de banco de dados compatível com o Aurora PostgreSQL ou uma instância de banco de dados Amazon RDS para PostgreSQL

Limitações

- Os limites de tamanho do banco de dados são 64 TB para Amazon RDS para PostgreSQL e 128 TB para Aurora compatível com PostgreSQL.
- Se você estiver usando a opção de migração do AWS DMS, analise as limitações do AWS DMS sobre o uso de um banco de dados PostgreSQL como fonte.

Versões do produto

- Para suporte às versões principal e secundária do PostgreSQL no Amazon RDS, consulte as atualizações do Amazon RDS para PostgreSQL na documentação do Amazon RDS.
- Para suporte ao PostgreSQL no Aurora, consulte as atualizações do Amazon Aurora PostgreSQL na documentação do Aurora.
- Se você estiver usando a opção de migração do AWS DMS, consulte as versões compatíveis do PostgreSQL na documentação do AWS DMS.

Arquitetura

Pilha de tecnologia de origem

- Banco de dados PostgreSQL on-premises

Pilha de tecnologias de destino

- Instância de banco de dados compatível com o Aurora PostgreSQL.

Arquitetura de origem

Arquitetura de destino

Arquitetura de migração de dados

Uso do AWS DMS

Uso de ferramentas nativas do PostgreSQL

Ferramentas

- O AWS Database Migration Service (AWS DMS) ajuda você a migrar armazenamentos de dados para a nuvem AWS ou entre combinações de configurações na nuvem e on-premises. O serviço é compatível com vários bancos de dados de origem e destino diferentes. Para obter informações sobre como validar as versões e edições do banco de dados de origem e destino do PostgreSQL compatíveis para uso com o AWS DMS, consulte Uso de um banco de dados PostgreSQL como

fonte do AWS DMS. Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos.

- As ferramentas nativas do PostgreSQL incluem pg_dump, pg_restore e psql.

Épicos

Analise a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões dos bancos de dados de origem e de destino.	Se você estiver usando o AWS DMS, verifique se está usando uma versão compatível do PostgreSQL.	DBA
Identifique os requisitos para o tipo e a capacidade de armazenamento.	1. Calcule o armazenamento alocado para a instância do banco de dados de origem. 2. Reúna as métricas históricas de crescimento da instância do banco de dados de origem. 3. Antecipe a previsão de crescimento futuro para a instância do banco de dados de destino. 4. Aloque o armazenamento calculando o número total de IOPS de leitura e gravação no banco de dados de origem. Um volume SSD de uso geral (gp2) fornece 3 IOPS para cada 1 GB de armazenamento.	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Escolha o tipo de instância, a capacidade, os atributos de armazenamento e os atributos de rede adequados.	Determine os requisitos de computação da instância do banco de dados de destino. Analise os problemas de desempenho conhecido s que talvez precisem de atenção adicional. Considere os seguintes fatores para determinar o tipo de instância apropriado: • Utilização da CPU da instância do banco de dados de origem • IOPS (operações de leitura e gravação) para a instância do banco de dados de origem • Espaço de memória na instância do banco de dados de origem Para ter mais informações, consulte Classes de instância de banco de dados do Aurora na documentação do Aurora.	DBA, administrador de sistemas
Identifique os requisitos de segurança de acesso à rede para os bancos de dados de origem e de destino.	Determine os grupos de segurança apropriados que permitiriam que o aplicativo se comunicasse com o banco de dados.	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Identifique a estratégia de migração de aplicativos.	• Determine a estratégia de substituição da migração com base na complexidade do seu aplicativo. • Determine o objetivo de tempo de recuperação (RTO) e o objetivo de ponto de recuperação (RPO) para o aplicativo e planeje a substituição de acordo.	DBA, proprietário do aplicativo, administrador de sistemas

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	Crie uma nuvem privada virtual (VPC) para a instância do banco de dados de destino.	Administrador de sistemas
Criar grupos de segurança.	Crie um grupo de segurança dentro da VPC (conforme determinado no épico anterior) para permitir conexões de entrada com a instância do banco de dados.	Administrador de sistemas
Configure e inicie o cluster de banco de dados do Aurora.	Crie a instância do banco de dados de destino com a nova VPC e o grupo de segurança e inicie a instância.	Administrador de sistemas

Migração de dados: opção 1 (usando o AWS DMS)

Tarefa	Descrição	Habilidades necessárias
Conclua as etapas de pré-migração.	1. Limpe os dados no banco de dados de origem. 2. Crie de uma instância de replicação. 3. Criar endpoints de origem e de destino 4. Identifique o número de tabelas e objetos disponíveis a serem migrados.	DBA
Concluir as etapas de migração.	1. Elimine restrições de chave externa e triggers no banco de dados de destino. 2. Elimine índices secundários no banco de dados de destino. 3. Use uma tarefa de carga completa para migrar dados do banco de dados de origem para o de destino. 4. Habilite chaves externas. 5. Se você estiver usando a migração instantânea e seu aplicativo exigir um tempo de inatividade mínimo, habilite a captura de dados de alterações (CDC) para replicar as alterações em andamento 6. Habilite triggers. 7. Atualize as sequências.	DBA

Tarefa	Descrição	Habilidades necessárias
	8. Valide os dados de origem e de destino.	
Valide os dados.	Para garantir que seus dados foram migrados com precisão da origem para o destino, siga as etapas de validação de dados na documentação do AWS DMS.	DBA

Migração de dados: opção 2 (usando pg_dump e pg_restore)

Tarefa	Descrição	Habilidades necessárias
Prepare o banco de dados de origem.	1. Crie um diretório para armazenar o backup do pg_dump se ele ainda não existir. 2. Crie um usuário de migração que tenha permissões para executar pg_dump em objetos de banco de dados. 3. Conecte-se à EC2 instância e execute pg_dump backup. Para obter mais informações, consulte a documentação do pg_dump e o passo a passo na documentação do AWS DMS.	DBA
Preparar o banco de dados de destino.	1. Crie um usuário de migração que tenha	DBA

Tarefa	Descrição	Habilidades necessárias
	permissões para usar pg_restore em objetos de banco de dados. 2. Importe o dump do banco de dados usando pg_restore. Para obter mais informações, consulte a documentação do pg_restore e o passo a passo na documentação do AWS DMS.	
Valide os dados.	1. Compare as contagens de objetos do banco de dados entre os bancos de dados de origem e de destino. 2. Solucione todas as discrepâncias encontradas entre as contagens de objetos.	DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos.	Implemente a estratégia de migração de aplicativos que você criou no primeiro épico.	DBA, proprietário do aplicativo, administrador de sistemas

Vá para o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.	1. Pare todos os serviços de aplicativos e conexões de clientes que apontam para o banco de dados PostgreSQL on-premises. 2. Execute as tarefas do AWS DMS. 3. Configure uma tarefa de reversão (reverta CDC do Aurora PostgreSQL compatível com o banco de dados PostgreSQL on-premise), se necessário. 4. Valide os dados. 5. Inicie os serviços do aplicativo no novo destino configurando o Amazon Route 53 para a nova instância de banco de dados compatível com o Aurora PostgreSQL. 6. Adicione o monitoramento da Amazon CloudWatch e do Performance Insights à sua nova instância de banco de dados compatível com o Aurora PostgreSQL.	DBA, proprietário do aplicativo, administrador de sistemas
Se você precisar reverter a migração.	1. Pare todos os serviços de aplicativos que apontam para o banco de dados	DBA, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	compatível com o Aurora PostgreSQL. 2. Reverta as alterações no banco de dados PostgreSQL on-premises de origem usando a tarefa do AWS DMS que você criou na história anterior. 3. Interrompa a execução das tarefas do AWS DMS do banco de dados PostgreSQL on-premises para o banco de dados compatível com o Aurora PostgreSQL. 4. Configure o aplicativo para que ele aponte de volta para o banco de dados PostgreSQL on-premises de origem. 5. Confirme se toda a implantação de reversão foi concluída.	

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Desligar recursos.	Encerre os recursos temporários da AWS.	DBA, administrador de sistemas
Valide os documentos.	Revise e valide os documentos do projeto.	DBA, proprietário do aplicativo, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Colete métricas.	Reúna métricas sobre a hora de migrar, porcentagem de economia de custos manuais versus ferramentas e assim por diante.	DBA, proprietário do aplicativo, administrador de sistemas
Fechar o projeto.	Feche o projeto e forneça feedback, se houver.	DBA, proprietário do aplicativo, administrador de sistemas

Recursos relacionados

Referências

- AWS Data Migration Service
- VPCs e Amazon Aurora
- Preço do Amazon Aurora
- Uso do banco de dados PostgreSQL como origem para o AWS DMS
- Como criar uma instância de replicação do AWS DMS
- Como criar endpoints de origem e destino usando o AWS DMS

Recursos adicionais

- Conceitos básicos do AWS DMS
- Instruções sobre migração step-by-step de dados
- Recursos do Amazon Aurora

Migre um banco de dados local do Microsoft SQL Server para o Microsoft SQL Server na Amazon executando Linux EC2

Criado por Tirumala Dasari (AWS)

Resumo

Esse padrão descreve como migrar de um banco de dados local do Microsoft SQL Server executado no Microsoft Windows para o Microsoft SQL Server em uma instância Linux do Amazon Elastic Compute Cloud (Amazon EC2) usando utilitários de backup e restauração.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Amazon EC2 Linux AMI (Amazon Machine Image) com Microsoft SQL Server
- AWS Direct Connect entre o Windows local e o Microsoft SQL Server na instância Linux EC2

Arquitetura

Pilha de tecnologia de origem

- Banco de dados Microsoft SQL Server on-premises

Pilha de tecnologias de destino

- EC2 Instância Linux com um banco de dados Microsoft SQL Server

Arquitetura de migração de banco de dados

Ferramentas

- WinSCP - Essa ferramenta permite que os usuários do Windows compartilhem arquivos facilmente com usuários do Linux.
- Sqlcmd - Esse utilitário de linha de comando permite enviar instruções ou lotes de T-SQL para instâncias locais e remotas do SQL Server. O utilitário é extremamente útil para tarefas repetitivas de banco de dados, como processamento em lote ou teste de unidade.

Épicos

Prepare a instância EC2 Linux com o SQL Server

Tarefa	Descrição	Habilidades necessárias
Selecione uma AMI que forneça o sistema operacional Linux e inclua o Microsoft SQL Server.		Sysadmin
Configure a AMI para criar uma EC2 instância.		Sysadmin
Crie regras de entrada e saída para grupos de segurança:		Sysadmin
Configure a EC2 instância Linux para um banco de dados Microsoft SQL Server.		DBA
Crie usuários e forneça permissões como no banco de dados de origem.		Proprietário do aplicativo, DBA
Instale as ferramentas do SQL Server e o utilitário sqlcmd na instância Linux. EC2		DBA

Faça backup do banco de dados e mova o arquivo de backup para a EC2 instância Linux

Tarefa	Descrição	Habilidades necessárias
Faça o backup do banco de dados do SQL Server on-premises.		DBA

Tarefa	Descrição	Habilidades necessárias
Instale o WinSCP no Microsoft SQL Server		DBA
Mova o arquivo de backup para a EC2 instância Linux que executa o Microsoft SQL Server.		DBA

Restaure o banco de dados na EC2 instância Linux executando o SQL Server

Tarefa	Descrição	Habilidades necessárias
Restaure o banco de dados a partir do arquivo de backup do banco de dados usando o utilitário sqlcmd.		DBA
Valide objetos e dados do banco de dados.		Desenvolvedor, engenheiro de testes

Passe do Windows SQL Server para o Windows SQL Server em uma EC2 instância Linux

Tarefa	Descrição	Habilidades necessárias
Valide objetos e dados do banco de dados.		Desenvolvedor, engenheiro de testes
Passe do banco de dados local do Microsoft SQL Server para a EC2 instância Linux que executa o Microsoft SQL Server.		DBA

Recursos relacionados

- Como configurar o SQL Server 2017 no Amazon Linux e no Ubuntu AMIs
- Instalação de ferramentas SQL em uma instância Linux
- Backup e restauração de um banco de dados local do Microsoft SQL Server para o Microsoft SQL Server em uma instância Linux EC2

Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando servidores vinculados

Criado por Kevin Yung (AWS), Vishal Singh (AWS) e Viqash Adwani (AWS)

Resumo

Os servidores vinculados permitem que o Microsoft SQL Server execute instruções SQL em outras instâncias de servidores de banco de dados. Esse padrão descreve como você pode migrar seu banco de dados on-premises do Microsoft SQL Server para o Amazon Relational Database Service (Amazon RDS) para o Microsoft SQL Server a fim de obter menor custo e maior disponibilidade. Atualmente, o Amazon RDS para Microsoft SQL Server não é compatível com conexões fora de uma rede da Amazon Virtual Private Cloud (Amazon VPC).

Você pode usar esse padrão para atingir os seguintes objetivos:

- Migrar o Microsoft SQL Server para o Amazon RDS para Microsoft SQL Server sem interromper os recursos do servidor vinculado.
- Para priorizar e migrar o Microsoft SQL Server vinculado em diferentes ondas.

Pré-requisitos e limitações

Pré-requisitos

- Verifique se o Microsoft SQL Server no Amazon RDS é compatível com os atributos que você precisa.
- Certifique-se de que você possa usar o Amazon RDS para Microsoft SQL Server com agrupamentos padrão ou agrupamentos definidos em níveis de banco de dados.

Arquitetura

Pilha de tecnologia de origem

- Bancos de dados on-premises (Microsoft SQL Server)

Pilha de tecnologias de destino

- Amazon RDS para SQL Server

Arquitetura do estado de origem

Arquitetura do estado de destino

No estado de destino, você migra o Microsoft SQL Server para o Amazon RDS para Microsoft SQL Server usando servidores vinculados. Essa arquitetura usa um Network Load Balancer para proxy do tráfego do Amazon RDS para Microsoft SQL Server para servidores on-premises que executam o Microsoft SQL Server. O diagrama a seguir mostra a capacidade de proxy reverso do Network Load Balancer.

Ferramentas

- AWS CloudFormation
- Network Load Balancer
- Amazon RDS for SQL Server em várias zonas de disponibilidade (AZsmulti-)
- AWS Database Migration Service (AWS DMS)

Épicos

Criar uma VPC de zona de pouso

Tarefa	Descrição	Habilidades necessárias
Crie a alocação do CIDR.		AWS SysAdmin
Criar uma nuvem privada virtual (VPC).		AWS SysAdmin

Tarefa	Descrição	Habilidades necessárias
Crie as sub-redes VPC.		AWS SysAdmin
Crie as listas de controle de acesso à sub-rede (ACLs).		AWS SysAdmin
Crie as tabelas de rotas da sub-rede.		AWS SysAdmin
Crie uma conexão com o AWS Direct Connect ou a rede privada virtual (VPN).		AWS SysAdmin

Migrar o banco de dados para o Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Criar e conectar-se a uma instância de banco de dados do Amazon RDS para Microsoft SQL Server.		AWS SysAdmin
Criar uma instância de replicação do AWS DMS.		AWS SysAdmin
Crie endpoints para os bancos de dados de origem e destino no AWS DMS.		AWS SysAdmin
Crie a tarefa de migração e defina a replicação contínua como ATIVADA após uma carga completa.		AWS SysAdmin
Solicite uma alteração no firewall para permitir que o Amazon RDS para Microsoft		AWS SysAdmin

Tarefa	Descrição	Habilidades necessárias
SQL Server acesse os bancos de dados on-premises do SQL Server.		
Criar um Network Load Balancer.		AWS SysAdmin
Crie um grupo de destino que tenha como destino os servidores de banco de dados em seu datacenter	Recomendamos que você use nomes de host na configuração de destino para incorporar eventos de failover do datacenter (DC).	AWS SysAdmin
Execute a instrução SQL para configuração do servidor vinculado.	Execute as instruções SQL para adicionar um servidor vinculado usando a ferramenta de gerenciamento Microsoft SQL na instância de banco de dados Amazon RDS para Microsoft SQL Server. Na instrução SQL, defina @datasrc para usar o nome de host do Network Load Balancer. Adicione credenciais de login do servidor vinculado usando a ferramenta de gerenciamento Microsoft SQL na instância de banco de dados Amazon RDS para Microsoft SQL Server.	AWS SysAdmin
Teste e valide as funções do SQL Server.		AWS SysAdmin
Crie uma substituição.		AWS SysAdmin

Recursos relacionados

- Tarefas comuns de gerenciamento para o Microsoft SQL Server no Amazon RDS
- Agrupamentos e conjuntos de caracteres do Microsoft SQL Server
- Documentação do Network Load Balancer
- Implementar servidores vinculados com Amazon RDS para Microsoft SQL Server (publicação no blog)

Saiba como migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando backup e restauração nativos.

Criado por Tirumala Dasari (AWS), David Queiroz (AWS) e Vishal Singh (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados Microsoft SQL Server on-premises para uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS) for SQL Server (migração homogênea). O processo de migração é baseado em métodos nativos de backup e restauração do SQL Server. Ele usa o SQL Server Management Studio (SSMS) para criar um arquivo de backup do banco de dados e um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar o arquivo de backup antes de restaurá-lo no Amazon RDS para SQL Server.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Políticas de Identity and Access Management, perfil do IAM para acessar o bucket do S3 e a instância de banco de dados do Amazon RDS para SQL Server.

Limitações

- O processo descrito nesse padrão migra somente o banco de dados. Os logins do SQL ou os usuários do banco de dados, incluindo qualquer trabalho do SQL Server Agent, não são migrados porque exigem etapas adicionais.

Versões do produto

- SQL Server 2012-2017. Para obter a lista mais recente de versões e atributos compatíveis, consulte Microsoft SQL Server no Amazon RDS na documentação da AWS.

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados Microsoft SQL Server on-premises

Pilha de tecnologias de destino

- Instância de banco de dados do Amazon RDS para SQL Server

Arquitetura de migração de dados

Ferramentas

- O Microsoft SQL Server Management Studio (SSMS) é um ambiente integrado para o gerenciamento de uma infraestrutura do SQL Server. Ele fornece uma interface de usuário e um grupo de ferramentas com editores de scripts avançados que interagem com o SQL Server.

Épicos

Criar Instância de banco de dados do Amazon RDS para SQL Server

Tarefa	Descrição	Habilidades necessárias
Selecione SQL Server como mecanismo de banco de dados no Amazon RDS para SQL Server.		DBA
Escolha o SQL Server Express Edition		DBA
Especifique os detalhes do banco de dados.	Para obter mais informações, consulte documentação do Amazon RDS sobre a criação de uma instância de banco de dados Oracle.	DBA, proprietário do aplicativo

Crie um arquivo de backup a partir do banco de dados SQL Server on-premises

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao banco de dados do SQL Server on-premises por meio do SSMS.		DBA
Criação de um backup do banco de dados	Para obter instruções, consulte a Documentação do SSMS.	DBA, proprietário do aplicativo

Carregue o arquivo de backup no Amazon S3.

Tarefa	Descrição	Habilidades necessárias
Crie um bucket no Amazon S3.	Para obter mais informações, consulte a documentação do Amazon S3.	DBA
Faça upload do arquivo no bucket do S3.	Para mais informações, consulte a documentação do Amazon S3.	SysOps administrador

Restaure o banco de dados no Amazon RDS para SQL Server

Tarefa	Descrição	Habilidades necessárias
Adicione o grupo de opções ao Amazon RDS.	1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/. 2. No painel de navegação, escolha Grupos de opções, Criar grupo.	SysOps administrador

Tarefa	Descrição	Habilidades necessárias
	3. Preencha as informaçõ es do grupo de opções e escolha Criar. 4. Adicione a `SQLSERVER _BACKUP_RESTORE` opção ao grupo de opções e, em seguida, escolha Adicionar opção. Para obter mais informações, consulte a documentação do Amazon RDS.	
Restaure o banco de dados.	1. Conecte-se ao Amazon RDS para SQL Server por meio do SSMS. 2. Para fazer restaurar seu banco de dados, chame o `msdb.dbo.rds_resto re_database` procedimento armazenado.	DBA

Validar o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Valide objetos e dados.	Valide os objetos e dados entre o banco de dados de origem e o Amazon RDS para SQL Server.	Proprietário do aplicativo, DBA

Tarefa	Descrição	Habilidades necessárias
	Note Essa tarefa migra somente o banco de dados. Logins e trabalhos não serão migrados.	

Substituir

Tarefa	Descrição	Habilidades necessárias
Redirecione o tráfego do aplicativo.	Após a validação, redirecione o tráfego do aplicativo para a instância de banco de dados do Amazon RDS para SQL Server.	Proprietário do aplicativo, DBA

Recursos relacionados

- Documentação do Amazon S3
- Documentação do Amazon RDS para SQL Server
- Opções para o mecanismo de banco de dados do Microsoft SQL Server

Migre um banco de dados Microsoft SQL Server para o Aurora MySQL usando o AWS DMS e o AWS SCT

Criado por Mark Szalkiewicz (AWS) e Pavan Pusuluri (AWS)

Resumo

Esse padrão descreve como migrar um banco de dados Microsoft SQL Server que está no local ou em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para o Amazon Aurora MySQL. O padrão usa o AWS Database Migration Service (AWS DMS) e a AWS Schema Conversion Tool (AWS SCT) para migração de dados e conversão de esquemas.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem do Microsoft SQL Server em um data center local ou em uma instância EC2
- Drivers de conectividade de banco de dados Java (JDBC) para conectores AWS SCT, instalados em uma máquina local ou em uma instância em que o AWS SCT EC2 está instalado

Limitações

- Limite de tamanho do banco de dados: 64 TB

Versões do produto

- Microsoft SQL Server 2008, 2008R2, 2012, 2014, 2016, e 2017 para as edições Enterprise, Standard, Workgroup e Developer. As edições Web e Express não são compatíveis com o AWS DMS. Para obter a lista mais recente de versões compatíveis, consulte Usando um banco de dados Microsoft SQL Server como fonte para o AWS DMS. Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e atributos. Para obter informações sobre as versões do Microsoft SQL Server suportadas pelo AWS SCT, consulte a documentação do AWS SCT.
- MySQL, versões 5.5, 5.6 e 5.7. Para obter a lista mais recente de versões compatíveis, consulte Usando um banco de dados compatível com MySQL como destino para o AWS DMS.

Arquitetura

Pilha de tecnologia de origem

Um dos seguintes:

- Um banco de dados do Microsoft SQL Server on-premises
- Um banco de dados Microsoft SQL Server em uma EC2 instância

Pilha de tecnologias de destino

- Aurora MySQL

Arquitetura de migração de dados

- De um banco de dados do Microsoft SQL Server em execução na Nuvem AWS

- De um banco de dados do Microsoft SQL Server em execução em um datacenter on-premises do Microsoft SQL

Ferramentas

- AWS DMS: o AWS Data Migration Service (AWS DMS) ajuda você a migrar seus dados entre bancos de dados comerciais e de código aberto amplamente usados, incluindo Oracle, SQL Server, MySQL e PostgreSQL. É possível usar o AWS DMS para migrar seus dados para a Nuvem AWS, entre instâncias on-premises (por meio de uma configuração da Nuvem AWS) ou entre combinações de nuvem e configurações on-premises.
- AWS SCT: a AWS Schema Conversion Tool (AWS SCT) facilita as migrações heterogêneas de banco de dados convertendo automaticamente o schema do banco de dados de origem e a maioria do código personalizado para um formato compatível com o banco de dados de destino.

Épicos

Preparo para a migração

Tarefa	Descrição	Habilidades necessárias
Valide a versão e o mecanismo dos bancos de dados de origem e de destino.		DBA
Crie um grupo de segurança de saída para os bancos de dados de origem e de destino.		SysAdmin
Crie e configure uma EC2 instância para o AWS SCT, se necessário.		DBA
Faça download da versão mais recente do AWS SCT e dos drivers associados.		DBA
Adicione e valide os pré-requisitos de usuários e concessões no banco de dados de origem.		DBA
Crie um projeto AWS SCT para o workload e conecte-se ao banco de dados de origem.		DBA
Gere um relatório de avaliação e avalie a viabilidade.		DBA

Preparar o banco de dados de destino

Tarefa	Descrição	Habilidades necessárias
Crie uma instância de banco de dados Amazon RDS de destino, usando o Amazon Aurora como mecanismo de banco de dados.		DBA
Extraia a lista de usuários, funções e concessões da fonte.		DBA
Mapeie os usuários do banco de dados existentes para os novos usuários do banco de dados.		Proprietário do App
Criar usuários no banco de dados de destino.		DBA
Aplique funções da etapa anterior ao banco de dados de destino.		DBA
Examine as opções, os parâmetros, os arquivos de rede e os links do banco de dados no banco de dados de origem e, em seguida, avalie sua aplicabilidade ao banco de dados de destino.		DBA
Aplique todas as configura ções relevantes ao destino.		DBA

Transferir objetos

Tarefa	Descrição	Habilidades necessárias
Configure a conectividade do AWS SCT com o banco de dados de destino.		DBA
Converta o esquema usando o AWS SCT.	O AWS SCT converte automaticamente o esquema do banco de dados de origem e a maior parte do código personalizado em um formato compatível com o banco de dados de destino. Qualquer código que não possa ser convertido automaticamente pela ferramenta será marcado em destaque para que você mesmo possa convertê-lo.	DBA
Revise o relatório SQL gerado e salve quaisquer erros e avisos.		DBA
Aplique alterações automatizadas do esquema ao destino ou salve-as como um arquivo .sql.		DBA
Valide se o AWS SCT criou os objetos no destino.		DBA
Reescreva, rejeite ou redesenhe manualmente todos os itens que falharam na conversão automática.		DBA

Tarefa	Descrição	Habilidades necessárias
Aplique a função gerada e as concessões do usuário e analise todas as exceções.		DBA

Migre os dados

Tarefa	Descrição	Habilidades necessárias
Determine o método de migração.		DBA
Criar uma instância de replicação do console do AWS DMS.	Para obter informações detalhadas sobre o uso do AWS DMS, consulte os links na seção “Recursos relaciona dos”.	DBA
Criação de endpoints de origem e de destino.		DBA
Criar uma tarefa de replicaçã o.		DBA
Inicie a tarefa de replicação e monitore os logs.		DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Use o AWS SCT para analisar e converter os itens SQL no código do aplicativo.	Ao converter o esquema do seu banco de dados de um mecanismo para outro, é preciso também atualizar o código SQL nos seus aplicativ	Proprietário do App

Tarefa	Descrição	Habilidades necessárias
	os, a fim de interagir com o novo mecanismo de banco de dados, em vez do antigo. Você pode visualizar, analisar, editar e salvar o código SQL convertido. Para obter informações detalhadas sobre o uso do AWS SCT, consulte os links na seção “Recursos relacionados”.	
Crie os novos servidores de aplicativos na AWS.		Proprietário do App
Migre o código do aplicativo para os novos servidores.		Proprietário do App
Configure o servidor do aplicativo para o banco de dados e os drivers de destino.		Proprietário do App
Corrija qualquer código específico do mecanismo de banco de dados de origem no aplicativo.		Proprietário do App
Otimize o código do aplicativo para o mecanismo de destino.		Proprietário do App

Substituir

Tarefa	Descrição	Habilidades necessárias
Aplique quaisquer novos usuários, concessões e		DBA

Tarefa	Descrição	Habilidades necessárias
alterações de código ao destino.		
Bloqueie o aplicativo para quaisquer alterações.		Proprietário do App
Validar se todas as alteraçõe s foram propagadas para o banco de dados de destino.		DBA
Direcione o novo aplicativo para o novo banco de dados de destino.		Proprietário do App
Confira tudo novamente.		Proprietário do App
Acesse.		Proprietário do App

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporári os da AWS (instância de replicação do AWS DMS e EC2 instância usada para o AWS SCT).		DBA, proprietário do aplicativo
Atualize o feedback sobre o processo do AWS DMS para as equipes internas.		DBA, proprietário do aplicativo
Revise o processo do AWS DMS e melhore o modelo, se necessário.		DBA, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Revise e valide os documentos do projeto.		DBA, proprietário do aplicativo
Reúna métricas sobre o tempo de migração, porcentagem de manual versus economia de custos de ferramentas, etc.		DBA, proprietário do aplicativo
Feche o projeto e forneça feedback, se houver.		DBA, proprietário do aplicativo

Recursos relacionados

Referências

- Guia do usuário do AWS DMS
- Guia do usuário do AWS SCT
- Definição de preço do Amazon Aurora

Tutoriais e vídeos

- Introdução ao AWS Database Migration Service
- Conceitos básicos da AWS Schema Conversion Tool
- Recursos do Amazon RDS
- Instruções passo a passo do AWS DMS Step-by-Step

Migre um banco de dados MariaDB on-premises para o Amazon RDS para MariaDB usando ferramentas nativas

Criado por Shyam Sunder Rakhecha (AWS)

Resumo

Esse padrão fornece orientação para migrar um banco de dados MariaDB on-premises para o Amazon Relational Database Service (Amazon RDS) for MariaDB usando ferramentas nativas. Se você tiver ferramentas MySQL instaladas, poderá usar mysql e mysqldump. Se você tiver ferramentas MariaDB instaladas, poderá usar mariadb e mariadb-dump. As ferramentas MySQL e MariaDB têm a mesma origem, mas há pequenas diferenças na versão 10.6 e posterior do MariaDB.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um banco de dados de origem do MariaDB em um datacenter on-premises

Limitações

- Limite de tamanho do banco de dados: 64 TB

Versões do produto

- Versões 10.0-10.6 do MariaDB (para obter a lista mais recente de versões compatíveis, consulte MariaDB no Amazon RDS na documentação da AWS)

Arquitetura

Pilha de tecnologia de origem

- Banco de dados MariaDB em um datacenter on-premises

Pilha de tecnologias de destino

- Instâncias de banco de dados para o Amazon RDS para MariaDB

Arquitetura de destino

Arquitetura de migração de dados

Ferramentas

- Ferramentas nativas MySQL: mysql e mysqldump
- Ferramentas nativas MariaDB: mariadb e mariadb-dump

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide as versões e os motores dos bancos de dados de origem e de destino.		DBA
Identifique os requisitos de hardware para a instância do servidor de destino.		DBA, administrador de sistemas
Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).		DBA, administrador de sistemas
Escolha o tipo de instância adequado com base na capacidade, nos atributos de armazenamento e nos atributos de rede.		DBA, administrador de sistemas
Identifique os requisitos de segurança do acesso à rede		DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
para os bancos de dados de origem e de destino.		
Identifique a estratégia de migração de aplicativos.		DBA, proprietário do aplicativo, administrador de sistemas

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).		Administrador de sistemas
Criar grupos de segurança.		Administrador de sistemas
Configurar e iniciar uma instância de banco de dados do Amazon RDS executando o MariaDB.		Administrador de sistemas

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Use ferramentas nativas para migrar objetos e dados do banco de dados.	No banco de dados de origem, use mysqldump oumariadb-dump para criar um arquivo de saída que contenha objetos e dados do banco de dados. No banco de dados de destino, use mysql ou mariadb para restaurar os dados.	DBA
Valide os dados.	Verifique os bancos de dados de origem e destino para	DBA

Tarefa	Descrição	Habilidades necessárias
	confirmar se a migração de dados foi bem-sucedida.	

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia de migração de aplicativos.		DBA, proprietário do aplicativo, administrador de sistemas

Substituir

Tarefa	Descrição	Habilidades necessárias
Mude os clientes do aplicativo para a nova infraestrutura.		DBA, proprietário do aplicativo, administrador de sistemas

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Encerre os recursos temporários da AWS.		Administrador de sistemas
Revise e valide os documentos do projeto.		DBA, proprietário do aplicativo, administrador de sistemas
Reúna métricas na hora certa para migrar, com a economia de custos fornecida pelas ferramentas e assim por diante.		DBA, proprietário do aplicativo, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Feche o projeto e forneça feedback.		DBA, proprietário do aplicativo, administrador de sistemas

Recursos relacionados

Referências do Amazon RDS

- Amazon RDS para MariaDB
- Amazon Virtual Private Cloud VPCs e Amazon RDS
- Implantações multi-AZ do Amazon RDS
- Preços do Amazon RDS

Referências do MySQL e do MariaDB

- mariadb-dump/mysqldump
- Cliente da linha de comando mysql

Tutoriais e vídeos

- Conceitos básicos do Amazon RDS

Migrar um banco de dados MySQL on-premises para o Aurora MySQL

Criado por Igor Obradovic (AWS)

Resumo

Esse padrão explica como migrar um banco de dados de origem MySQL local para a edição compatível com o Amazon Aurora MySQL. Ele descreve duas opções de migração: usando AWS Database Migration Service (AWS DMS) ou usando ferramentas nativas do MySQL, como mysqldbcopy e mysqldump.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um banco de dados MySQL de origem em um datacenter on-premises

Limitações

- Limite de tamanho do banco de dados: 128 TB

Versões do produto

- A versão 8.0 do MySQL (Aurora MySQL versão 3) está disponível sob suporte padrão.
- A versão 5.7 do MySQL (Aurora MySQL versão 2) está disponível sob suporte estendido, por um custo adicional.

Para obter a lista mais recente de versões compatíveis, consulte as versões do Amazon Aurora na AWS documentação. Se você estiver usando AWS DMS, consulte também Usando um banco de dados compatível com MySQL como destino para versões do AWS DMS MySQL suportadas pelo. AWS DMS

Arquitetura

Pilha de tecnologia de origem

- Um banco de dados MySQL on-premises

Pilha de tecnologias de destino

- Amazon Aurora Edição Compatível com MySQL

Arquitetura de destino

Os dados do Aurora são armazenados em um volume de cluster, que é um único volume virtual que usa unidades de estado sólido ()SSDs. Um volume de cluster consiste em cópias dos dados em várias zonas de disponibilidade em uma única região da AWS. Como os dados são replicados automaticamente nas zonas de disponibilidade, eles são altamente duráveis com menos possibilidade de perda de dados.

O Aurora divide automaticamente o volume do seu banco de dados em segmentos de 10 GB espalhados por vários discos. Cada bloco de 10 GB do volume do seu banco de dados é replicado de seis maneiras, em três zonas de disponibilidade. O diagrama a seguir ilustra a relação entre o volume do cluster, a instância de banco de dados do gravador e as instâncias de banco de dados do leitor em um cluster de banco de dados Aurora e a separação entre capacidade computacional e armazenamento. Para obter mais informações sobre essa arquitetura, consulte a documentação e as perguntas frequentes do Aurora.

Arquitetura de migração de dados

Usando AWS DMS:

O diagrama a seguir ilustra a migração de um banco de dados MySQL local para um cluster compatível com o Aurora MySQL no, usando. Nuvem AWS AWS DMS

Usando ferramentas nativas do MySQL:

O diagrama a seguir ilustra a migração de um banco de dados MySQL local para um cluster compatível com o Aurora MySQL no, usando ferramentas nativas do MySQL Nuvem AWS, como mysqldbcopy e mysqldump.

Ferramentas

- AWS Database Migration Service (AWS DMS) oferece suporte a vários mecanismos de banco de dados de origem e destino. Para obter informações sobre bancos de dados de origem e destino

do MySQL compatíveis com AWS DMS, consulte Migração de bancos de dados compatíveis com MySQL para. AWS Recomendamos que você use a versão mais recente do AWS DMS para obter o suporte mais abrangente de versões e recursos.

- mysqldbcopy é um utilitário MySQL que copia um banco de dados MySQL em um único servidor ou entre servidores.
- mysqldump é um utilitário MySQL que cria um arquivo de despejo de um banco de dados MySQL para fins de backup ou migração.

Épicos

Planejar a migração

Tarefa	Descrição	Habilidades necessárias
Valide a versão e o mecanismo.	Valide a versão e o mecanismo do banco de dados para os bancos de dados de origem e de destino.	DBA
Identifique os requisitos de hardware.	Identifique os requisitos de hardware para a instância do servidor de destino.	DBA, administrador de sistemas
Identifique os requisitos de armazenamento.	Identifique os requisitos de armazenamento (tipo e capacidade de armazenam ento).	DBA, administrador de sistemas
Altere o tipo de instância.	Escolha o tipo de instância adequado com base em seus requisitos de computação, armazenamento e rede.	DBA, administrador de sistemas
Determine os requisitos de segurança de acesso à rede.	Identifique os requisitos de segurança de acesso à rede para os bancos de dados de origem e de destino.	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Determine a estratégia.	Identifique a estratégia de migração de aplicativos.	DBA, proprietário do aplicativo, administrador de sistemas

Configurar a infraestrutura

Tarefa	Descrição	Habilidades necessárias
Criar uma nuvem privada virtual (VPC).	Para obter instruções, consulte Criar uma VPC na documentação da Amazon Virtual Private Cloud (Amazon VPC).	Administrador de sistemas
Criar grupos de segurança.	Para obter instruções, consulte Criar um grupo de segurança para sua VPC na documentação da Amazon VPC.	Administrador de sistemas
Configure e inicie um cluster de banco de dados compatível com o Aurora MySQL no seu. Conta da AWS	Para obter instruções, consulte Criar um cluster de banco de dados do Amazon Aurora na documentação do Aurora.	Administrador de sistemas

Migrar dados - opção 1

Tarefa	Descrição	Habilidades necessárias
Use ferramentas nativas do MySQL ou terceirizadas para migrar objetos e dados do banco de dados.	Para obter instruções, consulte a documentação das ferramentas do MySQL, como mysqldbcopy e mysqldump.	DBA

Migrar dados - opção 2

Tarefa	Descrição	Habilidades necessárias
Migre dados com AWS DMS.	Para obter instruções, consulte Usando um banco de dados compatível com MySQL como fonte e Usando um banco de dados compatível com MySQL como destino na documentação. AWS DMS	DBA

Migrar o aplicativo

Tarefa	Descrição	Habilidades necessárias
Siga a estratégia.	Siga a estratégia de migração de aplicativos.	DBA, proprietário do aplicativo, administrador de sistemas

Substituir

Tarefa	Descrição	Habilidades necessárias
Troque clientes de aplicativos.	Troque os clientes do aplicativo para se conectarem ao novo endpoint do cluster Aurora.	DBA, proprietário do aplicativo, administrador de sistemas

Fechar o projeto

Tarefa	Descrição	Habilidades necessárias
Desligar recursos.	Encerre AWS os recursos temporários.	DBA, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
Revise a documentação.	Revise e valide os documentos do projeto.	DBA, proprietário do aplicativo, administrador de sistemas
Colete métricas.	Reúna métricas sobre o tempo de migração, porcentagem de etapas manuais versus uso de ferramentas, economia de custos e assim por diante.	DBA, proprietário do aplicativo, administrador de sistemas
Projeto completo de migração.	Feche o projeto e forneça feedback.	Proprietário do aplicativo, DBA, administrador de sistemas

Recursos relacionados

Referências

- Migração de dados para o cluster de banco de dados Amazon Aurora MySQL
- AWS DMS site
- AWS DMS documentação
- Definição de preço do Amazon Aurora
- Criação e conexão com um cluster de banco de dados Aurora MySQL
- Amazon VPC e Amazon RDS
- Documentação do Amazon Aurora

Tutoriais e vídeos

- Começando com AWS DMS
- Conceitos básicos do Amazon Aurora

Migre bancos de dados MySQL locais para o Aurora MySQL usando XtraBackup Percona, Amazon EFS e Amazon S3

Criado por Rohan Jamadagni (AWS), Sajith Menon (AWS) e Udayasimha Theepireddy (AWS)

Resumo

Esse padrão descreve como migrar bancos de dados MySQL grandes e locais de forma eficiente para o Amazon Aurora MySQL usando o Percona. XtraBackup O Percona XtraBackup é um utilitário de backup de código aberto e sem bloqueio para servidores baseados em MySQL. O padrão mostra como usar o Amazon Elastic File System (Amazon EFS) para reduzir o tempo de upload do backup para o Amazon Simple Storage Service (Amazon S3) e restaurar o backup no Amazon Aurora MySQL. O padrão também fornece detalhes sobre como fazer backups incrementais do Percona para minimizar o número de logs binários a serem aplicados ao banco de dados Aurora MySQL de destino.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões para criar perfis e políticas do Identity and Access Management (IAM) da AWS
- Conectividade de rede entre o banco de dados MySQL on-premises e a nuvem privada virtual (VPC) na AWS

Limitações

- Os servidores de origem devem ser sistemas baseados em Linux que possam instalar um cliente Network File System (NFS) (nfs-utils/nfs-common).
- O bucket do S3 usado para carregar arquivos de backup oferece suporte somente à criptografia do lado do servidor (SSE-S3/SSE-KMS).
- O Amazon S3 limita o tamanho dos arquivos de backup a 5 TB. Se o arquivo de backup exceder 5 TB, você poderá dividir o arquivo em vários arquivos menores.
- O número de arquivos de origem enviados por upload para um bucket do S3 não poderá exceder um milhão de arquivos.
- O padrão suporta somente o backup XtraBackup completo e o backup incremental do Percona. Ele não oferece suporte a backups parciais que usam `--tables`, `--tables-exclude`, `--tables-file`, `--databases`, `--databases-exclude` ou `--databases-file`.

- O Aurora não restaura usuários, funções, procedimentos armazenados ou informações de fuso horário do banco de dados MySQL de origem.

Versões do produto

- O banco de dados de origem deverá ser o MySQL versão 5.5, 5.6 ou 5.7.
- Para o MySQL 5.7, você deve usar o Percona 2.4. XtraBackup
- Para o MySQL 5.6 e 5.6, você deve usar o XtraBackup Percona 2.3 ou 2.4.

Arquitetura

Pilha de tecnologia de origem

- Sistema operacional baseado em Linux
- MYSQL server
- Percona XtraBackup

Pilha de tecnologias de destino

- Amazon Aurora
- Amazon S3
- Amazon EFS

Arquitetura de destino

Ferramentas

Serviços da AWS

- O Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado que torna a configuração, operação e escalabilidade de implantações do MySQL. O Aurora MySQL é um substituto imediato para o MySQL.
- O Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS.

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- O Percona XtraBackup é um utilitário de código aberto que realiza backups de streaming, compactados e incrementais de bancos de dados MySQL sem interromper ou bloquear seus bancos de dados.

Épicos

Criar um sistema de arquivos do Amazon EFS

Tarefa	Descrição	Habilidades necessárias
Crie um grupo de segurança para associar aos destinos de montagem do Amazon EFS.	Crie um grupo de segurança na VPC configurado com um anexo de VPN ao banco de dados on-premises no AWS Transit Gateway. Para obter mais informações sobre os comandos e as etapas descritos nesta e em outras histórias, consulte os links na seção “Recursos relaciona dos” no final desse padrão.	AWS DevOps /administrador de banco de dados
Editar as regras do grupo de segurança.	Adicione uma regra de entrada usando o tipo NFS, a porta 2049 e o intervalo de IP do servidor de banco de dados on-premises como origem. Por padrão, a regra de saída permite que todo tráfego saia. Se esse não for o caso, adicione uma regra de	AWS DevOps /administrador de banco de dados

Tarefa	Descrição	Habilidades necessárias
	saída para abrir uma conexão para a porta NFS. Adicione mais duas regras de entrada: porta 2049 (fonte: ID do grupo de segurança desse mesmo grupo de segurança) e porta 22 (origem: intervalo de IP de onde você se conectará a uma EC2 instância).	
Crie um sistema de arquivos.	Nos destinos de montagem, use a VPC e o grupo de segurança que você criou na história anterior. Escolha o modo de throughput e o desempenho com base nos requisitos de E/S do banco de dados on-premis es. Opcionalmente, habilite a criptografia em repouso.	AWS DevOps /administrador de banco de dados

Monte o sistema de arquivos

Tarefa	Descrição	Habilidades necessárias
Crie uma função de perfil de instância do IAM para ser associada a uma EC2 instância.	Crie um perfil do IAM que tenha permissões para carregar e acessar objetos no Amazon S3. Escolha o bucket do S3 no qual o backup será armazenado como um recurso de política.	AWS DevOps
Crie uma EC2 instância.	Inicie uma EC2 instância baseada em Linux e anexe a	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	função de perfil da instância do IAM que você criou na etapa anterior e o grupo de segurança que você criou anteriormente.	
Instale o NFS cliente.	Instale o cliente NFS no servidor de banco de dados local e na EC2 instância. Para obter instruções de instalação, consulte a seção “Informações adicionais”.	DevOps
Monte o sistema de arquivos do Amazon EFS.	Monte o sistema de arquivos Amazon EFS no local e na EC2 instância. Em cada servidor, crie um diretório para armazenar o backup e monte o sistema de arquivos usando o endpoint de destino de montagem. Consulte a seção “Informações adicionais”.	DevOps

Fazer backups do banco de dados de origem MySQL

Tarefa	Descrição	Habilidades necessárias
Instale o Percona XtraBackup.	Instale o Percona XtraBackup 2.3 ou 2.4 (dependendo da versão do seu banco de dados MySQL) no servidor de banco de dados local. Para ver os links de instalação, consulte	Administrador de banco de dados

Tarefa	Descrição	Habilidades necessárias
	a seção “Recursos relaciona dos”.	
Conte os esquemas e as tabelas no banco de dados de origem.	Reúna e anote o número de esquemas e objetos no banco de dados MySQL de origem. Você usará essas contagens para validar o banco de dados Aurora MySQL após a migração.	Administrador de banco de dados
(Opcional) Observe a sequência de log binário mais recente do banco de dados de origem.	Execute essa etapa se quiser estabelecer a replicação de log binário entre o banco de dados de origem e o Aurora MySQL para minimizar o tempo de inatividade. O log-bin deverá estar ativado e o server_id deve ser exclusivo . Observe a sequência de log binário atual do banco de dados de origem, pouco antes de iniciar um backup. Execute essa etapa logo antes do backup completo se você planeja usar somente o backup completo. Se você planeja fazer backups incrementais após um backup completo, execute essa etapa logo antes do backup incremental final que você restaurará na instância de banco de dados Aurora MySQL.	Administrador de banco de dados

Tarefa	Descrição	Habilidades necessárias
Iniciar um backup completo do banco de dados MySQL de origem.	Faça um backup completo do banco de dados de origem do MySQL usando o Percona. XtraBackup Por exemplo, comandos para backups completos e incrementais, consulte a seção “Informações adicionais”.	Administrador de banco de dados

Tarefa	Descrição	Habilidades necessárias
(Opcional) Faça backups incrementais usando o XtraBackup Percona.	Os backups incrementais poderão ser usados para reduzir a quantidade de registros binários que você precisa aplicar para sincroniz ar o banco de dados de origem com o Aurora MySQL. Bancos de dados grandes e com muitas transações poderão gerar um grande número de logs binários durante os backups. Ao fazer backups incrementais e armazená-los em um sistema de arquivos compartilhado do Amazon EFS, você poderá reduzir significativamente o tempo de backup e upload do seu banco de dados. Consulte a seção “Informaç ões adicionais” para obter detalhes. Continue fazendo backups incrementais até que esteja pronto para começar o processo de migração para o Aurora.	Administrador de banco de dados

Tarefa	Descrição	Habilidades necessárias
Preparar backups.	Nesta etapa, os logs transacionais são aplicados ao backup para transações que estavam em andamento durante o backup. Continue aplicando registros transacionais (--apply-log-only) a cada backup incremental para mesclar os backups, exceto para o último backup. Para obter exemplos, consulte a seção “Informações adicionais”. Após essa etapa, o backup completo e mesclado estará em ~/<efs_mount_name>/fullbackup.	Administrador de banco de dados
Compactar e dividir o backup mesclado.	Depois de preparar o backup final mesclado, use os comandos tar, zip e split para criar arquivos compactados menores do backup. Para obter exemplos, consulte a seção “Informações adicionais”.	Administrador de banco de dados

Restaurar o backup em um cluster de banco de dados do Aurora MySQL

Tarefa	Descrição	Habilidades necessárias
Carregar o backup no Amazon S3.	O sistema de arquivos do Amazon EFS, no qual os arquivos de backup são armazenados, é montado	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	no banco de dados local e em uma EC2 instância, de forma que os arquivos de backup estejam prontamente disponíveis para a EC2 instância. <efs_mount_name><bucket_name>Conecte-se à EC2 instância usando o Secure Shell (SSH) e carregue os arquivos de backup compactados em um bucket S3 novo ou existente; por exemplo: aws s3 sync ~/ /fullbackup s3:///fullbackup. Para obter detalhes adicionais, consulte os links na seção “Recursos relacionados”.	
Criar um perfil de serviço para o Aurora acessar o Amazon S3.	Crie um perfil do IAM com a confiança “rds.amazonaws.com” e uma política que permitirá que o Aurora acesse o bucket do S3 onde os arquivos de backup estão armazenados. As permissões necessárias são ListBucket GetObject, GetObjectVersion e.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Criar a configuração de rede para o Aurora.	Criar um grupo de sub-redes de banco de dados de cluster com pelo menos duas zonas de disponibilidade e uma configuração de tabela de rotas de sub-rede que permita conectividade de saída com o banco de dados de origem. Criar um grupo de segurança que permita conexões de saída com o banco de dados on-premises e permita que os administradores se conectem ao cluster de banco de dados Aurora. Para obter mais informações, acesse os links na seção “Recursos relacionados”.	AWS DevOps /administrador de banco de dados
Restaurar o backup em um cluster de banco de dados do Aurora MySQL.	Restaurar seus dados do backup que você enviou para o Amazon S3. Especificar a versão MySQL do seu banco de dados de origem, fornecer o nome do bucket do S3 e o prefixo do caminho da pasta em que você fez o upload do arquivo de backup (por exemplo, “fullbackup” para os exemplos na seção “Informações adicionais”) e forneça o perfil do IAM que você criou para autorizar o Aurora a acessar o Amazon S3.	AWS DevOps /administrador de banco de dados

Tarefa	Descrição	Habilidades necessárias
Validar o banco de dados MySQL do Aurora.	Valide a contagem de esquemas e objetos no cluster de banco de dados Aurora restaurado em relação à contagem que você obteve do banco de dados de origem.	Administrador de banco de dados
Configurar a replicação do log binário.	Usar a sequência de log binário que você anotou anteriormente, antes de fazer o último backup que foi restaurado no cluster de banco de dados do Aurora. Criar um usuário de replicaçã o no banco de dados de origem e siga as instruções na seção “Informações adicionai s” para fornecer os privilégi os adequados, habilitar a replicação no Aurora e confirmar se a replicação está sincronizada.	AWS DevOps /administrador de banco de dados

Recursos relacionados

Criar um sistema de arquivos do Amazon EFS

- Criação de um grupo de segurança (Documentação do Amazon VPC)
- Anexos do VPN do gateway de trânsito (Documentação do Amazon VPC)
- Escalar o throughput de VPN usando o AWS Transit Gateway (blog sobre redes e entrega de conteúdo)
- Criar um sistema de arquivos do Amazon EFS (Documentação do Amazon EFS)
- Criação de destinos de montagem (Documentação do Amazon EFS)
- Criptografar dados em repouso (Documentação do Amazon EFS)

Montagem do sistemas de arquivos

- Funções do IAM para a Amazon EC2 (EC2 documentação da Amazon)
- Lançamento de uma instância Amazon EC2 Linux (EC2 documentação da Amazon)
- Instalação do cliente NFS (Documentação do Amazon EFS)
- Montagem do sistema de arquivos do Amazon EFS em seu cliente on-premises (Documentação do Amazon EFS)
- Montagem de sistemas de arquivos EFS (Documentação do Amazon EFS)

Realizar um backup do banco de dados de origem MySQL

- Instalando o Percona XtraBackup 2.3 (documentação do XtraBackup Percona)
- Instalando o Percona XtraBackup 2.4 (documentação do XtraBackup Percona)
- Definir a configuração principal de replicação (Documentação do MySQL)
- Migrar dados de um banco de dados MySQL externo para um cluster de banco de dados do Amazon Aurora MySQL (Documentação do Aurora)
- Backup incremental (documentação da XtraBackup Percona)

Restaurar o backup no Amazon Aurora MySQL

- Criar um bucket (Documentação do Amazon S3)
- Conectar-se à instância do Linux usando o SSH (Documentação do Amazon EC2)
- Configurando a AWS CLI (documentação da AWS CLI)
- comando sync (referência de comando da AWS CLI)
- Criar uma política do IAM para acessar recursos do Amazon S3 (Documentação do Aurora)
- Pré-requisitos do cluster de banco de dados (Documentação do Aurora)
- Trabalhar com grupos de sub-redes de banco de dados (Documentação do Aurora)
- Criar um grupo de segurança da VPC para uma instância de banco de dados privada (Documentação do Aurora)
- Restaurar um cluster de banco de dados do Aurora MySQL a partir de um bucket do S3 (Documentação do Aurora)
- Configurar a replicação com MySQL ou outro cluster de banco de dados do Aurora (Documentação do Aurora)

- procedimento mysql.rds_set_external_master (MySQL na referência SQL do Amazon RDS)
- procedimento mysql.rds_start_replication (MySQL na referência SQL do Amazon RDS)

Referências adicionais

- Migrar dados de um banco de dados MySQL externo para um cluster de banco de dados do Amazon Aurora MySQL (Documentação do Aurora)
- Downloads do servidor MySQL (site da Oracle)

Tutoriais e vídeos

- Migração de dados do MySQL para um cluster de banco de dados Aurora MySQL usando o Amazon S3 (Centro de conhecimento da AWS)
- Configuração e montagem do Amazon EFS (vídeo)

Mais informações

Instalar um cliente NFS

- Se você estiver usando o Red Hat ou um sistema operacional Linux similar, use o comando:

```
$ sudo yum -y install nfs-utils
```

- Se você estiver usando o Ubuntu ou um sistema operacional Linux similar, use o comando:

```
$ sudo apt-get -y install nfs-common
```

Para obter mais informações, consulte o passo a passo na documentação do Amazon EFS.

Montar o sistema de arquivos do Amazon EFS

Use os comandos:

```
mkdir ~/<efs_mount_name>
```

```
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-IP:/ ~/<efs_mount_name>
```

Para obter mais informações, consulte o passo a passo e montagem de sistemas de arquivos EFS na documentação do Amazon EFS.

Fazendo backups do banco de dados de origem MySQL

Backups completos

Use um comando como o seguinte, que pega o backup, o compacta e o divide em partes menores de 1 GB cada:

```
xtrabackup --backup --user=dbuser --password=<password> --binlog-info=AUTO --stream=tar
 --target-dir=~/<efs_mount_name>/fullbackup | gzip - | split -d --bytes=1024MB - ~/
<efs_mount_name>/fullbackup/backup.tar.gz &
```

Se você planeja fazer backups incrementais subsequentes após o backup completo, não compacte e divida o backup. Em vez disso, use um comando semelhante ao seguinte:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/fullbackup/
```

Backups incrementais

Use o caminho de backup completo para o parâmetro `--incremental-basedir`; por exemplo:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/incremental/backupdate --incremental-basedir=~/<efs_mount_name>/
fullbackup
```

em que basedir é o caminho para o backup completo e o arquivo xtrabackup_checkpoints.

Para obter mais informações, consulte Migrar dados de um banco de dados MySQL externo para um cluster de banco de dados MySQL do Amazon Aurora na documentação do Aurora.

Preparar backups

Preparar um backup completo:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup
```

Para preparar um backup incremental:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup --
incremental-dir=~/<efs_mount_name>/incremental/06062020
```

Para preparar o backup final:

```
xtrabackup --prepare --target-dir=~/<efs_mount_name>/fullbackup --incremental-dir=~/
<efs_mount_name>/incremental/06072020
```

Para obter mais informações, consulte Backups incrementais na documentação da XtraBackup Percona.

Compactar e dividir o backup mesclado

Para compactar o backup mesclado em ~/<efs_mount_name>/fullbackup:

```
tar -zcvf <backupfilename.tar.gz> ~/<efs_mount_name>/fullbackup
```

Para dividir o backup:

```
split -d -b1024M --verbose  <backupfilename.tar.gz> <backupfilename.tar.gz>
```

Configurar a replicação do log binário

Para criar um usuário de replicação no banco de dados de origem e fornecer os privilégios adequados:

```
CREATE USER 'repl_user'@'' IDENTIFIED BY ''; GRANT REPLICATION CLIENT, REPLICATION
 SLAVE ON *.* TO 'repl_user'@'';
```

Para habilitar a replicação no Aurora conectando-se ao cluster de banco de dados Aurora, habilite os registros binários no grupo de parâmetros do cluster de banco de dados. Definir `binlog_format = mixed` (o modo misto é preferido). Essa alteração exige que você reinicie a instância para aplicar a atualização.

```
CALL mysql.rds_set_external_master ('sourcedbinstanceIP', sourcedbport, 'repl_user',
 '', 'binlog_file_name', binlog_file_position, 0); CALL mysql.rds_start_replication;
```

Para confirmar se a replicação está sincronizada:

```
SHOW Slave Status \G;
```

O campo Segundos atrás do mestre mostra o quanto o Aurora está atrasado em relação ao banco de dados on-premises.

Migrar aplicações Java on-premises para a AWS usando o App2Container da AWS

Criado por Dhananjay Karanjkar (AWS)

Resumo

Aviso: CodeCommit A AWS não está mais disponível para novos clientes. Os clientes atuais da AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

O AWS App2Container (A2C) é uma ferramenta de linha de comando que ajuda a transformar aplicativos existentes executados em máquinas virtuais em contêineres, sem a necessidade de alterações no código. O A2C descobre aplicações em execução em um servidor, identifica dependências e gera artefatos relevantes para uma implantação sem contratempos no Amazon Elastic Container Service (Amazon ECS) e no Amazon Elastic Kubernetes Service (Amazon EKS).

Esse padrão fornece as etapas para migrar remotamente aplicativos Java on-premises implantados em um servidor de aplicativos para o AWS Fargate ou o Amazon EKS usando o App2Container por meio da máquina de trabalho.

A máquina de trabalho pode ser usada nos seguintes casos de uso:

- A instalação do Docker não é permitida ou não está disponível nos servidores de aplicativos em que os aplicativos Java estão sendo executados.
- Você deve gerenciar a migração de vários aplicativos implantados em diferentes servidores físicos ou virtuais.

Esse padrão usa AWS CodeCommit AWS CodePipeline, AWS CodeBuild e.

Pré-requisitos e limitações

Pré-requisitos

- Um servidor de aplicação com uma aplicação Java em execução em um servidor Linux
- Uma máquina de trabalho com um sistema operacional Linux
- Uma máquina de trabalho com pelo menos 20 GB de espaço em disco disponível

Limitações

- Nem todos os aplicativos são compatíveis. Para obter mais informações, consulte Aplicativos compatíveis para Linux.

Arquitetura

Pilha de tecnologia de origem

- Aplicativos Java em execução no servidor Linux

Pilha de tecnologias de destino

- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Amazon Elastic Container Registry
- AWS Fargate

Arquitetura de destino

Ferramentas

Ferramentas

- AWS App2Container: o AWS App2Container (A2C) é uma ferramenta da linha de comando que ajuda você a elevar e mudar aplicações executadas em seus datacenters on-premises ou em máquinas virtuais, para que eles sejam executados em contêineres gerenciados pelo Amazon ECS ou Amazon EKS.
- AWS CodeBuild — CodeBuild A AWS é um serviço de construção totalmente gerenciado na nuvem. CodeBuild compila seu código-fonte, executa testes de unidade e produz artefatos prontos para serem implantados.
- AWS CodeCommit — CodeCommit A AWS é um serviço de controle de versão hospedado pela Amazon Web Services que você pode usar para armazenar e gerenciar de forma privada ativos (como documentos, código-fonte e arquivos binários) na nuvem.
- AWS CodePipeline — CodePipeline A AWS é um serviço de entrega contínua que você pode usar para modelar, visualizar e automatizar as etapas necessárias para lançar seu software.

- Amazon ECS: o Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagem de contêiner, seguro, escalável e confiável.
- Amazon EKS: o Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço gerenciado que você pode usar para executar o Kubernetes na AWS, eliminando a necessidade de instalar, operar e manter seus próprios nós ou ambiente de gerenciamento do Kubernetes.
- AWS Fargate — O AWS Fargate é uma tecnologia que você pode usar com o Amazon ECS para executar contêineres sem precisar gerenciar servidores ou clusters de instâncias do Amazon Elastic Compute Cloud (Amazon). EC2 Com o Fargate, não é mais necessário provisionar, configurar nem escalar os clusters de máquinas virtuais para executar contêineres.

Épicos

Configurar credenciais

Tarefa	Descrição	Habilidades necessárias
Crie um segredo para acessar o servidor do aplicativo.	Para acessar o servidor do aplicativo remotamente a partir da máquina de trabalho, crie um segredo no AWS Secrets Manager. Como seu segredo, você pode usar a chave privada SSH ou o Certificado e a chave privada SSH. Para obter mais informações, consulte Gerenciar segredos para o AWS ApP2Container.	DevOps, Desenvolvedor

Configure a máquina do operador

Tarefa	Descrição	Habilidades necessárias
Instalar o arquivo tar.	Executar `sudo yum install -y tar`.	DevOps, Desenvolvedor
Instale a AWS CLI.	Instalar a interface da linha de comando Amazon (AWS CLI), execute `curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip" .` Descompacte `awscliv2.zip .` Executar `sudo ./aws/install .`	DevOps, Desenvolvedor

Instale o App2Container.	Execute os seguintes comandos :
	
	`curl -o AWSApp2Container-installer-linux.tar.gz https://app2container-release-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/AWSApp2Container-installer-linux.tar.gz`
	
	`sudo tar xvf AWSApp2Container-installer-linux.tar.gz`
		DevOps, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	`sudo ./install.sh`	
Configure os perfis.	Para configurar o perfil padrão da AWS, execute `sudo aws configure .` Para configurar o perfil da AWS, execute `sudo aws configure --profile <profile name>`.	DevOps, Desenvolvedor

Instalar o Docker.	Execute os seguintes comandos.
	
	`sudo yum install -y docker`
	
	`sudo systemctl enable docker & sudo systemctl restart docker`	

Tarefa	Descrição	Habilidades necessárias
Inicialize o App2Container.	Para inicializar o App2Container, você precisa das seguintes informações: • `workspace` : para armazenar artefatos de conteinerização de aplicativos. Recomendamos fornecer um caminho de diretório que tenha pelo menos 20 GB de espaço livre em disco. • `awsProfile` : perfil da AWS configurado no servidor. Isso é necessário para carregar artefatos no Amazon S3, executar o comando `containerize` e gerar artefatos da AWS para implantação no Amazon ECS ou no Amazon EKS. • `s3Bucket`: para extrair e armazenar o AWS Artifacts. • `metricsReportPermission` : para coletar e armazenar métricas relatadas. • `dockerContentTrust` : para assinar a imagem do Docker.	DevOps, Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	Executar `sudo app2container init .`	

Configurar a máquina de trabalho

Tarefa	Descrição	Habilidades necessárias
Configure a máquina de trabalho para se conectar e executar remotamente os comandos do App2Container no servidor do aplicativo.	Para configurar a máquina de trabalho, as seguintes informações são necessárias: • `Server FQDN`: o nome de domínio totalmente qualificado do servidor da aplicação. • `Server IP address`: o endereço IP do servidor da aplicação. O FQDN ou o endereço IP são suficientes. • `SecretARN` : o nome do recurso da Amazon (ARN) do segredo usado para se conectar ao servidor da aplicação e armazenado no Secrets Manager. • `AuthMethod` : os métodos de autenticação `key` ou `cert`. Executar `sudo app2container remote configure` .	DevOps, Desenvolvedor

Descubra, analise e extraia aplicativos na máquina de trabalho

Tarefa	Descrição	Habilidades necessárias
Descubra os aplicativos Java locais on-premises.	Para descobrir remotamente todos os aplicativos em execução no servidor de aplicativos, execute o comando a seguir. `sudo app2container remote inventory --target <FQDN/IP of App server>` Esse comando gera uma lista de aplicativos implantados em `inventory.json` .	Desenvolvedor, DevOps
Analise os aplicativos descobertos.	Para analisar remotamente cada aplicativo usando o que foi obtido no estágio de inventário, execute o comando a seguir. `sudo app2container remote analyze --application-id <java-app-id> --target <FQDN/IP of App Server>` Isso gera um arquivo `analysis.json` no local do espaço de trabalho. Depois que esse arquivo for gerado, você poderá alterar os parâmetros de conteiner	Desenvolvedor, DevOps

Tarefa	Descrição	Habilidades necessárias
	ização com base nas suas necessidades.	
Extraia os aplicativos analisados.	Para gerar um arquivo do aplicativo analisado, execute remotamente o comando a seguir, que deverá gerar o pacote tar no local do espaço de trabalho. `sudo app2container remote extract --application-id <application id> --target <FQDN/IP of App Server>` Os artefatos extraídos podem ser gerados na máquina de trabalho local.	Desenvolvedor, DevOps

Coloque em contêineres os artefatos extraídos na máquina de trabalho

Tarefa	Descrição	Habilidades necessárias
Coloque os artefatos extraídos em contêineres.	Coloque em contêineres os artefatos extraídos na etapa anterior executando o comando a seguir. `sudo app2container containerize --input-archive <tar bundle location on worker machine>`	Desenvolvedor, DevOps

Tarefa	Descrição	Habilidades necessárias
Finalize o destino.	Para finalizar o destino, abra `deployment.json` , que será criado quando o comando `containerize` for executado. Para especificar o AWS Fargate como destino, defina `createEcsArtifacts` como `true`. Para definir o Amazon EKS como destino, defina `createEksArtifacts` como verdadeiro.	Desenvolvedor, DevOps

Gere e provisione artefatos da AWS

Tarefa	Descrição	Habilidades necessárias
Gere artefatos de implantação da AWS na máquina do operador.	Para gerar artefatos de implantação, execute o comando a seguir. `sudo app2container generate app-deployment --application-id <application id>` Isso gera o CloudFormation modelo `ecs-master.yml` da AWS no espaço de trabalho.	DevOps
Provisionar os artefatos.	Para provisionar ainda mais os artefatos gerados, implante o CloudFormation modelo da	DevOps

Tarefa	Descrição	Habilidades necessárias
	AWS executando o comando a seguir. `aws cloudformation deploy --template-file <path to ecs-master.yml> --capabilities CAPABILITY_NAMED_IAM --stack-name <application id>-ECS`	
Gere o pipeline.	Modifique `pipeline.json` , que foi criada na história anterior, com base nas suas necessidades. Em seguida, execute o `generate pipeline` comando para gerar os artefatos de implantação do pipeline.	DevOps

Recursos relacionados

- O que é o App2Container?
- Publicação no blog do AWS App2Container
- Princípios básicos da configuração da AWS CLI
- Noções básicas do Docker para Amazon ECS
- Comandos do Docker

Migrar sistemas de arquivos compartilhados em uma grande migração da AWS

Criado por Amit Rudraraju (AWS), Sam Apa (AWS), Bheemeswararao Balla (AWS), Wally Lu (AWS) e Sanjeev Prakasam (AWS)

Resumo

A migração de 300 ou mais servidores é considerada uma grande migração. O objetivo de uma grande migração é migrar workloads de seus datacenters on-premises existentes para a Nuvem AWS, e esses projetos geralmente se concentram em workloads de aplicativos e bancos de dados. No entanto, os sistemas de arquivos compartilhados exigem atenção concentrada e um plano de migração separado. Este padrão descreve o processo de migração para sistemas de arquivos compartilhados e fornece as práticas recomendadas para migrá-los com êxito como parte de um grande projeto de migração.

Um sistema de arquivos compartilhado (SFS), também conhecido como sistema de arquivos em rede ou cluster, é um compartilhamento de arquivos montado em vários servidores. Os sistemas de arquivos compartilhados são acessados por meio de protocolos como Network File System (NFS), Common Internet File System (CIFS) ou Server Message Block (SMB).

Esses sistemas não são migrados com ferramentas de migração padrão, como o AWS Application Migration Service, porque não são dedicados ao host que está sendo migrado nem são representados como um dispositivo de blocos. Embora a maioria das dependências do host seja migrada de forma transparente, a coordenação e o gerenciamento dos sistemas de arquivos dependentes devem ser tratados separadamente.

Você migra sistemas de arquivos compartilhados nas seguintes fases: descobrir, planejar, preparar, substituir e validar. Usando esse padrão e as pastas de trabalho anexadas, você migra seu sistema de arquivos compartilhado para um serviço de armazenamento da AWS, como Amazon Elastic File System (Amazon EFS), Amazon FSx for NetApp ONTAP ou Amazon FSx for Windows File Server. Para transferir o sistema de arquivos, você pode usar a AWS DataSync ou uma ferramenta de terceiros, como NetApp SnapMirror.

> **Note**
>
> Esse padrão faz parte de uma série de orientação prescritiva da AWS sobre grandes migrações para a nuvem da AWS. Esse padrão inclui as melhores práticas e instruções para SFSs incorporação em seus planos de ondas para servidores. Se você estiver

migrando um ou mais sistemas de arquivos compartilhados fora de um grande projeto de migração, consulte as instruções de transferência de dados na documentação da AWS para Amazon EFS, Amazon FSx para Windows File Server e Amazon FSx para NetApp ONTAP.

Pré-requisitos e limitações

Pré-requisitos

Os pré-requisitos podem variar dependendo dos sistemas de arquivos compartilhados de origem e destino e do seu caso de uso. Os problemas mais comuns são os seguintes:

- Uma conta AWS ativa
- Você concluiu a descoberta do portfólio de aplicativos para seu grande projeto de migração e começou a desenvolver planos de ondas. Para obter mais informações, consulte o Manual de portfólio para grandes migrações da AWS.
- Nuvens privadas virtuais (VPCs) e grupos de segurança que permitem tráfego de entrada e saída entre o datacenter local e seu ambiente da AWS. Para obter mais informações, consulte as opções de conectividade da Network-to-Amazon VPC e os requisitos de DataSync rede da AWS.
- Permissões para criar CloudFormation pilhas da AWS ou permissões para criar FSx recursos do Amazon EFS ou da Amazon. Para obter mais informações, consulte a CloudFormation documentação, a documentação do Amazon EFS ou a FSx documentação da Amazon.
- Se você estiver usando DataSync a AWS para realizar a migração, precisará das seguintes permissões:
  - Permissões para DataSync a AWS enviar registros para um grupo de CloudWatch registros do AWS Logs. Para obter mais informações, consulte Permitir DataSync o upload de registros para grupos de CloudWatch registros.
  - Permissões para acessar o grupo CloudWatch de registros de registros. Para obter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos seus recursos do CloudWatch Logs.
  - Permissões para criar agentes e tarefas em DataSync. Para obter mais informações, consulte Permissões obrigatórias do IAM para usar a AWS DataSync.

Limitações

- Esse padrão foi projetado para migrar SFSs como parte de um grande projeto de migração. Ele inclui as melhores práticas e instruções para SFSs incorporação em seus planos de migração de aplicativos. Se você estiver migrando um ou mais sistemas de arquivos compartilhados fora de um grande projeto de migração, consulte as instruções de transferência de dados na documentação da AWS para Amazon EFS, Amazon FSx para Windows File Server e Amazon FSx para NetApp ONTAP.
- Esse padrão é baseado em arquiteturas, serviços e padrões de migração comumente usados. No entanto, grandes projetos e estratégias de migração podem variar entre as organizações. Talvez seja necessário personalizar essa solução ou as pastas de trabalho fornecidas com base em seus requisitos.

Arquitetura

Pilha de tecnologia de origem

Um ou mais itens a seguir:

- Servidor de arquivos Linux (NFS)
- Servidor de arquivos Windows (SMB)
- NetApp matriz de armazenamento
- Matriz de armazenamento Dell EMC Isilon

Pilha de tecnologias de destino

Um ou mais itens a seguir:

- Amazon Elastic File System
- Amazon FSx para NetApp ONTAP
- Servidor FSx de arquivos Amazon para Windows

Arquitetura de destino

O diagrama mostra o seguinte processo:

1. Você estabelece uma conexão entre o datacenter local e a nuvem da AWS usando um serviço da AWS, como o AWS Direct Connect ou o AWS Site-to-Site VPN.

2. Você instala o DataSync agente no data center local.
3. De acordo com seu plano wave, você usa DataSync para replicar dados do sistema de arquivos compartilhado de origem para o compartilhamento de arquivos da AWS de destino.

Fases de migração

A imagem a seguir mostra as fases e etapas de alto nível para migrar um SFS em um grande projeto de migração.

A seção Épicos desse padrão contém instruções detalhadas sobre como concluir a migração e usar as pastas de trabalho anexadas. Veja a seguir uma visão geral de alto nível das etapas dessa abordagem em fases.

Phase (Fase)	Etapas
Descobrir	1. Usando uma ferramenta de descoberta, você coleta dados sobre o sistema de arquivos compartilhado, incluindo servidores, pontos de montagem e endereços IP. 2. Usando um banco de dados de gerenciam ento de configuração (CMDB) ou sua ferrament a de migração, você coleta detalhes sobre o servidor, incluindo informações sobre a onda de migração, ambiente, proprietário do aplicativ o, nome do serviço de gerenciamento de serviços de TI (ITSM), unidade organizacional e ID do aplicativo.
Planejar	3. Usando as informações coletadas sobre os servidores SFSs e os servidores, crie o plano de ondas do SFS. 4. Usando as informações na planilha de criação, para cada SFS, escolha um serviço de destino da AWS e uma ferramenta de migração.

Preparar	5. Configure a infraestrutura de destino no Amazon EFS, Amazon FSx for NetApp ONTAP ou Amazon FSx for Windows File Server. 6. Configure o serviço de transferência de dados, como DataSync, e inicie a sincroniz ação inicial de dados. Quando a sincronização inicial estiver concluída, você poderá configura r sincronizações recorrentes para serem executadas de acordo com uma programação. 7. Atualize o plano SFS em ondas com informações sobre o compartilhamento de arquivos de destino, como endereço IP ou caminho.
Substituir	8. Interrompa os aplicativos que acessam ativamente o SFS de origem. 9. No serviço de transferência de dados, execute uma sincronização final de dados. 10. Quando a sincronização estiver concluída , verifique se ela foi totalmente bem-sucedida revisando os dados de registro em CloudWatch Registros.
Validar	11. Nos servidores, altere o ponto de montagem para o novo caminho do SFS. 12. Reinicie e valide os aplicativos.

Ferramentas

Serviços da AWS

- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas, aplicativos e serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.

- DataSyncA AWS é um serviço on-line de transferência e descoberta de dados que ajuda você a mover arquivos ou dados de objetos de, para e entre os serviços de armazenamento da AWS.
- Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS.
- FSxA Amazon fornece sistemas de arquivos que suportam protocolos de conectividade padrão do setor e oferecem alta disponibilidade e replicação em todas as regiões da AWS.

Outras ferramentas

- SnapMirroré uma ferramenta de replicação de NetApp dados que replica dados de volumes de origem ou qtrees especificados para volumes ou qtrees de destino, respectivamente. Você pode usar essa ferramenta para migrar um sistema de arquivos de NetApp origem para a Amazon FSx for ONTAP.
- Robocopy, abreviação de Robust File Copy, é um diretório de linha de comando e comando para Windows. Você pode usar essa ferramenta para migrar um sistema de arquivos de origem do Windows para o Amazon FSx for Windows File Server.

Práticas recomendadas

Abordagens de planejamento de ondas

Ao planejar ondas para seu grande projeto de migração, considere a latência e o desempenho do aplicativo. Quando o SFS e os aplicativos dependentes estão operando em locais diferentes, como um na nuvem e outro no datacenter on-premises, isso pode aumentar a latência e afetar o desempenho do aplicativo. Veja a seguir as opções disponíveis ao criar planos de onda:

1. Migrar o SFS e todos os servidores dependentes na mesma onda: essa abordagem evita problemas de desempenho e minimiza o retrabalho, como reconfigurar pontos de montagem várias vezes. É recomendado quando é necessária uma latência muito baixa entre o aplicativo e o SFS. No entanto, o planejamento de ondas é complexo e o objetivo geralmente é remover variáveis dos agrupamentos de dependências, não as adicionar. Além disso, essa abordagem não é recomendada se muitos servidores acessarem o mesmo SFS, pois isso torna a onda muito grande.
2. Migrar o SFS após a migração do último servidor dependente: por exemplo, se um SFS for acessado por vários servidores e esses servidores estiverem programados para migrar nas ondas 4, 6 e 7, programe o SFS para migrar na onda 7.

Essa abordagem geralmente é a mais lógica para grandes migrações e é recomendada para aplicativos sensíveis à latência. Ela reduz os custos associados à transferência de dados. Também minimiza o período de latência entre o SFS e os aplicativos de nível superior (como produção) porque os aplicativos de nível superior geralmente são programados para serem migrados por último, após o desenvolvimento e os aplicativos de controle de qualidade.

No entanto, essa abordagem ainda exige descoberta, planejamento e agilidade. Talvez seja necessário migrar o SFS em uma onda anterior. Confirme se os aplicativos podem suportar a latência adicional pelo período de tempo entre a primeira onda dependente e a onda contendo o SFS. Conduza uma sessão de descoberta com os proprietários do aplicativo e migre o aplicativo na mesma onda para o aplicativo mais sensível à latência. Se forem descobertos problemas de desempenho após a migração de um aplicativo dependente, esteja preparado para migrar rapidamente o SFS o mais rápido possível.

3. Migrar o SFS no final de um grande projeto de migração: essa abordagem é recomendada se a latência não for um fator, como quando os dados no SFS são acessados com pouca frequência ou não são essenciais para o desempenho do aplicativo. Essa abordagem agiliza a migração e simplifica as tarefas de substituição.

Você pode combinar essas abordagens com base na sensibilidade à latência do aplicativo. Por exemplo, você pode migrar de forma sensível à latência SFSs usando as abordagens 1 ou 2 e, em seguida, migrar o restante usando a abordagem 3. SFSs

Escolha de um serviço de sistema de arquivos da AWS

A AWS oferece vários serviços em nuvem para armazenamento de arquivos. Cada um oferece benefícios e limitações diferentes para desempenho, escala, acessibilidade, integração, conformidade e otimização de custos. Há algumas opções lógicas padrão. Por exemplo, se seu sistema de arquivos local atual estiver operando o Windows Server, o Amazon FSx for Windows File Server é a opção padrão. Ou se o sistema de arquivos local estiver operando o NetApp ONTAP, o Amazon FSx for NetApp ONTAP é a opção padrão. No entanto, você pode escolher um serviço de destino com base nos requisitos do seu aplicativo ou para obter outros benefícios operacionais na nuvem. Para obter mais informações, consulte Escolher o serviço de armazenamento de arquivos da AWS certo para sua implantação (apresentação do AWS Summit).

Escolher uma ferramenta de migração

O Amazon EFS e a Amazon FSx oferecem suporte ao uso da AWS DataSync para migrar sistemas de arquivos compartilhados para a nuvem da AWS. Para obter mais informações sobre sistemas e serviços de armazenamento compatíveis, benefícios e casos de uso, consulte O que é a AWS DataSync. Para uma visão geral do processo de uso DataSync para transferir seus arquivos, consulte Como funcionam as DataSync transferências da AWS.

Também há várias ferramentas de terceiros disponíveis, incluindo as seguintes:

- Se você escolher a Amazon FSx para NetApp ONTAP, poderá usá-la NetApp SnapMirror para migrar os arquivos do data center local para a nuvem. SnapMirror usa replicação em nível de bloco, que pode ser mais rápida DataSync e reduzir a duração do processo de transferência de dados. Para obter mais informações, consulte Migrando FSx para o uso do ONTAP. NetApp SnapMirror
- Se você escolher o Amazon FSx para Windows File Server, poderá usar o Robocopy para migrar arquivos para a nuvem. Para obter mais informações, consulte Migração de arquivos existentes FSx para o Windows File Server usando o Robocopy.

Épicos

Descobrir

Tarefa	Descrição	Habilidades necessárias
Preparar a pasta de trabalho de descoberta do SFS.	1. Baixe as pastas de trabalho na seção Anexos deste padrão. Elas contêm dois arquivos, SFS-Discovery-Workbook.xlsx e SFS-Wave-Plan-Workbook.xlsx. 2. Abra o arquivo SFS-Discovery-Workbook no Microsoft Excel. 3. Na planilha Painel, faça o seguinte: • Na coluna A, atualize o nome do ambiente.	Engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	• Na coluna B, atualize a ordem dos ambientes para colocá-los na ordem da menor (1) prioridade para a maior prioridade. • Nas colunas D-E, atualize a programação das ondas. • Nas colunas C e K, atualize os nomes das contas da AWS. • Na coluna L, atualize a VPC IDs. • Nas colunas M—O, atualize a sub-rede. IDs 4. Revise o restante do modelo de pasta de trabalho e atualize todos os outros valores necessários para sua organização ou caso de uso. 5. Salvar a pasta de trabalho.	

Tarefa	Descrição	Habilidades necessárias
Coletar informações sobre o SFS de origem.	1. Usando sua ferramenta de descoberta preferida , identifique todas as montagens do SFS em todos os dispositivos de armazenamento, servidores Linux e servidores Windows aplicáveis. Normalmente, você precisa coletar as seguintes informações: • Dispositivos cliente • Endereço IP do cliente • Detalhes do SFS • Ponto de montagem **Note** Você pode adicionar detalhes do ponto de montagem ao seu runbook de migração para remontar o SFS após a migração. 2. Abra o arquivo SFS-Discovery-Workbook. 3. Na planilha Wave-Sheet, faça o seguinte: • Na coluna Localização do servidor (D), na fórmula, confirme se o formato do intervalo CIDR da fonte	Engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	on-premises funciona para o seu intervalo. Por exemplo, se seu intervalo de CIDR for `10.0.0.0/8` , insira `10.*.*.*`. • Na coluna Localização do SFS (E), na fórmula, confirme se o formato do intervalo CIDR do VPC de destino funciona para o seu intervalo. Por exemplo, se seu intervalo de CIDR for `176.16.0.0/16` , insira `176.16.*.*` . 4. Na planilha SFS-Data, faça o seguinte: • Na coluna Nome do servidor (A), insira o nome do servidor em que o SFS está montado. • Na coluna SFS path (B), insira o nome do SFS. • Na coluna Endereço IP (C), insira o endereço IP do servidor. • Adicione qualquer outra informação relevante que você coletou durante a descoberta, como o ponto de montagem e o tamanho do SFS. Você pode usar esses dados posteriormente para	

Tarefa	Descrição	Habilidades necessárias
	modificar os cálculos de planejamento de ondas. 5. Salvar a pasta de trabalho.	

Tarefa	Descrição	Habilidades necessárias
Coletar informações sobre os servidores.	1. Usando seu CMDB ou os registros de registro de dados em sua ferrament a de migração, identifiq ue todas as informações a seguir sobre os servidores que têm montagens SFS: • Nome do servidor • Endereço IP • Onda • Unidade organizacional (UO) • Ambiente de servidor, como `DEV`, `QA`, ou `PROD` • Nome do aplicativo • Proprietário do aplicativo e informações de contato 2. Abra o arquivo SFS-Disco very-Workbook. 3. Na planilha Server-Data, nas colunas A-H, insira as informações que você coletou sobre os servidore s de origem. Observe o seguinte: • Na coluna Onda # (C), insira o nome da onda (como `Wave1`), out-of-sc ope (00S) ou `Retire`. • Se a coluna de Contato do proprietário do aplicativo (H) for exibida,	Engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	verifique se o endereço de e-mail está correto. Esse endereço de e-mail é gerado automatic amente com base no nome que você forneceu na coluna Proprietário do aplicativo (G). Se necessário, atualize manualmente o valor para refletir o endereço de e-mail correto. • Não modifique as colunas I-J, que contêm fórmulas. 4. Salvar a pasta de trabalho.	

Planejar

Tarefa	Descrição	Habilidades necessárias
Criar o plano de ondas do SFS.	1. Abra o arquivo SFS-Disco very-Workbook. 2. Verifique se todas as informações coletadas na fase de descoberta são precisas e atuais. 3. Na planilha Wave-Shee t, filtre a coluna Onda do SFS (K) no valor 1. Esta é uma lista de tudo SFSs na primeira onda.	Líder de construção, líder de substituição, engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	Note Um valor de `0` nesta coluna indica que o SFS está fora do escopo da migração. Isso pode ser porque o SFS já está hospedado na AWS ou porque os servidores que acessam o compartil hamento estão fora do escopo da migração. 4. Verifique se você deseja migrá-los SFSs nessa onda. Para obter mais informações sobre como SFSs atribuir ondas, consulte Abordagens de planejamento de ondas na seção Melhores práticas. 5. Selecione e copie as células que contêm os valores filtrados. Não copie a linha do cabeçalho que contém os títulos das colunas. 6. Abra o arquivo SFS-Wave-Plan-Workbook que você baixou anteriormente.	

Tarefa	Descrição	Habilidades necessárias
	7. Na planilha Export-from-Discovery, selecione a célula A2. 8. Cole os dados copiados. 9. Salve os arquivos SFS-Discovery-Workbook e SFS-Wave-Plan-Workbook.	

Tarefa	Descrição	Habilidades necessárias
Escolha o serviço e a ferramenta de migração da AWS de destino.	1. No SFS-Wave-Plan-Work book arquivo, na Exported-from-Discovery planilha, selecione e copie os valores na coluna Caminho antigo (C). 2. Na planilha Build-Wave, selecione a célula A2. 3. Cole os dados copiados. As colunas B-M nessa planilha são atualizadas automatic amente para refletir outros dados associados a esse caminho. 4. Remova quaisquer valores duplicados na coluna A. Para obter instruçõe s, consulte Remover valores duplicados (site do Microsoft Support). 5. Na coluna Padrão ou serviço de destino (F), analise o serviço de destino recomendado da AWS e atualize conforme necessário. Para obter mais informações, consulte Escolha de um serviço de sistema de arquivos da AWS na seção Práticas recomendadas desse padrão.	Engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	6. Na coluna Método de migração (G), revise a ferramenta de migração recomendada e atualize conforme necessário. Para obter mais informações, consulte Escolha de uma ferramenta de migração na seção Práticas recomendadas desse padrão. 7. Salve o arquivo SFS-Discovery-Workbook. Você terminou de criar um plano de onda para essa onda. 8. Repita essas instruções para preparar um plano de onda para cada onda. Como os planos de ondas estão sujeitos a alterações durante a migração, recomendamos que você planeje com no máximo 5 ondas de antecedência.	

Preparar

Tarefa	Descrição	Habilidades necessárias
Configurar o sistema de arquivos de destino.	De acordo com os detalhes registrados em seu plano de ondas, configure os sistemas de arquivos de destino na conta da AWS, na VPC e nas sub-redes de destino. Para	Engenheiro de migração, líder de migração, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	obter instruções, consulte a seguinte documentação do AWS: • Amazon EFS • Amazon FSx para NetApp ONTAP • Servidor FSx de arquivos Amazon para Windows	

Tarefa	Descrição	Habilidades necessárias
Configurar a ferramenta de migração e transfira dados.	1. Se você estiver usando a AWS DataSync, configure o registro em log para DataSync tarefas. Para obter instruções, consulte Registrar suas atividades de DataSync tarefas na AWS. 2. Configure a ferramenta de migração e realize uma transferência inicial de dados de acordo com as instruções da ferramenta selecionada: • Para o Amazon EFS, consulte o seguinte: • Transferir arquivos para o Amazon EFS usando a AWS DataSync • Para Amazon FSx for ONTAP, veja o seguinte: • Migrando FSx para o ONTAP usando NetApp SnapMirror • Migração FSx para o ONTAP usando a AWS DataSync • Para o Amazon FSx para Windows File Server, consulte o seguinte: • Migração de arquivos existentes FSx para	Administrador da AWS, administrador de nuvem, engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	o Windows File Server usando a AWS DataSync • Migrando arquivos existentes FSx para o Windows File Server usando o Robocopy 3. Alterações no SFS de origem podem ocorrer durante ou após a transferência inicial. Configure transferências de dados recorrentes entre os sistemas de arquivos de origem e de destino para manter os dados sincronizados: • Se você estiver usando DataSync, consulte Programação de sua DataSync tarefa da AWS. DataSync transfere somente os arquivos modificados ou novos no SFS de origem. • Se você estiver usando uma ferramenta de terceiros, consulte a documentação da ferramenta selecionada.	

Tarefa	Descrição	Habilidades necessárias
Atualizar o plano de ondas.	1. Abra o arquivo SFS-Wave-Plan-Workbook para a onda atual. 2. Na planilha Build-Wave, na coluna Novo endereço IP de caminho (N), insira o endereço IP do sistema de arquivos de destino. Siga um destes procedimentos para localizar o endereço IP: • FSx Para Windows File Server, no FSx console da Amazon, escolha Sistemas de arquivos, escolha seu sistema de arquivos e, em seguida, veja a seção Rede e Segurança. • FSx Para ONTAP, consulte Montagem de volumes. • Para o Amazon EFS, consulte Montagem com um endereço IP. 3. Na coluna Novo caminho (O), insira o novo caminho de montagem. O caminho de montagem é o nome DNS do sistema de arquivos. Siga um destes procedimentos para	Engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	localizar o caminho de montagem: • FSx Para Windows File Server, no FSx console da Amazon, escolha Sistemas de arquivos, escolha seu sistema de arquivos e, em seguida, escolha Anexar. • FSx Para o ONTAP, consulte a página de detalhes do sistema de arquivos. Para obter instruções, consulte Montagem de volumes. • Para o Amazon EFS, consulte Obter mais informações. 4. Na planilha de Resumo da remontagem, confirme se as colunas Novo caminho (C) e Endereço IP do novo caminho (D) refletem os valores atualizados. 5. Confirme se sua organizaç ão preparou runbooks para remontar os sistemas de arquivos Linux e Windows após a substituição. Para obter instruções gerais, consulte o seguinte: • Montagem de sistemas de arquivos do EFS	

Tarefa	Descrição	Habilidades necessárias
	• Acesso FSx aos compartilhamentos de arquivos do Windows File Server • Montagem FSx para volumes ONTAP 6. Se algum servidor dependente não estiver incluído nessa onda, registre-o na planilha App-Team-Communication. Informe os respectivos proprietários de aplicativos ou servidores, pois eles podem não estar incluídos nas comunicações padrão de ondas. 7. Se SFSs forem removidos da onda após concluir o plano de onda, rastreie-os na planilha Descoped.	

Substituir

Tarefa	Descrição	Habilidades necessárias
Interromper aplicativos.	Se aplicativos ou clientes estiverem executando ativamente operações de leitura e gravação no SFS de origem, interrompa-as antes de realizar a sincronização final dos dados. Para	Proprietário do aplicativo, desenvolvedor do aplicativo

Tarefa	Descrição	Habilidades necessárias
	obter instruções, consulte a documentação do aplicativo ou seus processos internos para interromper as atividades de leitura e gravação. Por exemplo, consulte Iniciar ou interromper o servidor Web (IIS 8) (documentação da Microsoft) ou Gerenciar serviços do sistema com systemctl (documentação da Red Hat).	
Executar a transferência final de dados.	1. Na ferramenta de migração, execute manualmente uma tarefa ou trabalho final de transferência de dados para sincronizar o sistema de arquivos de destino com o SFS de origem. Para obter instruções, consulte Iniciando sua DataSync tarefa ou consulte a documentação da ferramenta de migração terceirizada selecionada. 2. Aguarde a conclusão da transferência de dados. Para obter mais informações, consulte AWS Monitorando a DataSync atividade da AWS com a Amazon CloudWatch e Monitorando sua DataSync tarefa na linha de comando.	Engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
Validar a transferência de dados.	Se você estiver usando a AWS DataSync, faça o seguinte para validar a transferência final de dados concluída com sucesso: 1. No DataSync console da AWS, anote o ID da tarefa e da execução, como `task-0000-exec-1111` . 2. Navegue até a seção Registro de DataSync Tarefas da tarefa. 3. Escolha o link do grupo de CloudWatch registros. 4. Nos logs, pesquise o ID da tarefa e da execução. 5. Anote quaisquer erros de transferência. Para obter mais informações, consulte Erros comuns na DataSync documentação. 6. Valide o seguinte: • Compare as listas de arquivos da origem e do destino SFSs para confirmar que todos os dados foram transferidos • Compare as permissões de acesso ao arquivo entre a origem e o destino SFSs.	Engenheiro de migração, líder de migração

Tarefa	Descrição	Habilidades necessárias
	Se você estiver usando uma ferramenta de terceiros, consulte as instruções de validação da transferência de dados na documentação da ferramenta de migração selecionada.	

Validar

Tarefa	Descrição	Habilidades necessárias
Remonte o sistema de arquivos e valide a função e o desempenho do aplicativo.	1. Se os servidores dependentes foram migrados nessa onda, no arquivo SFS-Wave-Plan-Workbook, na planilha Remount-Summary, insira o novo endereço IP do servidor na coluna Novo endereço IP do servidor (F). 2. Em todos os servidores, atualize o ponto de montagem do sistema de arquivos do caminho antigo para o novo. Use o runbook da sua organização para remontagem, discutido anteriormente na fase de Preparação. 3. Confirme se o sistema de arquivos está montado corretamente e está acessível verificando as	Administrador de sistemas da AWS, proprietário do aplicativos

Tarefa	Descrição	Habilidades necessárias
	montagens e verificando se os arquivos estão presentes . A equipe de infraestrutura normalmente realiza essas atividades. 4. Reinicie os aplicativos e envolva os proprietários do aplicativo ou a equipe de controle de qualidade para concluir os testes funcionais e de desempenho do aplicativo, conforme necessário para o aplicativo.	

Solução de problemas

Problema	Solução
Os valores das células no Microsoft Excel não são atualizados.	Copie as fórmulas nas linhas de amostra arrastando a alça de preenchimento. Para obter mais informações, consulte as instruções para Windows ou Mac (site de suporte da Microsoft).

Recursos relacionados

Documentação da AWS

- DataSync Documentação da AWS
- Documentação do Amazon EFS
- FSx Documentação da Amazon
- Grandes migrações para a Nuvem AWS

- Guia para grandes migrações da AWS
- Manual do portfólio para grandes migrações da AWS

Solução de problemas

- Solução de DataSync problemas da AWS
- Solução de problemas do Amazon EFS
- Solução de problemas do Amazon FSx para Windows File Server
- Solução de problemas da Amazon FSx para NetApp ONTAP

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Migre um banco de dados Oracle para o Amazon RDS for Oracle usando adaptadores de arquivo simples GoldenGate Oracle

Criado por Dhairya Jindani (AWS) e Baji Shaik (AWS)

Resumo

GoldenGate O Oracle é um serviço de captura e replicação de dados em tempo real para bancos de dados e ambientes de TI heterogêneos. No entanto, esse serviço não é compatível atualmente com o Amazon Relational Database Service (Amazon RDS) para Oracle. Para obter uma lista dos bancos de dados compatíveis, consulte Oracle GoldenGate for Heterogeneous Databases (documentação da Oracle). Esse padrão descreve como usar os adaptadores de arquivo GoldenGate simples Oracle GoldenGate e Oracle para gerar arquivos simples do banco de dados Oracle de origem, que pode estar no local ou em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Em seguida, você pode importar esses arquivos simples para uma instância de banco de dados Amazon RDS para Oracle.

Nesse padrão, você usa o Oracle GoldenGate para extrair os arquivos de trilha do seu banco de dados Oracle de origem. A bomba de dados copia os arquivos de trilha para um servidor de integração, que é uma EC2 instância da Amazon. No servidor de integração, a Oracle GoldenGate usa o adaptador de arquivo simples para gerar uma série de arquivos simples sequenciais com base na captura de dados transacionais dos arquivos de trilha. O Oracle GoldenGate formata os dados como valores separados por delimitador ou valores delimitados por comprimento. Em seguida, você usa o Oracle SQL*Loader para importar os arquivos simples para a instância de banco de dados de destino do Amazon RDS para Oracle.

Público-alvo

Esse padrão é destinado para aqueles que têm experiência e conhecimento dos blocos de construção fundamentais GoldenGate de um Oracle. Para obter mais informações, consulte Visão geral da GoldenGate arquitetura Oracle (documentação da Oracle).

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Uma GoldenGate licença Oracle.
- Uma licença separada para um GoldenGate adaptador Oracle.

- Um banco de dados Oracle de origem, executado localmente ou em uma EC2 instância da Amazon.
- Uma instância Amazon EC2 Linux usada como servidor de integração. Para obter mais informações, consulte Comece a usar instâncias do Amazon EC2 Linux (EC2 documentação da Amazon).
- Uma instância de destino do banco de dados do Amazon RDS para Oracle. Para obter mais informações, consulte Criação de uma instância de banco de dados Oracle (documentação do Amazon RDS).

Versões do produto

- Oracle Database Enterprise Edition versão 10g, 11g, 12c ou superior
- Oracle GoldenGate versão 12.2.0.1.1 ou posterior

Arquitetura

Pilha de tecnologia de origem

Um banco de dados Oracle (no local ou em uma EC2 instância da Amazon)

Pilha de tecnologias de destino

Amazon RDS para Oracle

Arquitetura de origem e destino

1. O Oracle GoldenGate extrai trilhas dos registros do banco de dados de origem.
2. O data pump extrai as trilhas e as migra para um servidor de integração.
3. O adaptador de arquivo GoldenGate simples Oracle lê as trilhas, as definições de origem e os parâmetros de extração.
4. Você sai da extração, que gera um arquivo de controle e arquivos de dados simples.
5. Você migra os arquivos de dados simples para uma instância de banco de dados Amazon RDS for Oracle no. Nuvem AWS

Ferramentas

Serviços da AWS

- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Relational Database Service (Amazon RDS) para Oracle ajuda você a configurar, operar e escalar um banco de dados relacional Oracle no. Nuvem AWS

Outros serviços

- GoldenGateO Oracle é um serviço que ajuda você a replicar, filtrar e transformar dados de um banco de dados em outro banco de dados heterogêneo ou em outra topologia de destino, como arquivos simples.
- Os adaptadores de GoldenGate aplicativos Oracle permitem GoldenGate que a Oracle produza uma série de arquivos simples sequenciais e arquivos de controle a partir de dados transacionais capturados nos arquivos de trilha de um banco de dados de origem. Esses adaptadores são amplamente usados para operações de extração, transformação e carregamento (ETL) em aplicativos de data warehouse e aplicativos proprietários ou legados. GoldenGate A Oracle realiza essa captura e a aplica quase em tempo real em bancos de dados, plataformas e sistemas operacionais heterogêneos. Os adaptadores suportam formatos diferentes para os arquivos de saída, como CSV ou Apache Parquet. Você pode carregar esses arquivos gerados para carregar os dados em diferentes bancos de dados heterogêneos.

Épicos

Configurar o Oracle GoldenGate no servidor de banco de dados de origem

Tarefa	Descrição	Habilidades necessárias
Baixe o Oracle GoldenGate.	No servidor do banco de dados de origem, baixe o Oracle GoldenGate versão 12.2.0.1.1 ou posterior. Para obter instruções, consulte Fazendo o download do Oracle GoldenGate (document ação da Oracle).	DBA

Tarefa	Descrição	Habilidades necessárias
Instale o Oracle GoldenGate.	Para obter instruções, consulte Instalando o Oracle GoldenGate (documentação da Oracle).	DBA
Configure o Oracle GoldenGate.	Para obter instruções, consulte Preparando o banco de dados para Oracle GoldenGate (documentação da Oracle).	DBA

Configure o Oracle GoldenGate no servidor de integração

Tarefa	Descrição	Habilidades necessárias
Baixe o Oracle GoldenGate.	No servidor de integração, baixe o Oracle GoldenGate versão 12.2.0.1.1 ou posterior. Para obter instruções, consulte Fazendo o download do Oracle GoldenGate (documentação da Oracle).	DBA
Instale o Oracle GoldenGate.	Crie diretórios, configure o processo do gerenciador e crie o arquivo `defgen` para um ambiente heterogêneo. Para obter instruções, consulte Instalando o Oracle GoldenGate (documentação da Oracle).	DBA

Alterar a configuração de captura GoldenGate de dados do Oracle

Tarefa	Descrição	Habilidades necessárias
Prepare os GoldenGate adaptadores Oracle.	No servidor de integração, configure o software do GoldenGate adaptador Oracle. Faça o seguinte: 1. No Oracle Software Delivery Cloud, baixe o ggs_Adapters_Linux_x64.zip. 2. Descompacte o ggs_Adapters_Linux_x64.zip. 3. Execute o comando a seguir para instalar os adaptadores: `tar -xvf ggs_Adapters_Linux_x64.tar`	DBA
Configure a data pump.	No servidor de origem, configure o data pump para transferir o arquivo de trilha do servidor de origem para o servidor de integração. Crie o arquivo de parâmetros do data pump e o diretório do arquivo de trilhas. Para obter instruções, consulte Configurando o adaptador de arquivo simples (documentação da Oracle).	DBA

Gere e migre os arquivos simples

Tarefa	Descrição	Habilidades necessárias
Gere os arquivos simples.	Crie o arquivo de extração e o arquivo de controle e, em seguida, inicie o processo de extração no servidor de integração. Isso extrai as alterações do banco de dados e grava o banco de dados de origem nos arquivos simples. Para obter instruções, consulte Usando o adaptador de arquivo simples (documentação da Oracle).	DBA
Carregue os arquivos simples no banco de dados de destino.	Carregue os arquivos simples na instância de destino do banco de dados do Amazon RDS para Oracle. Para obter mais informações, consulte Importação usando o Oracle SQL*Loader (documentação do Amazon RDS).	DBA

Solução de problemas

Problema	Solução
O adaptador de arquivo GoldenGate simples Oracle gera um erro.	Para obter uma descrição dos erros do adaptador, consulte Localizar mensagens de erro (documentação da Oracle). Para obter instruções de solução de problemas, consulte Solução de problemas do adaptador de arquivo simples (documentação da Oracle).

Recursos relacionados

- Instalando o Oracle GoldenGate (documentação da Oracle)
- Configurando o Oracle GoldenGate (documentação da Oracle)
- Compreendendo GoldenGate os adaptadores Oracle (documentação da Oracle)
- Configurando o adaptador de arquivo simples (documentação da Oracle)

Altere os aplicativos Python e Perl para oferecer suporte à migração do banco de dados do Microsoft SQL Server para o Amazon Aurora Edição Compatível com PostgreSQL

Criado por Dwarika Patra (AWS) e Deepesh Jayaprakash (AWS)

Resumo

Esse padrão descreve as alterações nos repositórios de aplicativos que podem ser necessárias quando você migra bancos de dados do Microsoft SQL Server para o Amazon Aurora Edição Compatível com PostgreSQL. O padrão pressupõe que esses aplicativos sejam baseados em Python ou em Perl e fornece instruções separadas para essas linguagens de script.

A migração de bancos de dados do SQL Server para o Aurora compatível com PostgreSQL envolve conversão de esquemas, conversão de objetos de banco de dados, migração de dados e carregamento de dados. Devido às diferenças entre o PostgreSQL e o SQL Server (relacionadas a tipos de dados, objetos de conexão, sintaxe e lógica), a tarefa de migração mais difícil envolve fazer as alterações necessárias na base de código para que ela funcione corretamente com o PostgreSQL.

Em um aplicativo baseado em Python, objetos e classes de conexão estão espalhados por todo o sistema. Além disso, a base de código do Python pode usar várias bibliotecas para se conectar ao banco de dados. Se a interface de conexão do banco de dados mudar, os objetos que executam as consultas em linha do aplicativo também precisarão de alterações.

Em um aplicativo baseado em Perl, as alterações envolvem objetos de conexão, drivers de conexão de banco de dados, instruções SQL em linha estáticas e dinâmicas e como o aplicativo lida com consultas dinâmicas complexas de DML e conjuntos de resultados.

Ao migrar seu aplicativo, você também pode considerar possíveis melhorias na AWS, como a substituição do servidor FTP pelo acesso ao Amazon Simple Storage Service (Amazon S3).

O processo de migração de aplicativos envolve os seguintes desafios:

- Objetos de conexão. Se os objetos de conexão estiverem espalhados no código com várias bibliotecas e chamadas de função, talvez seja necessário encontrar uma maneira generalizada de alterá-los para oferecer suporte ao PostgreSQL.
- Tratamento de erros ou exceções durante a recuperação ou atualizações de registros. Se você tiver operações condicionais de criação, leitura, atualização e exclusão (CRUD) no banco de dados que retornam variáveis, conjuntos de resultados ou data frames, quaisquer erros

ou exceções podem resultar em erros de aplicativo com efeitos em cascata. Eles devem ser tratados com cuidado, com validações adequadas e pontos de economia. Um desses pontos de salvamento é chamar grandes consultas SQL em linha ou objetos de banco de dados dentro de blocos `BEGIN...EXCEPTION...END`.

- Controle de transações e sua validação. Isso inclui confirmações e reversões manuais e automáticas. O driver do PostgreSQL para Perl exige que você sempre defina explicitamente o atributo de confirmação automática.
- Tratamento de consultas SQL dinâmicas. Isso requer uma forte compreensão da lógica de consulta e testes iterativos para garantir que as consultas funcionem conforme o esperado.
- Desempenho. Você deve garantir que as alterações no código não resultem na degradação do desempenho do aplicativo.

Esse padrão explica detalhadamente o processo de conversão.

Pré-requisitos e limitações

Pré-requisitos

- Conhecimento prático das sintaxes Python e Perl.
- Habilidades básicas em SQL Server e PostgreSQL.
- Compreensão da arquitetura de seu aplicativo existente.
- Acesso ao código do aplicativo, ao banco de dados do SQL Server e ao banco de dados do PostgreSQL.
- Acesso ao ambiente de desenvolvimento Windows ou Linux (ou outro Unix) com credenciais para desenvolver, testar e validar alterações em aplicativos.
- Para um aplicativo baseado em Python, bibliotecas Python padrão que seu aplicativo pode exigir, como Pandas para lidar com quadros de dados e psycopg2 ou para conexões de banco de dados. SQLAlchemy
- Para um aplicativo baseado em Perl, são necessários pacotes Perl com bibliotecas ou módulos dependentes. O módulo rede abrangente de arquivos do Perl (CPAN) pode oferecer suporte à maioria dos requisitos do aplicativo.
- Todas as bibliotecas ou módulos personalizados dependentes necessários.
- Credenciais do banco de dados para acesso de leitura ao SQL Server e acesso de leitura e gravação ao Aurora.
- PostgreSQL para validar e depurar alterações de aplicativos com serviços e usuários.

- Acesso a ferramentas de desenvolvimento durante a migração de aplicativos, como Visual Studio Code, Sublime Text ou pgAdmin.

Limitações

- Algumas versões, módulos, bibliotecas e pacotes do Python ou Perl não são compatíveis com o ambiente de nuvem.
- Algumas bibliotecas e estruturas de terceiros usadas para o SQL Server não podem ser substituídas para oferecer suporte à migração do PostgreSQL.
- As variações de desempenho podem exigir alterações em seu aplicativo, nas consultas em linha do Transact-SQL (T-SQL), nas funções do banco de dados e nos procedimentos armazenados.
- PostgreSQL suporta nomes em minúsculas para nomes de tabelas, nomes de colunas e outros objetos de banco de dados.
- Alguns tipos de dados, como colunas UUID, são armazenados somente em letras minúsculas. Os aplicativos Python e Perl devem lidar com essas diferenças de maiúsculas e minúsculas.
- As diferenças na codificação de caracteres devem ser tratadas com o tipo de dados correto para as colunas de texto correspondentes no banco de dados do PostgreSQL.

Versões do produto

- Python 3.6 ou superior (use a versão compatível com seu sistema operacional)
- Perl 5.8.3 ou superior (use a versão compatível com seu sistema operacional)
- Edição 4.2 ou superior do Aurora compatível com PostgreSQL (veja detalhes)

Arquitetura

Pilha de tecnologia de origem

- Linguagem de script (programação de aplicativos): Python 2.7 ou superior ou Perl 5.8
- Banco de dados: Microsoft SQL Server versão 13
- Sistema operacional: Red Hat Enterprise Linux (RHEL) 7

Pilha de tecnologias de destino

- Linguagem de script (programação de aplicativos): Python 3.6 ou superior ou Perl 5.8 ou superior

- Banco de dados: Aurora 4.2 compatível com PostgreSQL
- Sistema operacional: RHEL 7

Arquitetura de migração

Ferramentas

Ferramentas e serviços da AWS

- A Edição compatível com PostgreSQL do Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado, compatível com PostgreSQL e compatível com ACID que combina a velocidade e a confiabilidade de bancos de dados comerciais de alta tecnologia com a economia de bancos de dados de código aberto. O Aurora PostgreSQL é um substituto imediato do PostgreSQL e torna mais fácil e econômico configurar, operar e escalar suas implantações novas e existentes do PostgreSQL.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

Outras ferramentas

- Bibliotecas de conexão de banco de dados Python e PostgresSQL, como psycopg2 e SQLAlchemy
- Perl e seus módulos do DBI
- Terminal interativo do PostgreSQL (psql)

Épicos

Migre seu repositório de aplicativos para o PostgreSQL (etapas de alto nível)

Tarefa	Descrição	Habilidades necessárias
Siga estas etapas de conversão de código para migrar seu aplicativo para o PostgreSQL.	1. Defina drivers e bibliotecas ODBC específicos do banco de dados para o PostgreSQL. Por exemplo, você pode usar um dos módulos CPAN para Perl	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	e pyodbc, psycopg2 ou Python. SQLAlchemy 2. Converta objetos de banco de dados usando essas bibliotecas para se conectar ao Aurora compatível com PostgreSQL. 3. Aplique alterações de código nos módulos de aplicativos existentes para obter instruções T-SQL compatíveis. 4. Reescreva chamadas de função específicas do banco de dados e procedimentos armazenados no código do aplicativo. 5. Gerencie as alterações nas variáveis do seu aplicativo e seus tipos de dados que são usados para consultas SQL em linha. 6. Gerencie funções específicas de banco de dados incompatíveis. 7. end-to-endTeste completo do código de aplicativo convertido para migração de banco de dados. 8. Compare os resultados do Microsoft SQL Server com o aplicativo que você migrou para o PostgreSQL.	

Tarefa	Descrição	Habilidades necessárias
	9. Realize testes comparativos de desempenho de aplicativos entre o Microsoft SQL Server e o PostgreSQL. 10. Revise os procedimentos armazenados ou as instruções T-SQL em linha chamadas pelo aplicativo para melhorar o desempenho. Os épicos a seguir fornecem instruções detalhadas para algumas dessas tarefas de conversão para aplicativos Python e Perl.	

Tarefa	Descrição	Habilidades necessárias
Use uma lista de verificação para cada etapa da migração.	Adicione o seguinte à sua lista de verificação para cada etapa da migração do aplicativo, incluindo a etapa final: • Revise a documentação do PostgreSQL para garantir que todas as suas alteraçõe s sejam compatíveis com o padrão do PostgreSQL. • Verifique os valores inteiros e flutuantes das colunas. • Identifique o número de linhas inseridas, atualizad as e extraídas, junto com os nomes das colunas e os carimbos de data/hora. Você pode usar um utilitári o diff ou escrever um script para automatizar essas verificações. • Conclua as verificações de desempenho de grandes instruções SQL em linha e verifique o desempenho geral do aplicativo. • Verifique o tratament o correto de erros nas operações do banco de dados e na saída normal do programa usando vários blocos try/catch.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	• Verifique se os processos de registro adequados em log estão em vigor.	

Analise e atualize seu aplicativo — base de código Python

Tarefa	Descrição	Habilidades necessárias
Analise sua base de código Python existente.	Sua análise deve incluir o seguinte para facilitar o processo de migração do aplicativo: • Identifique todos os objetos de conexão no código. • Identifique todas as consultas SQL em linha incompatíveis (como instruções T-SQL e procedimentos armazenados) e analise as alterações necessárias. • Revise a documentação do seu código e acompanhe o fluxo de controle para entender a funcionalidade do código. Isso será útil posteriormente, quando você testar o aplicativo para comparações de desempenho ou carga. • Entenda a finalidade do aplicativo para que você possa testá-lo com	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	eficácia após a conversão do banco de dados. A maioria dos aplicativos do Python candidatos à conversão com migrações de banco de dados são feeds que carregam dados de outras fontes em tabelas de banco de dados ou extratores que recuperam dados das tabelas e os transformam em diferente s formatos de saída (como CSV, JSON ou arquivos simples) adequados para criar relatórios ou fazer chamadas de API para realizar validações.	

Tarefa	Descrição	Habilidades necessárias

Converta suas conexões de banco de dados para suportar o PostgreSQL.	A maioria dos aplicativos Python usa a biblioteca pyodbc para se conectar aos bancos de dados do SQL Server da seguinte maneira.
	`import pyodbc`
	`....`
	`try:`
	`conn_string = "Driver=ODBC Driver 17 for SQL Server;UID={};PWD={};Server={};Database={}".format (conn_user, conn_password, conn_server, conn_database)`
	`conn = pyodbc.connect(conn_string)`
	`cur = conn.cursor()`
	`result = cur.execute(query_string)`
	`for row in result:`
	`print (row)`
	`except Exception as e:`
	`print(str(e))`
	Converta a conexão do banco de dados para suportar o PostgreSQL da seguinte maneira.
	`import pyodbc`
	`import psycopg2`
	`....`
	`try:`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	conn_string = 'postgresql+psycopg2://'+ conn_user+':'+conn_password+'@'+conn_server+'/'+conn_database conn = pyodbc.connect(conn_string, connect_args={'options':'-csearch_path=dbo'}) cur = conn.cursor() result = cur.execute(query_string) for row in result: print (row) except Exception as e: print(str(e))	

Tarefa	Descrição	Habilidades necessárias

Altere as consultas SQL em linha para PostgreSQL.	Converta suas consultas SQL em linha em um formato compatível com PostgreSQL. Por exemplo, a consulta do SQL Server a seguir recupera uma string de uma tabela.
	
	`dtype = “type1”`
	`stm = ‘“SELECT TOP 1 searchcode FROM TypesTable (NOLOCK) WHERE code=”’ + “’” + str(dtype) + “’”`
	`# For Microsoft SQL Server Database Connection`
	`engine = create_engine(‘mssql+pyodbc:///?odbc_connect=%s’ % urllib.parse.quote_plus(conn_string), connect_args={‘connect_timeout’:login_timeout})`
	`conn = engine_connect()`
	`rs = conn.execute(stm)`
	`for row in rs:`
	`  print(row)`
	
	Após a conversão, a consulta SQL em linha compatível com PostgreSQL tem a seguinte aparência.
	
	`dtype = “type1”`
	`stm = ‘“SELECT searchcode FROM TypesTable`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	WHERE code=”’ + “’” + str(dtype) + “’ LIMIT 1”
	# For PostgreSQL Database Connection
	engine = create_engine(‘postgres+psycopg2://%s’ %conn_string, connect_args={‘connect_timeout’:login_timeout})
	conn = engine.connect()
	rs = conn.execute(stm)
	for row in rs:
	print(row)	

Tarefa	Descrição	Habilidades necessárias

Gerencie consultas SQL dinâmicas.	O SQL dinâmico pode estar presente em um script ou em vários scripts do Python. Exemplos anteriores mostraram como usar a função string replace (substituição de strings) do Python para inserir variáveis para estruturar consultas SQL dinâmicas. Uma abordagem alternativa é anexar a string de consulta com variáveis sempre que aplicável.
	
	No exemplo a seguir, a string de consulta é estruturada dinamicamente com base nos valores retornados por uma função.
	
	`query = '"SELECT id from equity e join issues i on e.permId=i.permId where e.id'"`
	`query += get_id_filter(ids) + " e.id is NOT NULL`
	
	Esses tipos de consultas dinâmicas são muito comuns durante a migração do aplicativo. Siga estas etapas para lidar com consultas dinâmicas:
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	• Verifique a sintaxe geral (por exemplo, a sintaxe da declaração `SELECT` com uma cláusula `JOIN`). • Verifique todas as variáveis ou nomes de colunas usados na consulta, como `i` e `id`. • Verifique as funções, argumentos e valores de retorno usados na consulta (por exemplo, `get_id_filter` e o argumento `ids`).	

Tarefa	Descrição	Habilidades necessárias

Gerencie conjuntos de resultados, variáveis e data frames.	No Microsoft SQL Server, você usa métodos Python, como `fetchone()` ou `fetchall()` para recuperar o conjunto de resultados do banco de dados. Você também pode usar `fetchmany(size)` e especificar o número de registros a serem retornados do conjunto de resultados. Para fazer isso, você pode usar o objeto de conexão pyodbc, conforme mostrado no exemplo a seguir.
	
	pyodbc (Microsoft SQL Server)
	
	`import pyodbc`
	`server = 'tcp:myserver.database.windows.net'`
	`database = 'exampledb'`
	`username = 'exampleusername'`
	`password = 'examplepassword'`
	`conn = pyodbc.connect('DRIVER={ODBC Driver 17 for SQL Server};SERVER='+server+';DATABASE='+database+';UID='+username+';PWD='+ password)`
	`cursor = conn.cursor()`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	``
	cursor.execute("SELECT
	 * FROM ITEMS")
	row = cursor.fe
	tchone()
	while row:
	    print(row[0])
	    row = cursor.fe
	tchone()
	``	

	No Aurora, para realizar tarefas semelhantes, como conectar-se ao PostgreSQ L e buscar conjuntos de resultados, você pode usar psycopg2 ou. SQLAlchemy Essas bibliotecas do Python fornecem o módulo de conexão e o objeto cursor para percorrer os registros do banco de dados do PostgreSQ L, conforme mostrado no exemplo a seguir.
	
	psycopg2 (Aurora compatível com PostgreSQL)
	
	``
	import psycopg2
	query = "SELECT * FROM
	 ITEMS;"
	//Initialize
	 variables
	host=dbname=user=
	password=port=sslm
	ode=connect_timeou
	t=""
	connstring = "host='{h
	ost}' dbname='{
	``	

Tarefa	Descrição	Habilidades necessárias
	dbname}' user='{user}' \ password='{passw ord}'port='{port}' ".format(host=host ,dbname=dbname,\ user=user,password= password,port=port) conn = psycopg2. connect(connstring) cursor = conn.cursor() cursor.execute(query) column_names = [column[0] for column in cursor.description] print("Column Names: ", column_names) print("Column values: " for row in cursor: print("itemid :", row[0]) print("itemdescrpt ion :", row[1]) print("it emprice :", row[3]))	
	SQLAlchemy (Compatível com Aurora PostgreSQL) from sqlalchemy import create_engine from pandas import DataFrame conn_string = 'postgres ql://core:database @localhost:5432/ex ampledatabase' engine = create_en gine(conn_string)	

Tarefa	Descrição	Habilidades necessárias
	`conn = engine.co nnect() dataid = 1001 result = conn.exec ute("SELECT * FROM ITEMS") df = DataFrame (result.fetchall()) df.columns = result.ke ys() df = pd.DataFrame() engine.connect() df = pd.read_sql_query( sql_query, engine, coerce_float=False) print(“df=”, df)`	

Tarefa	Descrição	Habilidades necessárias
Teste seu aplicativo durante e após a migração.	Testar o aplicativo do Python migrado é um processo contínuo. Como a migração inclui alterações no objeto de conexão (psycopg2 ou SQLAlchemy), tratament o de erros, novos recursos (quadros de dados), alteraçõe s de SQL em linha, funcional idades de cópia em massa (`bcp`em vez de`COPY`) e alterações semelhantes, ela deve ser testada cuidadosa mente durante e após a migração do aplicativo. Verifique se existe: • Condições e tratamento de erros • Qualquer incompatibilidade de registro após a migração • Registre atualizações ou exclusões • Tempo necessário para executar o aplicativo	Desenvolvedor de aplicativos

Analise e atualize seu aplicativo — base de código Perl

Tarefa	Descrição	Habilidades necessárias
Analise sua base de código Perl existente.	Sua análise deve incluir o seguinte para facilitar o processo de migração do	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	aplicativo. Você deve identificar: • Qualquer código INI ou baseado em configuração • Drivers Perl do Open Database Connectivity (ODBC) padrão específico do banco de dados ou qualquer driver personalizado • Alterações de código necessárias para consultas em linha e T-SQL • Interações entre vários módulos do Perl (por exemplo, um único objeto de conexão do Perl ODBC que é chamado ou usado por vários componentes funcionais) • Tratamento do conjunto de dados e do conjunto de resultados • Bibliotecas do Perl externas e dependentes • Qualquer APIs um que seja usado no aplicativo • Compatibilidade da versão do Perl e compatibilidade de drivers com o Aurora compatível com PostgreSQL	

Tarefa	Descrição	Habilidades necessárias
Converta as conexões do aplicativo do Perl e do módulo do DBI para suportar o PostgreSQL.	Os aplicativos baseados em Perl geralmente usam o módulo do Perl DBI, que é um módulo padrão de acesso ao banco de dados para a linguagem de programação Perl. Você pode usar o mesmo módulo do DBI com drivers diferentes para SQL Server e PostgreSQL. Para obter mais informações sobre os módulos do Perl, instalações e outras instruções necessários, consulte a documentação do DBD::Pg. O exemplo a seguir se conecta ao Aurora compatível com PostgreSQL em `examplete st-aurorapg-databa se.cluster-samplec lusture.us-east-.r ds.amazonaws.com` . `#!/usr/bin/perl use DBI; use strict; my $driver = "Pg"; my $hostname = “examplet est-aurorapg-datab ase-sampleclusture .us-east.rds.amazo naws.com” my $dsn = "DBI:$driver: dbname = $hostname ;host = 127.0.0.1;port = 5432";`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	`my $username = "postgres";`
	`my $password = "pass123";`
	`$dbh = DBI->connect("dbi:Pg:dbname=$hostname;host=$host;port=$port;options=$options",`
	`$username,`
	`$password,`
	`{AutoCommit => 0, RaiseError => 1, PrintError => 0}`
	`);`	

Tarefa	Descrição	Habilidades necessárias

Altere as consultas SQL em linha para PostgreSQL.	Seu aplicativo pode ter consultas SQL em linha com `SELECT`, `DELETE`, `UPDATE` e declarações semelhantes que incluam cláusulas de consulta que o PostgreSQL não suporta. Por exemplo, palavras-chave de consulta como `TOP` e `NOLOCK` não são suportadas no PostgreSQL. Os exemplos a seguir mostram como você pode gerenciar variáveis `TOP`, `NOLOCK` e booleanas.
	
	No SQL Server:
	
	`$sqlStr = $sqlStr . "WHERE a.student_id in (SELECT TOP $numofRecords c_student_id \ FROM active_student_record b WITH (NOLOCK) \ INNER JOIN student_contributor c WITH (NOLOCK) on c.contributor_id = b.c_st)`
	
	Para o PostgreSQL, converta para:
	
	`$sqlStr = $sqlStr . "WHERE a.student_id in (SELECT TOP $numofRecords c_student_id \`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	FROM active_student_rec ord b INNER JOIN student_contributor c \ on c.contributor_id = b.c_student_contr_id WHERE b_current_1 is true \ LIMIT $numofRecords)"	

Tarefa	Descrição	Habilidades necessárias
Gerencie consultas SQL dinâmicas e variáveis do Perl.	As consultas SQL dinâmicas são instruções SQL criadas no runtime do aplicativo. Essas consultas são estruturadas dinamicamente quando o aplicativo está em execução, dependendo de determinadas condições, portanto, o texto completo da consulta não é conhecido até o runtime. Um exemplo é um aplicativ o de análise financeira que analisa as 10 principais ações diariamente, e essas ações mudam todos os dias. As tabelas SQL são criadas com base nos melhores desempenhos e os valores não são conhecidos até o runtime. Digamos que as consultas SQL em linha deste exemplo sejam passadas para uma função de encapsulamento para obter o conjunto de resultados em uma variável e, em seguida, uma variável use uma condição para determinar se a tabela existe: • Se a tabela existir, não a crie; faça algum processam ento.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	• Se a tabela não existir, crie a tabela e também faça algum processamento.
	
	Este é um exemplo de manipulação de variáveis, seguido pelas consultas SQL Server e PostgreSQL para este caso de uso.
	
	`my $tableexists = db_read( arg 1, $sql_qry, undef, 'writer'); my $table_already_exists = $tableexists->[0]{table_exists}; if ($table_already_exists){ # do some thing } else { # do something else }`
	
	SQL Server:
	
	`my $sql_qry = “SELECT OBJECT_ID('$backendTable', 'U') table_exists", undef, 'writer') ";`
	
	PostgreSQL:
	
	`my $sql_qry = “SELECT TO_REGCLASS('$backendTable', 'U')`	

Tarefa	Descrição	Habilidades necessárias

	table_exists", undef, 'writer')";
	
	O exemplo a seguir usa uma variável do Perl em SQL em linha, que executa uma instrução `SELECT` com uma `JOIN` para buscar a chave primária da tabela e a posição da coluna chave.
	
	SQL Server:
	
	`my $sql_qry = "SELECT column_name', character_maxi mum_length \ FROM INFORMATION_SCHEMA .COLUMNS \ WHERE TABLE_SCH EMA='$example_sche maInfo' \ AND TABLE_NAME='$examp le_table' \ AND DATA_TYPE IN ('varchar','nvarch ar');";`
	
	PostgreSQL:
	
	`my $sql_qry = "SELECT c1.column_name, c1.ordinal_position \ FROM information_schema .key_column_usage AS c LEFT \ JOIN information_schema .table_constraints AS t1 \`	

Tarefa	Descrição	Habilidades necessárias
	`ON t1.constraint_name = c1.constraint_name \ WHERE t1.table_name = $example_schemaInfo'.'$example_table' \ AND t1.constraint_type = 'PRIMARY KEY' ;";`	

Faça alterações adicionais em seu aplicativo baseado em Perl ou Python para oferecer suporte ao PostgreSQL

Tarefa	Descrição	Habilidades necessárias
Converta estruturas adicionais do SQL Server em PostgreSQL.	As alterações a seguir se aplicam a todos os aplicativos, independentemente da linguagem de programação. • Qualifique os objetos do banco de dados que seu aplicativo usa com nomes de esquema novos e apropriados. • Use operadores LIKE para correspondência com distinção entre maiúsculas e minúsculas com o atributo de agrupamento no PostgreSQL. • Manipule funções específicas de banco de dados não suportadas como os operadores `DATEDIFF`, `DATEADD`, `GETDATE`, `CONVERT` e `CAST`. Para	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	funções equivalentes compatíveis com PostgreSQL, consulte Funções SQL nativas ou integradas na seção Informações adicionais. • Manipule valores booleanos em declarações de comparação. • Manipule os valores de retorno das funções. Podem ser conjuntos de registros, data frames, variáveis e valores booleanos. Trate-os de acordo com os requisitos do seu aplicativo e para oferecer suporte ao PostgreSQL. • Manipule blocos anônimos (como `BEGIN TRAN`) com novas funções do PostgreSQL definidas pelo usuário. • Converta inserções em massa para linhas. O equivalente do PostgreSQL do utilitário de cópia em massa (`bcp`) do SQL Server, que é chamado de dentro do aplicativo, é `COPY`. • Converta operadores de concatenação de colunas. O SQL Server usa + para	

Tarefa	Descrição	Habilidades necessárias
	concatenação de strings, mas o PostgreSQL usa ||.	

Melhorar o desempenho

Tarefa	Descrição	Habilidades necessárias
Aproveite os serviços da AWS para aprimorar o desempenho.	Ao migrar para a nuvem AWS, você pode refinar o design do aplicativo e do banco de dados para aproveitar os serviços da AWS. Por exemplo, se as consultas do seu aplicativo do Python, que está conectado a um servidor de banco de dados compatível com o Aurora PostgreSQL, estiverem demorando mais do que as consultas originais do Microsoft SQL Server, considere criar um feed de dados históricos diretamente para um bucket do Amazon Simple Storage Service (Amazon S3) a partir do servidor Aurora e usar consultas SQL baseadas no Amazon Athena para gere relatórios e consultas de dados analíticos para seus painéis de usuário.	Desenvolvedor de aplicativos, arquiteto de nuvem

Recursos relacionados

- Perl
- Módulo do Perl DBI
- Python
- psycopg2
- SQLAlchemy
- Cópia em massa: PostgreSQL
- Cópia em massa: Microsoft SQL Server
- PostgreSQL
- Trabalho com Amazon Aurora PostgreSQL

Mais informações

Tanto o Microsoft SQL Server quanto o Aurora compatível com PostgreSQL são compatíveis com o ANSI SQL. No entanto, você ainda deve estar ciente de quaisquer incompatibilidades na sintaxe, nos tipos de dados da coluna, nas funções específicas do banco de dados nativo, nas inserções em massa e na diferenciação de maiúsculas e minúsculas ao migrar seu aplicativo do Python ou Perl do SQL Server para o PostgreSQL.

As seções a seguir fornecem mais informações sobre possíveis inconsistências.

Comparação de tipos de dados

Alterações no tipo de dados do SQL Server para o PostgreSQL podem levar a diferenças significativas nos dados resultantes com os quais os aplicativos operam. Para obter uma comparação dos tipos de dados, consulte a tabela no site da Sqlines.

Funções SQL nativas ou integradas

O comportamento de algumas funções difere entre os bancos de dados SQL Server e PostgreSQL. A tabela a seguir oferece uma comparação.

Microsoft SQL Server	Descrição	PostgreSQL
`CAST`	Converte um valor de um tipo de dados para outro.	PostgreSQL `type :: operator`

`GETDATE()`	Retorna a data e hora do sistema de banco de dados atual, em um formato `YYYY-MM-DD hh:mm:ss.mmm` .	`CLOCK_TIMESTAMP`
`DATEADD`	Adiciona um intervalo de hora/data a uma data.	Expressão `INTERVAL`
`CONVERT`	Converte um valor em um formato de dados específico.	`TO_CHAR`
`DATEDIFF`	Retorna a diferença entre duas datas.	`DATE_PART`
`TOP`	Limita o número de linhas em um conjunto de `SELECT` resultados.	`LIMIT/FETCH`

Blocos anônimos

Uma consulta SQL estruturada é organizada em seções como declaração, executáveis e tratamento de exceções. A tabela a seguir compara as versões do Microsoft SQL Server e PostgreSQL de um bloco anônimo simples. Para blocos anônimos complexos, recomendamos que você chame uma função de banco de dados personalizada em seu aplicativo.

Microsoft SQL Server

```
my $sql_qry1=
my $sql_qry2 =
my $sqlqry = "BEGIN TRAN
$sql_qry1 $sql_qry2
if @\@error !=0 ROLLBACK
TRAN
else COMIT TRAN";
```

PostgreSQL

```
my $sql_qry1=
my $sql_qry2 =
my $sql_qry = " DO \$\$
BEGIN
$header_sql $content_sql
END
\$\$";
```

Outras diferenças

- Inserções de linhas em massa: o equivalente do PostgreSQL do utilitário bcp do Microsoft SQL Server é COPY.
- Sensibilidade a maiúsculas e minúsculas: os nomes das colunas diferenciam maiúsculas de minúsculas no PostgreSQL, portanto, é necessário converter os nomes das colunas do SQL Server para letras minúsculas ou maiúsculas. Isso se torna um fator quando você extrai ou compara dados ou coloca nomes de colunas em conjuntos de resultados ou variáveis. O exemplo a seguir identifica colunas nas quais os valores podem ser armazenados em maiúsculas ou minúsculas.

```
my $sql_qry = "SELECT $record_id FROM $exampleTable WHERE LOWER($record_name) =
 \'failed transaction\'";
```

- Concatenação: o SQL Server usa + como operador para concatenação de strings, enquanto o PostgreSQL usa | |.
- Validação: você deve testar e validar consultas e funções SQL em linha antes de usá-las no código do aplicativo para PostgreSQL.
- Inclusão da biblioteca ORM: você também pode procurar incluir ou substituir a biblioteca de conexão de banco de dados existente por bibliotecas ORM Python, como SQLAlchemyPynomoDB. Isso ajudará a consultar e manipular facilmente dados de um banco de dados usando um paradigma orientado a objetos.

Transmita dados do IBM Db2, SAP, Sybase e outros bancos de dados para o MongoDB Atlas em AWS

Criado por Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) e Igor Alekseev (AWS)

Resumo

Esse padrão descreve as etapas para migrar dados do IBM Db2 e de outros bancos de dados, como bancos de dados de mainframe e Sybase para o MongoDB Atlas no. Nuvem AWS Ele é usado AWS Gluepara ajudar a acelerar a migração de dados para o MongoDB Atlas.

O padrão acompanha o guia Migrating to MongoDB Atlas no site Prescriptive Guidance. AWS AWS Ele fornece as etapas de implementação de um dos cenários de migração discutidos nesse guia. Para cenários adicionais de migração, consulte os seguintes padrões no site da Orientação AWS Prescritiva:

- Migre um ambiente MongoDB auto-hospedado para o MongoDB Atlas em AWS
- Migre bancos de dados relacionais para o MongoDB Atlas em AWS

O padrão é destinado a parceiros e AWS usuários do AWS Managed Services.

Pré-requisitos e limitações

Pré-requisitos

- Um banco de dados de origem, como SAP, Sybase, IBM Db2 e outros, para migrar para o MongoDB Atlas.
- Familiaridade com bancos de dados como SAP, Sybase, IBM Db2, MongoDB Atlas e. Serviços da AWS

Versões do produto

- MongoDB versão 5.0 ou posterior.

Arquitetura

O diagrama a seguir ilustra o carregamento de dados em lote e o streaming de dados usando o AWS Glue Studio Amazon Kinesis Data Streams e o MongoDB Atlas.

Essa arquitetura de referência é usada AWS Glue Studio para criar pipelines de extração, transformação e carregamento (ETL) para migrar dados para o MongoDB Atlas. O An Crawler do AWS Glue se integra ao MongoDB Atlas para facilitar a governança de dados. Os dados podem ser transferidos em lote ou transmitidos para o MongoDB Atlas usando o Amazon Kinesis Data Streams.

Carregamento de dados em lote

Para obter mais informações sobre a migração de dados em lote, consulte a postagem do AWS blog Crie suas tarefas de ETL para o MongoDB Atlas com. AWS Glue

Streaming de dados

Para arquiteturas de referência do MongoDB Atlas que oferecem suporte a diferentes cenários de uso, consulte Migração para o MongoDB Atlas no site Prescriptive Guidance. AWS AWS

Ferramentas

- AWS Glueé um serviço ETL totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.
- O Amazon Kinesis Data Streams ajuda você a coletar e processar grandes fluxos de registros de dados em tempo real.
- O MongoDB Atlas é um banco de dados como serviço (DBaaS) totalmente gerenciado para implantar e gerenciar bancos de dados MongoDB na nuvem.

Práticas recomendadas

Para obter diretrizes, consulte o Guia de melhores práticas para o MongoDB no repositório do MongoDB. GitHub

Épicos

Descoberta e avaliação

Tarefa	Descrição	Habilidades necessárias
Determine o tamanho do cluster.	Estime o tamanho do conjunto de trabalho usando as	MongoDB DBA, arquiteto de aplicativos

Tarefa	Descrição	Habilidades necessárias
	informações do `db.stats( )` espaço total do índice. Suponha que uma porcentagem do seu espaço de dados seja acessada com frequência. Ou você pode estimar seus requisitos de memória com base em suas suposições. Essa tarefa deve levar aproximadamente uma semana. Para obter mais informações e exemplos dessa e de outras histórias deste épico, consulte os links na seção Recursos relacionados.	

Tarefa	Descrição	Habilidades necessárias
Estime os requisitos de largura de banda da rede.	Para estimar seus requisitos de largura de banda da rede, multiplique o tamanho médio dos documentos pelo número de documentos processados por segundo. Considere o tráfego máximo que qualquer nó do seu cluster suportará como base. Para calcular as taxas de transferência de dados downstream do seu cluster para os aplicativos cliente, use a soma do total de documentos retornados em determinado período. Se seus aplicativos fizerem a leitura a partir de nós secundários, divida esse número total de documentos pelo número de nós que podem processar operações de leitura. Para encontrar o tamanho médio do documento para um banco de dados, use o `db.stats().avgObjSize` comando. Essa tarefa normalmente leva um dia.	MongoDB DBA
Selecione a camada do Atlas.	Siga as instruções na documentação do MongoDB para selecionar a camada correta do cluster Atlas.	MongoDB DBA
Planeje a transição.	Planeje a substituição do aplicativo.	MongoDB DBA, arquiteto de aplicativos

Configure um novo ambiente MongoDB Atlas na AWS

Tarefa	Descrição	Habilidades necessárias
Crie um novo cluster MongoDB Atlas em. AWS	No MongoDB Atlas, escolha Criar um cluster e AWS selecione como provedor de nuvem.	MongoDB DBA
Selecione Regiões da AWS uma configuração global do cluster.	Selecione na lista de disponíveis Regiões da AWS para seu cluster Atlas. Configure clusters globais, se necessário.	MongoDB DBA
Selecione o nível cluster.	Selecione o nível de cluster de sua preferência. Sua seleção de camadas determina fatores como memória, armazenam ento e especificação de IOPS.	MongoDB DBA
Configurar definições adicionai s de cluster.	Definir configurações adicionai s de cluster, como opções de versão, backup e criptogra fia do MongoDB. Para obter mais informações sobre essas opções, consulte a seção Recursos relacionados.	MongoDB DBA

Configure a segurança e a conformidade

Tarefa	Descrição	Habilidades necessárias
Configure a lista de acesso.	Para se conectar ao cluster Atlas, você deve adicionar uma entrada à lista de acesso do projeto. O Atlas usa	MongoDB DBA

Tarefa	Descrição	Habilidades necessárias
	Transport Layer Security (TLS) / Secure Sockets Layer (SSL) para criptografar as conexões com a nuvem privada virtual (VPC) do seu banco de dados. Para configurar a lista de acesso do projeto e obter mais informaçõ es sobre as histórias desse épico, consulte os links na seção Recursos relacionados.	
Autentique e autorize usuários.	Você deve criar e autentica r os usuários do banco de dados que acessarão os clusters MongoDB Atlas. Para acessar os clusters em um projeto, os usuários devem pertencer a esse projeto e podem pertencer a vários projetos. Você também pode ativar a autorizaç ão com AWS Identity and Access Management (IAM). Para obter mais informaçõ es, consulte Configurar a autenticação com o IAM na documentação do MongoDB.	MongoDB DBA

Tarefa	Descrição	Habilidades necessárias
Criar funções personalizadas.	(Opcional) O Atlas oferece suporte à criação de funções personalizadas se os privilégios de usuário do banco de dados Atlas incorporado não cobrirem o conjunto de privilégios desejado.	MongoDB DBA
Configurar o emparelhamento de VPC.	(Opcional) O Atlas oferece suporte ao emparelhamento de VPC com outras AWS. VPCs	MongoDB DBA
Configure um AWS PrivateLink endpoint.	(Opcional) Você pode configurar endpoints privados AWS usando AWS PrivateLink.	MongoDB DBA
Ative a autenticação de dois fatores.	(Opcional) O Atlas fornece suporte à autenticação de dois fatores (2FA) para ajudar os usuários a controlar o acesso às suas contas do Atlas.	MongoDB DBA
Configure a autenticação e autorização do usuário com o LDAP.	(Opcional) O Atlas fornece suporte à autenticação e autorização do usuário com o Lightweight Directory Access Protocol (LDAP).	MongoDB DBA

Tarefa	Descrição	Habilidades necessárias
Configure o AWS acesso unificado.	(Opcional) Alguns recursos do Atlas, incluindo o Atlas Data Lake e a criptografia em repouso usando o gerenciam ento de chaves do cliente, usam funções do IAM para autenticação.	MongoDB DBA
Configure a criptografia em repouso usando AWS KMS o.	(Opcional) O Atlas suporta o uso de AWS Key Managemen t Service (AWS KMS) para criptografar mecanismos de armazenamento e backups de provedores de nuvem.	MongoDB DBA
Configure o CSFLE.	(Opcional) O Atlas oferece suporte à criptografia em nível de campo do lado do cliente (CSFLE), incluindo criptografia automática de campos.	MongoDB DBA

Migrar dados

Tarefa	Descrição	Habilidades necessárias
Execute seu conjunto de réplicas de destino no MongoDB Atlas.	Execute seu conjunto de réplicas de destino no MongoDB Atlas. No Atlas Live Migration Service, escolha Estou pronto para migrar.	MongoDB DBA
Estabeleça a conexão AWS Glue com o MongoDB Atlas.	Use an Crawler do AWS Glue para se conectar AWS Glue ao MongoDB Atlas (banco de dados de destino). Essa etapa	MongoDB DBA

Tarefa	Descrição	Habilidades necessárias
	ajuda a preparar o ambiente de destino para a migração. Para obter mais informações, consulte a documentação do AWS Glue.	
Estabeleça a conexão AWS Glue com o banco de dados de origem ou o fluxo de origem.	Isso ajuda a preparar o ambiente de destino para a migração.	MongoDB DBA
Configure a transformação de dados.	Configure a lógica de transformação para migrar os dados do esquema estrutura do legado para o esquema flexível do MongoDB.	MongoDB DBA
Migre os dados.	Agende a migração em AWS Glue Studio.	MongoDB DBA

Configurar integração operacional

Tarefa	Descrição	Habilidades necessárias
Conecte-se ao cluster.	Conecte-se ao cluster MongoDB Atlas.	Desenvolvedor de aplicativos
Interaja com os dados.	Interaja com os dados do cluster.	Desenvolvedor de aplicativos
Monitore os clusters.	Monitore seus clusters MongoDB Atlas.	MongoDB DBA
Faça backup e restaure dados.	Faça backup e restaure os dados do cluster.	MongoDB DBA

Solução de problemas

Problema	Solução
Se você encontrar problemas	Consulte Solução de problemas no repositório MongoDB Atlas Resources. CloudFormation

Recursos relacionados

Todos os links a seguir, salvo indicação em contrário, vão para páginas da web na documentação do MongoDB.

Guia de migração

- Migrando para o MongoDB AWS Atlas em (orientação prescritiva)AWS

Descoberta e avaliação

- Memória
- Exemplo de dimensionamento com conjuntos de dados de amostra do Atlas
- Exemplo de dimensionamento para aplicativos móveis
- Tráfego de rede
- Ajuste de escala automático de cluster
- Modelo de dimensionamento do Atlas

Configurar a segurança e a conformidade

- Configurar entradas da lista de acesso via IP
- Configurar usuários do banco de dados
- Configurar o acesso à interface do usuário do Atlas
- Configurar funções personalizadas do banco de dados
- Configurar usuários do banco de dados
- Configurar uma conexão de emparelhamento de rede
- Saiba mais sobre endpoints privados no Atlas
- Gerencie suas opções de autenticação multifatorial

- Configurar a autenticação e autorização do usuário com o LDAP
- Atlas Data Lake
- Criptografia em repouso usando o gerenciamento de chaves do cliente
- Métodos para assumir uma função (documentação do IAM)
- Criptografia em nível de campo do lado do cliente
- Criptografia automática
- Controles de segurança do MongoDB Atlas
- Central de confiabilidade do MongoDB
- Configurar recursos de segurança para clusters

Configurando um novo ambiente MongoDB Atlas em AWS

- Provedores de nuvem e regiões
- Gerencie clusters globais
- Selecione o nível do cluster
- Definir configurações adicionais
- Comece a usar o Atlas
- Configurar o acesso à interface do usuário do Atlas
- Gerenciar clusters

Migração de dados

- Migrar ou importar dados

Clusters de monitoramento

- Monitore seus clusters

Integração de operações

- Conectar-se a um cluster
- Interaja com seus dados
- Monitore seus clusters

- Faça backup, restaure e arquive dados

GitHub repositório

- Transmita dados para o MongoDB Atlas usando AWS Glue

Padrões de migração por workload

Tópicos

- IBM
- Microsoft
- N/D
- Código aberto
- Oracle
- SAP

IBM

- Migre um banco de dados Db2 da Amazon para o EC2 Aurora MySQL compatível usando o AWS DMS
- Migre o Db2 for LUW para a Amazon EC2 usando o envio de registros para reduzir o tempo de interrupção
- Migre o Db2 for LUW para a Amazon EC2 com recuperação de desastres de alta disponibilidade
- Migre do IBM Db2 na Amazon para o EC2 Aurora compatível com PostgreSQL usando o AWS DMS e o AWS SCT
- Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2
- Transmita dados do IBM Db2, SAP, Sybase e outros bancos de dados para o MongoDB Atlas em AWS

Microsoft

- Acelere a descoberta e a migração de cargas de trabalho da Microsoft para a AWS
- Altere os aplicativos Python e Perl para oferecer suporte à migração do banco de dados do Microsoft SQL Server para o Amazon Aurora Edição Compatível com PostgreSQL
- Crie CloudFormation modelos da AWS para tarefas do AWS DMS usando Microsoft Excel e Python
- Exportar um banco de dados do Microsoft SQL Server para o Amazon S3 usando o AWS DMS
- Implemente SHA1 o hashing para dados de PII ao migrar do SQL Server para o PostgreSQL
- Ingira e migre instâncias EC2 do Windows para uma conta do AWS Managed Services
- Migrar uma fila de mensagens do Microsoft Azure Service Bus para o Amazon SQS
- Migre um banco de dados Microsoft SQL Server da Amazon EC2 para o Amazon DocumentDB usando o AWS DMS
- Migre um banco de dados Microsoft SQL Server para o Aurora MySQL usando o AWS DMS e o AWS SCT
- Migre uma aplicação .NET do Microsoft Azure App Service para o AWS Elastic Beanstalk
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando servidores vinculados
- Saiba como migrar um banco de dados Microsoft SQL Server on-premises para o Amazon RDS para SQL Server utilizando backup e restauração nativos.
- Migrar um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift utilizando o AWS DMS
- Migre um banco de dados Microsoft SQL Server on-premises para o Amazon Redshift usando agentes de extração de dados da AWS SCT
- Migre um banco de dados local do Microsoft SQL Server para o Microsoft SQL Server na Amazon executando Linux EC2
- Migre dados do Microsoft Azure Blob para o Amazon S3 usando o Rclone
- Migre um banco de dados local do Microsoft SQL Server para a Amazon EC2 usando o Application Migration Service
- Migre um banco de dados relacional para o MongoDB Atlas em AWS

- Migrar certificados SSL do Windows para um Application Load Balancer usando o ACM
- Redefinir a hospedagem de workloads on-premises na Nuvem AWS: lista de verificação de migração
- Resolva erros de conexão após migrar o Microsoft SQL Server para a Nuvem AWS
- Configure a infraestrutura Multi-AZ para um SQL Server Always On FCI usando a Amazon FSx

N/D

- Crie um processo de aprovação para solicitações de firewall durante uma migração de rehospedagem para AWS

Código aberto

- Crie usuários e funções do aplicativo no Aurora compatível com PostgreSQL
- Migre o Amazon RDS for Oracle para o Amazon AWS SCT RDS for PostgreSQL com e usando e AWS DMSAWS CLIAWS CloudFormation
- Migre um banco de dados MariaDB on-premises para o Amazon RDS para MariaDB usando ferramentas nativas
- Migre um banco de dados MySQL local para a Amazon EC2
- Migrar um banco de dados MySQL on-premises para o Amazon RDS para MySQL
- Migrar um banco de dados MySQL on-premises para o Aurora MySQL
- Migrar um banco de dados PostgreSQL on-premises para o Aurora PostgreSQL
- Migrar um banco de dados do Couchbase Server para a Amazon EC2
- Migre do IBM WebSphere Application Server para o Apache Tomcat na Amazon EC2 com o Auto Scaling
- Migre da Oracle GlassFish para o AWS Elastic Beanstalk
- Migre do PostgreSQL na Amazon para o EC2 Amazon RDS for PostgreSQL usando pglogical
- Migre o ML Crie, treine e implante cargas de trabalho para a Amazon SageMaker usando as ferramentas do desenvolvedor da AWS
- Migrar aplicações Java on-premises para a AWS usando o App2Container da AWS
- Migre bancos de dados MySQL locais para o Aurora MySQL usando XtraBackup Percona, Amazon EFS e Amazon S3
- Migre tabelas externas da Oracle para a compatibilidade com o Amazon Aurora PostgreSQL
- Migre cargas de trabalho do Redis para o Redis Enterprise Cloud na AWS
- Reinicie o AWS Replication Agent automaticamente sem desativá-lo SELinux após a reinicialização de um servidor de origem RHEL
- Transporte bancos de dados PostgreSQL entre duas instâncias de banco de dados Amazon RDS usando pg_transport

Oracle

- Converter VARCHAR2 (1) tipo de dados para Oracle para tipo de dados booleano para Amazon Aurora PostgreSQL
- Emule o Oracle DR usando um banco de dados global Aurora compatível com PostgreSQL
- Migre incrementalmente do Amazon RDS para Oracle para o Amazon RDS para PostgreSQL usando o Oracle SQL Developer e o AWS SCT
- Faça o upload de arquivos BLOB em TEXT usando a codificação de arquivos no Aurora PostgreSQL-Compatible
- Migre o Amazon RDS para Oracle para o Amazon RDS para PostgreSQL no modo SSL usando o AWS DMS
- Migre um banco de dados Amazon RDS for Oracle para Conta da AWS outro Região da AWS e AWS DMS use-o para replicação contínua
- Migrar uma instância do banco de dados Amazon RDS para Oracle para outra VPC
- Migre um banco de dados Oracle local para a Amazon EC2 usando o Oracle Data Pump
- Migre um banco de dados Oracle local para o Amazon OpenSearch Service usando o Logstash
- Migre um banco de dados Oracle on-premises para o Amazon RDS para MySQL, usando o AWS DMS e o AWS SCT.
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump Import direto em um link de banco de dados
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para Oracle usando o Oracle Data Pump
- Migrar um banco de dados Oracle on-premises para o Amazon RDS para PostgreSQL usando um Oracle bystander e o AWS DMS
- Migre um banco de dados Oracle local para o Oracle na Amazon EC2
- Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for MariaDB usando o AWS DMS e o AWS SCT
- Migre um banco de dados Oracle da Amazon EC2 para o Amazon RDS for Oracle usando o AWS DMS
- Migrar um banco de dados Oracle para o Amazon DynamoDB usando AWS DMS
- Migre um banco de dados Oracle para o Amazon RDS for Oracle usando adaptadores de arquivo simples GoldenGate Oracle

- Migre um banco de dados Oracle para o Amazon Redshift usando o AWS DMS e o AWS SCT
- Migrar um banco de dados Oracle para o Aurora PostgreSQL usando AWS DMS e AWS SCT
- Migre um banco de dados Oracle JD Edwards EnterpriseOne para a AWS usando o Oracle Data Pump e o AWS DMS
- Migre uma tabela particionada do Oracle para o PostgreSQL usando o AWS DMS
- Migre um PeopleSoft banco de dados Oracle para a AWS usando o AWS DMS
- Migrar dados de um banco de dados Oracle on-premises para o Aurora PostgreSQL
- Migre do Amazon RDS para Oracle para o Amazon RDS para MySQL
- Migre do Oracle 8i ou 9i para o Amazon RDS para PostgreSQL usando visões materializadas e o AWS DMS
- Migre do Oracle 8i ou 9i para o Amazon RDS for PostgreSQL usando o AWS DMS SharePlex
- Migre do banco de dados Oracle para o Amazon RDS for PostgreSQL usando o Oracle GoldenGate
- Migre do Oracle na Amazon EC2 para o Amazon RDS for MySQL usando o AWS DMS e o AWS SCT
- Migrar do Oracle para o Amazon DocumentDB usando o AWS DMS
- Migre do Oracle WebLogic para o Apache Tomcat (TomEE) no Amazon ECS
- Migre índices baseados em funções do Oracle para o PostgreSQL
- Migre aplicativos legados do Oracle Pro*C para o ECPG
- Migrar valores do Oracle CLOB para linhas individuais no PostgreSQL na AWS
- Migre códigos de erro do banco de dados Oracle para um banco de dados compatível com Amazon Aurora PostgreSQL
- Migre o Oracle E-Business Suite para o Amazon RDS Custom
- Migre funções nativas do Oracle para o PostgreSQL usando extensões
- Migre o Oracle PeopleSoft para o Amazon RDS Custom
- Migre a funcionalidade Oracle ROWID para o PostgreSQL na AWS
- Migrar os pacotes de pragma Oracle SERIALLY_REUSABLE para o PostgreSQL
- Migre colunas geradas virtualmente do Oracle para o PostgreSQL
- Configure a funcionalidade Oracle UTL_FILE no Aurora compatível com PostgreSQL
- Valide objetos de banco de dados após migrar do Oracle para o Amazon Aurora PostgreSQL

SAP

- Migre um banco de dados SAP ASE local para a Amazon EC2
- Migre do SAP ASE para o Amazon RDS para SQL Server usando o AWS DMS
- Migre o SAP ASE na Amazon EC2 para o Amazon Aurora compatível com PostgreSQL usando o AWS SCT e o AWS DMS
- Reduza o tempo de substituição homogêneo da migração do SAP usando o Application Migration Service

Mais padrões

- Acesse Serviços da AWS a partir do IBM z/OS instalando o AWS CLI
- Avaliar a prontidão do aplicativo para migração para a Nuvem AWS usando o CAST Highlight
- Avaliar o desempenho das consultas para migrar bancos de dados do SQL Server para o MongoDB Atlas na AWS
- Automatize o failover e o failback entre regiões usando o DR Orchestrator Framework
- Automatize tarefas de banco de dados na edição SQL Server Express em execução na Amazon EC2 usando AWS Lambda um Agendador de Tarefas
- Crie um visualizador avançado de arquivos de mainframe na Nuvem AWS
- Configure uma extensão de datacenter para a VMware nuvem na AWS usando o modo vinculado híbrido
- Conecte-se ao ambiente de gerenciamento e dados do Application Migration Service em uma rede privada
- Containerize workloads de mainframe que foram modernizadas pela Blu Age
- Converta consultas JSON Oracle em SQL do banco de dados PostgreSQL
- Converta o atributo temporal Teradata NORMALIZE em Amazon Redshift SQL
- Converter o atributo Teradata RESET WHEN para Amazon Redshift SQL
- Copie tabelas do Amazon DynamoDB entre contas usando AWS Backup
- Implemente um cluster Cassandra na Amazon EC2 com estática privada IPs para evitar o reequilíbrio
- Implante aplicativos de várias pilhas usando o AWS CDK com TypeScript
- Implante instâncias de cluster de failover do SQL Server na Amazon EC2 e na Amazon FSx usando o Terraform
- Emule workloads do Oracle RAC usando endpoints personalizados no Aurora PostgreSQL
- Estime o tamanho do mecanismo Amazon RDS para um banco de dados Oracle usando relatórios AWR
- Gere insights de dados usando o AWS Mainframe Modernization e o Amazon Q em QuickSight
- Manipule blocos anônimos em instruções de SQL dinâmico no Aurora PostgreSQL
- Lide com funções sobrecarregadas do Oracle no Aurora compatível com PostgreSQL
- Identifique automaticamente imagens de contêineres duplicadas ao migrar para um repositório Amazon ECR

- Integre o VMware vRealize Network Insight com a VMware nuvem na AWS
- Migre instâncias do banco de dados Amazon RDS para Oracle para outras contas que usam AMS
- Migre um cluster Apache Kafka local para o Amazon MSK usando MirrorMaker
- Migre cargas de trabalho do Apache Cassandra para o Amazon Keyspaces usando o AWS Glue
- Migre suas cargas de trabalho de contêiner do Azure Red Hat OpenShift (ARO) para Serviço Red Hat OpenShift na AWS (ROSA)
- Migre do Oracle 8i ou 9i para o Amazon RDS for Oracle usando o AWS DMS SharePlex
- Migre dados do Hadoop para o Amazon S3 usando o Migrator WANdisco LiveData
- Migre funções e procedimentos do Oracle que tenham mais de 100 argumentos para o PostgreSQL
- Migrar variáveis de ligação Oracle OUT para um banco de dados PostgreSQL
- Migre o SAP HANA para a AWS usando o SAP HSR com o mesmo nome de host
- Migre o SQL Server para a AWS usando grupos de disponibilidade distribuídos
- Migre VMs para a VMware nuvem na AWS usando a migração assistida do sistema operacional HCX
- Modernize as workloads de impressão on-line de mainframe na AWS usando o Micro Focus Enterprise Server e o LRS VPSX/MFI
- Modernize o gerenciamento de saída do mainframe AWS usando o Rocket Enterprise Server e o LRS X PageCenter
- Modifique os cabeçalhos HTTP ao migrar de F5 para um Application Load Balancer na AWS
- Gerencie o failover Multi-AZ para clusters do EMR usando o Application Recovery Controller
- Envie registros do VMware Cloud on AWS para o Splunk usando o VMware Aria Operations for Logs
- Configure um pipeline de CI/CD para migração de banco de dados usando o Terraform
- Configure a recuperação de desastres para o Oracle JD Edwards com o EnterpriseOne AWS Elastic Disaster Recovery
- Simplificar o gerenciamento de certificados privados usando a CA privada da AWS e o AWS RAM
- Transferir dados do Db2 z/OS em grande escala para o Amazon S3 em arquivos CSV

Modernização

Tópicos

- Analisar e visualizar a arquitetura de software no CAST Imaging
- Avaliar a prontidão do aplicativo para migração para a Nuvem AWS usando o CAST Highlight
- Arquivar automaticamente itens no Amazon S3 usando o DynamoDB TTL
- Crie uma arquitetura sem servidor multilocatário no Amazon Service OpenSearch
- Implante aplicativos de várias pilhas usando o AWS CDK com TypeScript
- Automatize a implantação de aplicativos aninhados usando o AWS SAM
- Implementar o isolamento de inquilinos SaaS para o Amazon S3 usando uma máquina de venda automática de tokens AWS Lambda
- Implementar o padrão de saga com tecnologia sem servidor usando o AWS Step Functions
- Gerencie aplicativos de contêineres on-premises configurando o Amazon ECS Anywhere com o AWS CDK
- Modernize aplicativos ASP.NET Web Forms na AWS
- Executar workloads agendadas e orientadas por eventos em grande escala com o AWS Fargate
- Integração de locatários na arquitetura de SaaS para o modelo de silo usando C# e o AWS CDK
- Decomponha monólitos em microsserviços usando o CQRS e o fornecimento de eventos
- Mais padrões

Analisar e visualizar a arquitetura de software no CAST Imaging

Criado por Arpita Sinha (Cast Software) e James Hurrell (Cast Software)

Resumo

Este padrão mostra como usar o CAST Imaging para navegar visualmente em um sistema de software complexo e realizar uma análise precisa da estrutura do software. Ao usar o CAST Imaging dessa forma, você pode tomar decisões mais fundamentadas sobre a arquitetura do seu aplicativo, principalmente para fins de modernização.

Para visualizar a arquitetura do seu aplicativo no CAST Imaging, primeiro você deve integrar o código-fonte do seu aplicativo por meio do CAST Console. Em seguida, o console publica os dados do seu aplicativo no CAST Imaging, onde você pode visualizar e navegar pela arquitetura do aplicativo camada por camada.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- A Imagem de máquina da Amazon (AMI) para o CAST Imaging
- Uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que inclui o seguinte (uma instância r5.xlarge da EC2 Amazon com memória otimizada é recomendada):
  - 4 vCPU
  - RAM de 32 GB
  - Volume mínimo de 500 GB de unidade de estado sólido (SSD) de uso geral (gp3)
- Chaves de licença do CAST Console e do CAST Imaging (para obter as chaves de licença necessárias, entre em contato com o CAST através do e-mail aws.contact-me@castsoftware.com)
- O código-fonte completo do aplicativo que você deseja analisar em formato compactado (.zip)
- Microsoft Edge, Mozilla Firefox ou Google Chrome

Arquitetura

O diagrama a seguir mostra um exemplo de fluxo de trabalho para integrar o código-fonte de um aplicativo por meio do CAST Console e, em seguida, visualizá-lo no CAST Imaging:

O diagrama mostra o seguinte fluxo de trabalho:

1. O CAST gera metadados de código-fonte do aplicativo por meio de engenharia reversa de código de frontend, middleware e backend.
2. Os dados do aplicativo gerados pelo CAST são importados automaticamente para o CAST Imaging, onde podem ser visualizados e analisados.

Confira a seguir um resumo de como esse processo funciona:

Ferramentas

- O CAST Imaging é um aplicativo baseado em navegador que ajuda você a enxergar o sistema de software e navegar visualmente por ele para que possa tomar decisões fundamentadas sobre sua arquitetura.
- O CAST Console é um aplicativo baseado em navegador que ajuda você a configurar, executar e gerenciar análises CAST AIP.

> **Note**
>
> O CAST Imaging e o CAST Console estão incluídos na AMI for CAST Imaging.

Épicos

Configurar o ambiente do CAST Imaging

Tarefa	Descrição	Habilidades necessárias
Execute a configuração inicial do CAST Console.	1. Abra seu navegador e conecte-se ao CAST Console inserindo o seguinte URL: http://localhost:8081 2. Quando solicitado, insira sua chave de licença	Arquitetos de software, desenvolvedores, líderes técnicos

Tarefa	Descrição	Habilidades necessárias
	do CAST Console. Em seguida, escolha Próximo. 3. Revise as definições da configuração. Se nenhuma alteração for necessária, escolha Salvar e concluir.	
Execute a configuração inicial do CAST Imaging.	1. Abra seu navegador e conecte-se ao CAST Imaging inserindo o seguinte URL: http://localhost:8083 2. Quando solicitado, faça login digitando admin para o nome de usuário e a senha. 3. Quando solicitado, insira sua chave de licença do CAST Imaging. Em seguida, escolha Atualizar para salvar a chave.	Arquitetos de software, desenvolvedores, líderes técnicos

Tarefa	Descrição	Habilidades necessárias
Configure o servidor local CAST Extend.	(Opcional) Por definição , o servidor local CAST Extend está configurado para funcionar no modo off-line. Se isso for aceitável, nenhuma configuração adicional será necessária. No entanto, se você preferir configurar o servidor local CAST Extend no modo on-line/proxy com uma conexão direta com o CAST Extend, siga estas etapas. **Note** Para obter as credenciais do CAST Extend, consulte a página de registro do CAST Extend. 1. Use o atalho do CAST Extend Admin Center na área de trabalho para carregar seu navegador e conectar-se ao servidor local CAST Extend. 2. Escolha a opção On-line. 3. Insira suas credenciais do CAST Extend (e-mail e senha) e escolha Salvar para concluir o processo.	Arquitetos de software, desenvolvedores, líderes técnicos

Integrar seu aplicativo ao CAST Imaging

Tarefa	Descrição	Habilidades necessárias
Prepare o código-fonte do seu aplicativo.	Salve o código-fonte do seu aplicativo em um único arquivo .zip compactado.	Arquitetos de software, desenvolvedores, líderes técnicos
Adicione seu aplicativo ao CAST Console.	1. Abra seu navegador e conecte-se ao CAST Console inserindo o seguinte URL: http://localhost:8081 2. Quando solicitado, faça login digitando admin para o nome de usuário e a senha. 3. Escolha Adicionar aplicativo. Em seguida, insira o nome do aplicativo e escolha Adicionar.	Arquitetos de software, desenvolvedores, líderes técnicos
Abra o assistente de entrega do código-fonte.	Encontre o aplicativo que você criou no CAST Console. Em seguida, escolha Adicionar versão.	Arquitetos de software, desenvolvedores, líderes técnicos
Faça o upload do código-fonte para seu aplicativo.	Execute um destes procedimentos: • Arraste e solte o arquivo .zip que contém o código-fonte do seu aplicativo no assistente de entrega do código-fonte. –ou– • Escolha o ícone da nuvem de upload. Em seguida,	Arquitetos de software, desenvolvedores, líderes técnicos

Tarefa	Descrição	Habilidades necessárias
	abra o arquivo .zip que contém o código-fonte do seu aplicativo.	
Inicie o processo de análise.	1. No assistente de entrega, forneça os detalhes da versão e especifique as opções de configuração. Para obter mais informaçõ es, consulte Integraçã o padrão para o CAST Imaging na documentação do CAST Imaging. 2. Certifique-se de que a opção Publicar no CAST Imaging esteja selecionada. Em seguida, escolha Continuar. **Note** Escolher Continuar inicia o processo de análise do código-fonte. A janela de progresso no CAST Console mostra cada etapa do processo de análise e exibe uma notificação quando a análise é concluída.	Arquitetos de software, desenvolvedores, líderes técnicos

Verificar os resultados da análise e os dados publicados no CAST Imaging

Tarefa	Descrição	Habilidades necessárias
Verifique o status e os logs.	Quando todas as ações de análise estiverem concluídas, verifique se há uma mensagem de sucesso na janela de progresso. **Note** Você pode verificar os registros individuais de cada ação de análise imediatamente após sua conclusão. Para revisar os logs de uma ação específica, escolha Exibir log na janela Progresso.	Arquitetos de software, desenvolvedores, líderes técnicos
Verifique os detalhes do aplicativo.	No painel Detalhes do aplicativo, revise os detalhes sobre os resultados da análise. Certifique-se de conferir as tecnologias que foram descobertas e a organização do código-fonte.	Arquitetos de software, desenvolvedores, líderes técnicos
Verifique e acesse o CAST Imaging.	1. No painel Gerenciamento de aplicativos no CAST Console, verifique se o status da versão do seu aplicativo é Processado pelo Imaging. Um ícone do CAST Imaging é exibido.	Arquitetos de software, desenvolvedores, líderes técnicos

Tarefa	Descrição	Habilidades necessárias
	2. Escolha o ícone do CAST Imaging para navegar diretamente até os dados do seu aplicativo no CAST Imaging. **Note** O status de processamento de imagens significa que o código-fonte foi analisado e carregado na sua instância do CAST Imaging.	

Iniciar a análise do seu aplicativo com o CAST Imaging

Tarefa	Descrição	Habilidades necessárias
Faça login no CAST Imaging.	Abra o Cast Imaging e insira as credenciais de administrador padrão (admin/admin). Os dados do seu aplicativo são exibidos.	Arquitetos de software, desenvolvedores, líderes técnicos
Explore os dados do seu aplicativo no CAST Imaging.	Comece a visualizar sua arquitetura de software usando os atributos do CAST Imaging. Para conferir um rápido tutorial sobre como usar os atributos do CAST Imaging,	Arquitetos de software, desenvolvedores, líderes técnicos

Tarefa	Descrição	Habilidades necessárias
	escolha o ícone Ajuda para exibir o CAST Imaging Helper. Para obter mais informações, consulte o Guia do usuário do CAST Imaging.	

Recursos relacionados

Documentação do CAST console

- Login
- Configuração de opções via CAST Console

Documentação do CAST Imaging

- Integração de aplicativos para o CAST Imaging – pré-requisitos
- Adicionar um novo aplicativo para o CAST Imaging
- Integração padrão para o CAST Imaging – verificar resultados
- Login
- Opções de configuração – GUI da Admin Center

Mais recursos sobre o CAST Imaging na AWS

- Modernização de aplicativos para a AWS acelerada pelo CAST — Técnica (PartnerCast webinar da AWS, requer uma conta gratuita)
- Uso do CAST e do AWS Migration Hub Refactor Spaces para modernizar aplicativos herdados (publicação do blog da AWS)
- Modernize aplicativos para arquiteturas da AWS com o CAST Imaging (workshop da AWS)
- AWS Marketplace: CAST Imaging
- Todos os recursos do CAST na AWS

Avaliar a prontidão do aplicativo para migração para a Nuvem AWS usando o CAST Highlight

Criado por Greg Rivera (Cast Software)

Resumo

O CAST Highlight é uma solução de software como serviço (SaaS) para realizar uma análise rápida do portfólio de aplicativos. Este padrão descreve como configurar e usar o CAST Highlight para avaliar a prontidão para a nuvem de aplicativos de software personalizados em todo o portfólio de TI de uma organização e planejar a modernização ou a migração para a nuvem da Amazon Web Services (AWS).

O CAST Highlight gera insights sobre a prontidão de um aplicativo para a nuvem, identifica bloqueadores de código que precisam ser removidos antes da migração, estima o esforço para remover esses bloqueadores e recomenda serviços da AWS que aplicativos individuais possam usar após a migração.

Este padrão descreve o procedimento para configurar e usar o CAST Highlight, que consiste em cinco etapas: configuração de novos usuários, gerenciamento de aplicativos, gerenciamento de campanhas, análise de código-fonte e análise de resultados. Você deve concluir todas as etapas na seção Tópicos desse padrão para garantir a verificação e a análise bem-sucedidas do aplicativo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta ativa do CAST Highlight com permissões do Portfolio Manager.
- Pelo menos 300 MB de espaço livre em disco e 4 GB de memória em seu computador local para instalar o agente local do CAST Highlight.
- Microsoft Windows 8 ou superior.
- O código-fonte do seu aplicativo deve ser armazenado em arquivos de texto acessíveis na máquina em que o agente local está instalado. Nenhum código-fonte sai das instalações e todo o código é verificado localmente.

Arquitetura

O diagrama a seguir ilustra o fluxo de trabalho de uso do CAST Highlight.

O fluxo de trabalho consiste nas seguintes etapas:

1. Faça login no portal do CAST Highlight, baixe o agente local e instale-o em seu computador local. O Amazon Simple Storage Service (Amazon S3) armazena o pacote de instalação do agente local.
2. Verifique seus arquivos de código-fonte e gere um arquivo de resultados.
3.
> **Important**
>
> Faça upload do arquivo de resultados para o portal do CAST Highlight. : nenhum código-fonte está incluído no arquivo de resultados.

4. Responda às perguntas da pesquisa para cada aplicativo que você verificou.
5. Veja os painéis e relatórios disponíveis no portal do CAST Highlight. O Amazon Relational Database Service (Amazon RDS) armazena a verificação do código, os resultados da análise e os dados do software CAST Highlight.

Pilha de tecnologia

O CAST Highlight oferece suporte às seguintes tecnologias para analisar a prontidão dos aplicativos para a nuvem:

- Java
- COBOL
- C#
- C++
- Clojure
- PHP
- JavaScript
- TypeScript
- Python
- Microsoft Transact-SQL
- VB.Net

- Kotlin
- Scala
- Swift

Automação e escala

- Um analisador de CLI pode ser usado para automatizar o processo de análise do CAST Highlight.

Ferramentas

Nenhuma ferramenta será necessária para esse padrão se todos os pré-requisitos forem atendidos. No entanto, você pode usar ferramentas opcionais, como utilitários de gerenciamento de código-fonte (SCM), extratores de código ou outras ferramentas para gerenciar seus arquivos de código-fonte.

Épicos

Nova configuração de usuário

Tarefa	Descrição	Habilidades necessárias
Ative sua conta do CAST Highlight e escolha sua senha.	Todos os usuários iniciantes do CAST Highlight recebem um e-mail de ativação da conta. Clique no link de ativação para ativar sua conta do CAST Highlight e digite uma senha para concluir o processo de ativação.	N/D
Faça login no portal do CAST Highlight.	A página inicial do CAST Highlight aparece depois que você digita sua nova senha. Faça login no portal do CAST Highlight com suas credencia is de usuário.	N/D

Gerenciamento de aplicações

Tarefa	Descrição	Habilidades necessárias
Criar um registro do aplicativo.	No portal do CAST Highlight, navegue até a guia Gerenciar aplicativo na seção Gerenciar portfólio. No bloco Aplicativos na parte superior da tela, escolha Adicionar.	N/D
Escolha um nome de aplicativo.	Depois, insira um nome para seu aplicativo, e em seguida, escolha Salvar. Este nome é usado para o registro do seu aplicativo no CAST Highlight.	N/D
Repita as etapas para todos os aplicativos.	Repita essas etapas para cada aplicativo que você quer verificar.	N/D

Gerenciamento de campanhas

Tarefa	Descrição	Habilidades necessárias
Criar uma campanha.	O CAST Highlight usa o termo “campanha” para descrever um conjunto de aplicativos que serão analisados em determinado momento. No portal do CAST Highlight, navegue até a guia Gerenciar campanhas na seção Gerenciar portfólio. Escolha Criar campanha	N/D

Tarefa	Descrição	Habilidades necessárias
	para abrir a tela de criação da campanha.	
Insira um nome e escolha uma data de encerramento para a campanha.	Insira um nome para sua campanha e escolha uma data de encerramento para a campanha. **Important** Os colaboradores não podem enviar os resultados da análise da inscrição após a data de encerramento da campanha.	N/D

Tarefa	Descrição	Habilidades necessárias
Decida incluir a verificação do código-fonte, as respostas da pesquisa e o escopo do domínio e do aplicativo.	Escolha uma ou mais das pesquisas padrão usadas para aprimorar os dados de análise do código-fonte com informações qualitativas. As categorias da pesquisa são Impacto nos negócios, Esforço de manutenção de software CloudReady, propriedades do aplicativo e Impacto verde. Escolha o domínio e os aplicativos que serão analisados durante a campanha. **Important** Certifique-se de adicionar todos os aplicativos que você deseja escanear na seção Gerenciar aplicativos antes de começar a campanha.	N/D
Personalize a mensagem de lançamento.	Personalize a mensagem de lançamento que será enviada por e-mail a todos os colaboradores associados aos aplicativos da campanha.	N/D
Lance a campanha.	Escolha Concluído para lançar a campanha.	N/D

Análise de código-fonte

Tarefa	Descrição	Habilidades necessárias
Baixe o agente local do CAST Highlight.	No portal do CAST Highlight , escolha Verificação de aplicativos baixe o agente local para seu computador local.	N/D
Instalar o agente local.	Inicie o programa de instalaçã o CASTHighlight Setup.exe e siga as instruções de configuração que aparecem. Depois que o agente local for instalado, você estará pronto para analisar seus aplicativos.	N/D
Defina o escopo da verificação do código do agente local.	A análise do código é realizada no nível do arquivo e não considera os links lógicos ou as dependências entre os arquivos. Todos os arquivos são considerados iguais e fazem parte do aplicativo. Para fornecer resultados precisos e consistentes, prepare seu escopo de verificação de código usando os recursos de exclusão de arquivos ou pastas disponíveis no agente local.	N/D
Inclua pacotes de código aberto ou COTS.	(Opcional) Se você quiser incluir pacotes de código aberto ou comerciais off-the-shelf (COTS), verifique	N/D

Tarefa	Descrição	Habilidades necessárias
	se eles estão incluídos nas pastas que você planeja verificar. Normalmente, as bibliotecas externas são agrupadas em uma subpasta chamada “terceiros” ou um título semelhante e o código principal geralmente está localizado na pasta de arquivos “src/principal”.	
Exclua as classes de teste.	As classes de teste com frequência são excluídas da análise do código-fonte porque geralmente não fazem parte do aplicativo compilado . Porém, você pode optar por incluí-las na verificação, se necessário.	N/D
Exclua as pastas de SCM, compilação e implantação.	Para obter resultados mais consistentes, você deve evitar a inclusão de pastas de SCM, compilação ou implantação (por exemplo, arquivos .git ou .svn) em sua verificação.	N/D

Tarefa	Descrição	Habilidades necessárias
Inclua arquivos de dependência.	Se você quiser obter informações sobre estruturas e dependências cujos arquivos físicos não fazem parte da pasta que está verificando, inclua os arquivos de dependência (como arquivos pom.xml, build.gradle, package.json ou .vcsproj).	N/D
Invoque o agente local.	Execute o agente local em sua máquina Windows local.	N/D
Escolha a pasta que contém seu código-fonte.	Escolha a pasta que contém seu código-fonte. Você pode adicionar várias pastas para serem descobertas pelo agente local. Embora o agente local ofereça suporte à descoberta de origens por meio de caminhos de rede, você deve se certificar de que as pastas de origem estejam localizadas na sua máquina local. **Important** Recomendamos executar várias varreduras se houver mais de 10.000 arquivos em suas pastas de origem.	N/D

Tarefa	Descrição	Habilidades necessárias
Inicie a descoberta de arquivos.	No painel do agente local, escolha Descobrir arquivos. O agente local descobre arquivos em suas pastas e subpastas, além de detectar suas tecnologias. Você pode escolher o botão Cancelar para cancelar a descoberta a qualquer momento. Depois que a descoberta do arquivo for concluída, o agente local listará as pastas e os arquivos encontrados. A coluna Tecnologias mostra as tecnologias associadas e a contagem de arquivos. A coluna Caminho mostra a localização das pastas e dos arquivos.	N/D

Tarefa	Descrição	Habilidades necessárias
Refine a configuração de verificação do código-fonte.	(Opcional) Para refinar a verificação do agente local, você pode desativar uma ou mais tecnologias para uma pasta ou um arquivo específico. Se todas as tecnologias forem desativadas, sua pasta ou seu arquivo será excluído do escopo da verificação. Para desativar tecnologias, escolha o rótulo amarelo da tecnologia que você deseja desativar. Você também pode escolher o ícone de filtro ao passar o mouse sobre um arquivo ou uma pasta para associar uma tecnologia a um arquivo ou uma pasta específica. Essas configurações são salvas e aceleram o processo de descoberta da pasta ou do arquivo.	N/D
Inicie a verificação do código-fonte.	Depois de configurar sua verificação, escolha “Verificar arquivos” para iniciar o processo de verificação.	N/D

Tarefa	Descrição	Habilidades necessárias
Verifique se há rótulos verdes ou cinza.	Depois que a verificação do código-fonte for concluída, um rótulo de status será exibido nos níveis de pasta e arquivo. Um rótulo verde significa que os arquivos foram verificados corretamente com a tecnologia associada. Um rótulo cinza significa que os arquivos não foram verificados, tendo sido excluídos. O motivo da exclusão é mostrado quando você passa o mouse sobre o rótulo de cada arquivo. Os possíveis motivos para a exclusão de arquivos são arquivos binários, arquivos ilegíveis, arquivos ausentes, biblioteca externa, arquivos codificados, arquivos gerados, erros de sintaxe, conteúdo que não está no idioma esperado, código que não está em conformidade com critérios de análise suficientes, arquivos que excedem o limite de tamanho (10 MB), problemas de tempo limite ou indisponibilidade do analisador.	N/D

Tarefa	Descrição	Habilidades necessárias
Modifique a configuração da verificação e verifique o código novamente.	(Opcional) Você pode modificar suas configurações de verificação e escolher Verificar arquivos para verificar os arquivos novamente.	N/D
Confirme os resultados da verificação.	Escolha Confirmar resultados se os resultados da verificação atenderem aos seus requisitos.	N/D
Visualize as estruturas e bibliotecas de software encontradas pelo agente local.	Visualize as estruturas e bibliotecas de software usadas ou referenciadas por seus aplicativos e descobertas pelo agente local durante a verificação do código. Você pode manter ou ignorar elementos dessas listas escolhendo o botão de alternância individual. Escolha Confirmar dependências para continuar. **Important** Se uma estrutura estiver desativada, ela não será listada no portal CAST Highlight nem anexada ao seu aplicativo.	N/D

Tarefa	Descrição	Habilidades necessárias
Salve os resultados da verificação do código.	O agente local exibe um resumo dos resultados da verificação de código agrupados por tecnologia. Escolha Salvar e especifique a pasta na qual você deseja que os resultados sejam salvos. O agente local gera um arquivo .zip por verificaç ão, que contém todos os resultados da análise. Dependendo do número de tecnologias distintas e pastas de código-fonte raiz, o Agente Local gera automaticamente um ou vários arquivos.csv com a estrutura de nomenclat ura FolderName.Technol ogy.Date.csv.	N/D
Faça upload dos resultados de verificação de código para o portal do CAST Highlight.	No portal do CAST Highlight , escolha os aplicativos que você analisou na seção Verificações de aplicativ os. Escolha Fazer upload dos resultados e escolha os arquivos .csv. Você também pode fazer upload dos arquivos .csv individua lmente. Depois do upload de cada arquivo, um registro do upload aparece na tela.	N/D

Tarefa	Descrição	Habilidades necessárias
Exclua os arquivos de resultados da análise, se necessário.	(Opcional) Um arquivo de resultados da análise pode ser excluído a qualquer momento durante o processo de upload ao escolher o ícone da lixeira. **⚠ Important** Somente usuários com privilégios do Portfolio Manager ou o colaborador que enviou os resultados podem excluí-los.	N/D
Responda à pesquisa do aplicativo.	Um botão Pesquisa aparece em aplicativos que exigem uma pesquisa. Escolha Pesquisa, responda às perguntas de cada seção e selecione Enviar depois de terminar. O progresso de sua pesquisa é exibido na parte superior da tela. Você pode enviar seus resultados após o envio de todas as informações obrigatórias. No entanto, você pode enriquecer os dados na instância do CAST Highlight da sua organizaç ão respondendo a todas as perguntas.	N/D

Tarefa	Descrição	Habilidades necessárias
Envie os resultados da verificação do código.	Depois de fazer upload de todos os arquivos de resultados .csv do aplicativo e responder as perguntas da pesquisa, escolha Enviar na seção Verificações de aplicativos. Essa etapa é necessária para concluir o processo e garantir que os resultados estejam disponíveis no portal do CAST Highlight.	N/D

Análise de resultados

Tarefa	Descrição	Habilidades necessárias
Veja a página inicial do portal do CAST Highlight.	A página inicial do portal CAST Highlight inclui blocos que contêm informações de alto nível sobre seu portfólio de aplicativos, como integridade do software e pontuações de segurança de código aberto para todo o seu portfólio. CloudReady A página inicial também inclui o número de aplicativos integrados. Para obter mais informações sobre as definições de métricas e a metodologia de medição do CAST Highlight, consulte CAST Highlight — Metrics and	N/D

Tarefa	Descrição	Habilidades necessárias
	methodology (PowerPoint apresentação da Microsoft).	
Veja o CloudReady painel.	Escolha o CloudReady bloco para abrir o CloudRead y painel. Esse é o painel principal no nível de portfólio para avaliar a prontidão de seus aplicativos para a nuvem. Ele ajuda você a planejar e desenvolver um roteiro de portfólio para sua migração para a nuvem	N/D

Tarefa	Descrição	Habilidades necessárias
Veja o painel do Portfolio Advisor for Cloud.	O painel do Portfolio Advisor for Cloud segmenta automaticamente os aplicativos nas categorias de migração recomendadas. A segmentação é baseada nas características técnicas de cada aplicativo. Os fatores incluem a análise do código-fonte (prontidão para a nuvem, resiliência do software e muito mais) e o impacto nos negócios, decorrente da pesquisa. No canto superior direito, escolha Computar para gerar as recomendações iniciais de segmentação. As bolhas nos gráficos na parte superior do painel representam cada aplicativo no portfólio, organizadas pela segmentação recomendada. Cada aplicativo também está listado em uma tabela de dados abaixo dos gráficos, incluindo métricas relevantes para cada aplicativo. Os possíveis segmentos recomendados incluem: • Redefinir a hospedagem: uma recomendação para alterar a configuração da	N/D

Tarefa	Descrição	Habilidades necessárias
	infraestrutura do aplicativo a fim de movê-lo sem alterações (lift-and-shift) para a nuvem usando uma solução de infraestrutura como serviço (IaaS). • Refatorar: uma recomendação para realizar modificações modestas no código do aplicativo sem alterar a arquitetura ou a funcionalidade para que ele possa ser migrado usando uma solução de contêiner como serviço (CaaS) ou plataforma como serviço (PaaS). • Redefinir a arquitetura: uma recomendação para modificar drasticamente o código do aplicativo a fim de aprimorar sua integridade e prepará-lo para a migração usando uma solução PaaS ou implantá-lo como um aplicativo de tecnologia sem servidor usando uma solução de função como serviço (FaaS). • Reconstruir: uma recomendação para descartar o código do aplicativo e desenvolvê-lo novamente na nuvem usando uma solução	

Tarefa	Descrição	Habilidades necessárias
	PaaS ou desenvolvê-lo novamente como um aplicativo de tecnologia sem servidor usando uma solução FaaS. • Retirar: uma recomendação para descartar completamente o aplicativo ou possivelmente substituí-lo por uma alternativa comercial de software como serviço (SaaS).	
Modifique as recomendações de segmentação.	Em alguns casos, você pode optar por alterar o segmento recomendado pelo CAST Highlight. Você pode fazer isso navegando até o aplicativo na tabela de dados e selecionando um segmento diferente na lista suspensa ao lado do nome do aplicativo. Escolha Salvar no canto superior direito para salvar essa alteração. Você também pode exportar esses dados a qualquer momento escolhendo Exportar no canto superior direito.	N/D

Tarefa	Descrição	Habilidades necessárias
Escolha um aplicativo para analisar.	No painel do Portfolio Advisor for Cloud, escolha uma bolha de aplicativo para analisar esse aplicativo. Escolha o nome do aplicativo na tabela após o gráfico de bolhas para iniciar uma análise aprofunda da. Painéis diferentes estão disponíveis para analisar aplicativos individuais, como Insights do código (padrões de integridade de software) , Tendências e Composição de software (riscos de código aberto).	N/D

Tarefa	Descrição	Habilidades necessárias
Analise os CloudReady resultados de uma aplicação individual.	Escolha a CloudReadyguia, que mostra a CloudReady pontuação geral do aplicativo. Essa pontuação é uma média ponderada baseada em uma combinação das respostas da CloudReady pesquisa e da verificação do CloudReady código. As respostas às perguntas da pesquisa aparecem na tabela abaixo dos blocos. Escolha Escaneamento de CloudReady código para ver os resultados do escaneamento de código. Há uma lista de CloudReady padrões pelos quais o código do aplicativo foi escaneado. Essa lista inclui as seguintes colunas: • Requisito de nuvem é o padrão de código específico. • Tecnologia é a linguagem de programação do padrão. “Impacto” é o impacto do padrão no aplicativo (C = código, F = estrutura, A = arquitetura). • Criticidade é o nível de importância da abordagem desse padrão antes da migração.	N/D

Tarefa	Descrição	Habilidades necessárias
	• A contribuição é como esse padrão contribui para a CloudReady pontuação geral. Se o padrão for verde, é um reforço e aumenta a CloudReady pontuação. Se o padrão for vermelho, é um bloqueador e diminui a CloudReady pontuação. Se o padrão não tiver cor, é um bloqueador que não foi detectado e aumenta a CloudReady pontuação. • Obstáculos são o número de ocorrências individuais de um padrão de bloqueador. Escolha o número do obstáculo para mostrar uma lista dos arquivos de código-fonte em que o padrão foi detectado. • Esforço est. é uma estimativa do número de dias necessários para resolver os obstáculos em cada linha.	

Tarefa	Descrição	Habilidades necessárias
Exporte dados para o Microsoft Excel.	(Opcional) Escolha Exportar para Excel para exportar os dados para análise posterior . Os dados dos resultados da análise do aplicativo podem ser usados para analisar em detalhes a prontidão de um aplicativo para a nuvem e determinar qual código deve ser atualizado antes da migração.	N/D
Exibir recomendações.	Escolha Recomendações ao lado de CloudReady Code Scan para ver a tela de Recomendações de Serviços em Nuvem. Identific a os serviços da AWS que o aplicativo poderia adotar com base em suas características. Repita esta etapa para ver as recomendações para todos os aplicativos que você analisou.	N/D

Recursos relacionados

Gerenciamento de campanhas

- Seção 3 do treinamento de certificação básica do CAST Highlight: configuração do portfólio (vídeo)

Análise de código-fonte

- Seção 4 do treinamento de certificação básica do CAST Highlight: análise de aplicativos (vídeo)

Outros recursos

- CAST Highlight no AWS Marketplace
- AWS e CAST: acelere a modernização dos aplicativos
- CAST Highlight: documentação, tutoriais de produtos e ferramentas de terceiros
- CAST Highlight: demonstração do produto com prontidão para a nuvem (vídeo)
- Modernização do portfólio de aplicativos com o CAST Highlight (workshop da AWS)

Arquivar automaticamente itens no Amazon S3 usando o DynamoDB TTL

Criado por Tabby Ward (AWS)

Resumo

Este padrão fornece etapas para remover dados antigos de uma tabela do Amazon DynamoDB e arquivá-los em um bucket do Amazon Simple Storage Service (Amazon S3) no Amazon Web Services (AWS) sem precisar gerenciar uma frota de servidores.

Este padrão usa a configuração de vida útil (TTL) do Amazon DynamoDB para excluir automaticamente itens antigos e o Amazon DynamoDB Streams para capturar itens com TTL expirado. Ele então conecta o DynamoDB Streams ao AWS Lambda, que executa o código sem provisionar ou gerenciar nenhum servidor.

Quando novos itens são adicionados ao stream do DynamoDB, a função Lambda é iniciada e grava os dados em um stream de entrega do Amazon Data Firehose. O Firehose fornece uma solução simples e totalmente gerenciada para carregar os dados como um arquivo no Amazon S3.

O DynamoDB é frequentemente usado para armazenar dados de séries temporais, como dados de fluxo de cliques em páginas da Web ou dados da Internet das Coisas (IoT) de sensores e dispositivos conectados. Em vez de excluir itens acessados com menos frequência, muitos clientes desejam arquivá-los para fins de auditoria. O TTL simplifica esse arquivamento excluindo automaticamente os itens com base no atributo timestamp.

Os itens excluídos pelo TTL podem ser identificados no DynamoDB Streams, que captura uma sequência em ordem temporal de modificações em nível de item e armazena a sequência em um log por até 24 horas. Esses dados podem ser consumidos por uma função do Lambda e arquivados em um bucket do Amazon S3 para reduzir o custo de armazenamento. Para reduzir ainda mais os custos, as regras de ciclo de vida do Amazon S3 podem ser criadas para fazer a transição automática dos dados (assim que eles são criados) para as classes de armazenamento de menor custo, como S3 Glacier Instant Retrieval ou S3 Glacier Flexible Retrieval, ou Amazon S3 Glacier Deep Archive para armazenamento de longo prazo.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa

- AWS Command Line Interface (AWS CLI) 1.7 ou mais recente, instalada e configurada em macOS, Linux ou Windows.
- Python 3.7 ou mais recente.
- Boto3, instalado e configurado. Se o Boto3 ainda não estiver instalado, execute o comando `python -m pip install boto3` para instalá-lo.

Arquitetura

Pilha de tecnologia

- Amazon DynamoDB
- Amazon DynamoDB Streams
- Amazon Data Firehose
- AWS Lambda
- Amazon S3

1. Os itens são excluídos pelo TTL.
2. O trigger do DynamoDB Streams invoca a função de processador de fluxo do Lambda.
3. A função Lambda coloca registros no stream de entrega do Firehose em formato de lote.
4. Os registros de dados são arquivados no bucket do S3.

Ferramentas

- AWS CLI: o AWS Command Line Interface (AWS CLI) é uma ferramenta unificada para gerenciar os serviços da AWS.
- Amazon DynamoDB: o Amazon DynamoDB é um banco de dados de documentos e de chave-valor e documentos que oferece desempenho de um dígito em milissegundos em qualquer escala.
- Vida útil (TTL) do Amazon DynamoDB: o Amazon DynamoDB ajuda a definir uma marca de hora por item para determinar quando um item não é mais necessário.
- Amazon DynamoDB Streams: o Amazon DynamoDB Streams captura uma sequência em ordem temporal de modificações em nível de item em qualquer tabela do DynamoDB e armazena essas informações em um log por até 24 horas.

- Amazon Data Firehose — O Amazon Data Firehose é a maneira mais fácil de carregar dados de streaming de forma confiável em data lakes, armazenamentos de dados e serviços de análise.
- AWS Lambda: o AWS Lambda executa código sem a necessidade de provisionar ou gerenciar servidores. É cobrado apenas o tempo de computação consumido.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade líder do setor, disponibilidade de dados, segurança e performance.

Código

O código desse padrão está disponível no GitHub Arquivamento de itens no S3 usando o repositório TTL do DynamoDB.

Épicos

Configure uma tabela do DynamoDB, TTL e um DynamoDB Streams

Tarefa	Descrição	Habilidades necessárias

Crie uma tabela do DynamoDB.	Use a AWS CLI para criar uma tabela no DynamoDB chamada `Reservation`. Escolha a unidade de capacidade de leitura aleatória (random read capacity unit, RCU) e a unidade de capacidade de gravação (write capacity unit, WCU) e atribua à sua tabela dois atributos: `ReservationID` e `ReservationDate`.
	`aws dynamodb create-table \`
	`--table-name Reservation \`
	`--attribute-definitions Attribute`
		Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`Name=ReservationID ,AttributeType=S AttributeName=Rese rvationDate,Attrib uteType=N \ --key-schema Attribute Name=ReservationID ,KeyType=HASH AttributeName=Rese rvationDate,KeyTyp e=RANGE \ --provisioned-th roughput ReadCapac ityUnits=100,Write CapacityUnits=100` `ReservationDate` é um timestamp de época que será usado para ativar o TTL.	
Ative o TTL do DynamoDB	Use a AWS CLI para ativar o TTL do DynamoDB para o atributo `ReservationDate`. `aws dynamodb update-ti me-to-live \ --table-name Reservati on\ --time-to-live-spe cification Enabled=t rue,AttributeName= ReservationDate`	Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Ative um DynamoDB Streams.	Use a AWS CLI para ativar um DynamoDB Streams para a tabela `Reservation` usando o tipo de fluxo `NEW_AND_OLD_IMAGES`.
	
	`aws dynamodb update-table \`
	`--table-name Reservation \`
	`  --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES`
	
	Esse fluxo conterá registros de novos itens, itens atualizados, itens excluídos e itens excluídos pelo TTL. Os registros dos itens excluídos pelo TTL contêm um atributo de metadados adicional para diferenciá-los dos itens que foram excluídos manualmente. O campo `userIdentity` para exclusões de TTL indica que o serviço do DynamoDB executou a ação de exclusão.
	
	Nesse padrão, somente os itens excluídos pelo TTL são arquivados, mas você pode arquivar somente os registros onde `eventName` é `REMOVE` e `userIdentity`
		Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	contém `principalId` igual a `dynamodb.amazonaws.com` .	

Criação e configuração de um bucket do S3

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Use a AWS CLI para criar um bucket S3 de destino na sua região da AWS, `us-east-1` substituindo-o pela sua região e amzn-s3- demo-destination-bucket pelo nome do seu bucket. `aws s3api create-bucket \ --bucket amzn-s3-demo-destination-bucket \ --region us-east-1` Certifique-se de que o nome do seu bucket do S3 seja globalmente exclusivo, pois o namespace é compartilhado por todas as contas da AWS.	Arquiteto de nuvem, desenvolvedor de aplicativos
Crie uma política de ciclo de vida de 30 dias para o bucket do S3.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon S3. 2. Escolha o bucket do S3 que contém os dados do Firehose.	Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	3. No bucket to S3, escolha a guia Gerenciamento e escolha Adicionar regra de ciclo de vida. 4. Insira um nome para sua regra na caixa de diálogo Regra de ciclo de vida e configure uma regra de ciclo de vida de 30 dias para seu bucket.	

Crie um stream de entrega do Firehose

Tarefa	Descrição	Habilidades necessárias
Crie e configure um stream de entrega do Firehose.	Baixe e edite o exemplo de `CreateFireHoseToS3.py` código do GitHub repositório. Esse código foi escrito em Python e mostra como criar um stream de entrega do Firehose e uma função do AWS Identity and Access Management (IAM). A função do IAM terá uma política que pode ser usada pelo Firehose para gravar no bucket S3 de destino. Para executar o script, use o comando abaixo e os seguintes argumentos da linha de comando.	Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Argumento 1=<Your_S3_bucket_ARN> , que é o nome do recurso da Amazon (ARN) do bucket criado anteriormente Argumento 2= Seu nome Firehose (Este piloto está firehose_to_s3_stream usando.) Argumento 3= nome do seu perfil do IAM (este piloto está usandofirehose_to_s3 .) `python CreateFirehoseToS3.py <Your_S3_Bucket_ARN> firehose_to_s3_stream firehose_to_s3` Se o perfil do IAM especificado não existir, o script criará um perfil assumido com uma política de relacionamento confiável, bem como uma política que conceda permissão suficiente ao Amazon S3. Para obter exemplos dessas políticas, consulte a seção Informações adicionais.	

Tarefa	Descrição	Habilidades necessárias
Verifique o stream de entrega do Firehose.	Descreva o stream de entrega do Firehose usando a AWS CLI para verificar se o stream de entrega foi criado com sucesso. `aws firehose describe-delivery-stream --delivery-stream-name firehose_to_s3_stream`	Arquiteto de nuvem, desenvolvedor de aplicativos

Crie uma função Lambda para processar o stream de entrega do Firehose

Tarefa	Descrição	Habilidades necessárias
Crie uma política de confiança para a função do Lambda.	Crie um arquivo da política de confiança com as seguintes informações. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ]`	Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	<pre>}</pre> Isso dá ao seu perfil permissão para acessar recursos da AWS.	

Crie um perfil de execução para a função do Lambda	Para criar o perfil de execução, execute o seguinte código.
	<pre>aws iam create-role
	--role-name lambda-
	ex --assume-role-poli
	cy-document file://Tr
	ustPolicy.json</pre>
		Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Adicione permissões ao perfil.	Para adicionar permissão para o perfil, use o comando `attach-policy-to-role` .
	
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/IAMFullAccess`
		Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Crie uma função do Lambda.	Comprima o arquivo `LambdaStreamProcessor.py` do repositório de código executando o comando a seguir.
	`zip function.zip LambdaStreamProcessor.py`
	Ao criar a função do Lambda, você precisará do ARN do perfil de execução do Lambda. Para obter o ARN, execute o código a seguir.
	`aws iam get-role \ --role-name lambda-ex`
	Para criar a função do Lambda, execute o seguinte código.
	`# Review the environment variables and replace them with your values.`
	`aws lambda create-function --function-name LambdaStreamProcessor \ --zip-file fileb://function.zip --handler LambdaStreamProcessor.handler --runtime python3.8 \`
		Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`--role {Your Lamda Execution Role ARN}\ --environment Variables="{firehose_name=firehose_to_s3_stream,bucket_arn = <Your_S3_bucket_ARN>,iam_role_name = firehose_to_s3, batch_size=400}"`	
Configure o trigger da função do Lambda.	Use a AWS CLI para configurar o trigger (DynamoDB Streams), que invoca a função do Lambda. O tamanho do lote ser de 400 é para evitar problemas de simultaneidade do Lambda. `aws lambda create-event-source-mapping --function-name LambdaStreamProcessor \ --batch-size 400 --starting-position LATEST \ --event-source-arn <Your Latest Stream ARN From DynamoDB Console>`	Arquiteto de nuvem, desenvolvedor de aplicativos

Teste a funcionalidade

Tarefa	Descrição	Habilidades necessárias
Adicione itens com timestamps expirados à tabela de reservas.	Para testar a funcionalidade, adicione itens com timestamps de época expirados à tabela `Reservation` . O TTL excluirá automaticamente os itens com base no timestamp. A função do Lambda é inicializada nas atividades do DynamoDB Stream e filtra o evento para identificar a atividade `REMOVE` ou itens excluídos. Em seguida, ele coloca os registros no fluxo de entrega do Firehose em formato de lote. O stream de entrega do Firehose transfere itens para um bucket S3 de destino com o prefixo. `firehose os3example/year=current year/month=current month/day=current day/hour=current hour/` **Important** Para otimizar a recuperação de dados, configure o Amazon S3 com `Prefix`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	os `ErrorOutp utPrefix` e que estão detalhados na seção Informações adicionais.	

Limpe os recursos

Tarefa	Descrição	Habilidades necessárias
Excluir todos os recursos.	Excluir todos os recursos para garantir que não será cobrado por nenhum serviço que não esteja usando.	Arquiteto de nuvem, desenvolvedor de aplicativos

Recursos relacionados

- Gerenciando seu ciclo de vida de armazenamento
- Classes de armazenamento do Amazon S3
- AWS SDK para Python (Boto3) documentation

Mais informações

Crie e configure um stream de entrega do Firehose — exemplos de políticas

Documento de exemplo de política de relacionamento confiável da Firehose

```
firehose_assume_role = {
        'Version': '2012-10-17',
        'Statement': [
            {
                'Sid': '',
                'Effect': 'Allow',
                'Principal': {
```

```
                    'Service': 'firehose.amazonaws.com'
                },
                'Action': 'sts:AssumeRole'
            }
        ]
    }
```

Exemplo de política de permissões do S3

```
s3_access = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "",
                "Effect": "Allow",
                "Action": [
                    "s3:AbortMultipartUpload",
                    "s3:GetBucketLocation",
                    "s3:GetObject",
                    "s3:ListBucket",
                    "s3:ListBucketMultipartUploads",
                    "s3:PutObject"
                ],
                "Resource": [
                    "{your s3_bucket ARN}/*",
                    "{Your s3 bucket ARN}"
                ]
            }
        ]
    }
```

Teste a funcionalidade — configuração do Amazon S3

A configuração do Amazon S3 com os seguintes `Prefix` e `ErrorOutputPrefix` é escolhida para otimizar a recuperação de dados.

prefix

```
firehosetos3example/year=! {timestamp: yyyy}/month=! {timestamp:MM}/day=!
 {timestamp:dd}/hour=!{timestamp:HH}/
```

O Firehose primeiro cria uma pasta base chamada `firehosetos3example` diretamente abaixo do bucket do S3. Em seguida, ele avalia as expressões `!{timestamp:yyyy}!{timestamp:MM},!{timestamp:dd},`, e `!{timestamp:HH}` para ano, mês, dia e hora usando o DateTimeFormatterformato Java.

Por exemplo, um timestamp de chegada aproximado de 1604683577 no Unix epoch time avaliado como `year=2020`, `month=11`, `day=06` e `hour=05`. Portanto, a localização no Amazon S3, onde os registros de dados são entregues, é avaliada como `firehosetos3example/year=2020/month=11/day=06/hour=05/`.

ErrorOutputPrefix

```
firehosetos3erroroutputbase/!{firehose:random-string}/!{firehose:error-output-type}/!{timestamp:yyyy/MM/dd}/
```

Os resultados `ErrorOutputPrefix` em uma pasta base chamada `firehosetos3erroroutputbase` diretamente abaixo do bucket do S3. A expressão `!{firehose:random-string}` é avaliada como uma string aleatória de 11 caracteres, como `ztWxkdg3Thg`. A localização de um objeto do Amazon S3 onde os registros com falha são entregues pode ser avaliada como `firehosetos3erroroutputbase/ztWxkdg3Thg/processing-failed/2020/11/06/`.

Crie uma arquitetura sem servidor multilocatário no Amazon Service OpenSearch

Criado por Tabby Ward (AWS) e Nisha Gambhir (AWS)

Resumo

O Amazon OpenSearch Service é um serviço gerenciado que facilita a implantação, a operação e a escalabilidade do Elasticsearch, que é um popular mecanismo de pesquisa e análise de código aberto. OpenSearch O serviço fornece pesquisa de texto livre, bem como ingestão e painéis quase em tempo real para streaming de dados, como registros e métricas.

Os provedores de software como serviço (SaaS) costumam usar o OpenSearch Serviço para lidar com uma ampla variedade de casos de uso, como obter informações sobre os clientes de forma escalável e segura, ao mesmo tempo em que reduzem a complexidade e o tempo de inatividade.

Usar o OpenSearch serviço em um ambiente multilocatário introduz uma série de considerações que afetam o particionamento, o isolamento, a implantação e o gerenciamento de sua solução SaaS. Os provedores de SaaS precisam considerar como escalar efetivamente seus clusters do Elasticsearch com workloads em constante mudança. Eles também precisam considerar como a hierarquização e as condições ruidosas dos vizinhos podem afetar seu modelo de particionamento.

Esse padrão analisa os modelos usados para representar e isolar dados de inquilinos com estruturas do Elasticsearch. Além disso, o padrão se concentra em uma arquitetura de referência simples sem servidor como exemplo para demonstrar a indexação e a pesquisa usando o OpenSearch Service em um ambiente multilocatário. Ele implementa o modelo de particionamento de dados do pool, que compartilha o mesmo índice entre todos os inquilinos, e mantém o isolamento dos dados do inquilino. Esse padrão usa os seguintes AWS serviços: Amazon API Gateway AWS Lambda, Amazon Simple Storage Service (Amazon S3) e Service. OpenSearch

Para obter mais informações sobre o modelo de pool e outros modelos de particionamento de dados, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- AWS Command Line Interface (AWS CLI) versão 2.x, instalada e configurada no macOS, Linux ou Windows

- Python versão 3.9
- pip3: o código-fonte do Python é fornecido como um arquivo .zip para ser implantado em uma função do Lambda. Se você quiser usar o código localmente ou personalizá-lo, siga estas etapas para desenvolver e recompilar o código-fonte:
  1. Gere o `requirements.txt` arquivo executando o seguinte comando no mesmo diretório dos scripts do Python: `pip3 freeze > requirements.txt`
  2. Instale as dependências: `pip3 install -r requirements.txt`

Limitações

- Esse código é executado em Python e atualmente não oferece suporte a outras linguagens de programação.
- O aplicativo de amostra não inclui suporte AWS entre regiões ou recuperação de desastres (DR).
- Este padrão é apenas para fins de demonstração. Não se destina a ser usado em ambientes de produção.

Arquitetura

O diagrama a seguir ilustra a arquitetura de alto nível de arquitetura deste padrão. A arquitetura inclui o seguinte:

- Lambda para indexar e consultar o conteúdo
- OpenSearch Serviço para realizar pesquisas
- API Gateway para fornecer uma interação de API com o usuário
- Amazon S3 para armazenar dados brutos (não indexados)
- Amazon CloudWatch monitorará registros
- AWS Identity and Access Management (IAM) para criar funções e políticas de inquilinos

Automação e escala

Para simplificar, o padrão é usado AWS CLI para provisionar a infraestrutura e implantar o código de amostra. Você pode criar um AWS CloudFormation modelo ou AWS Cloud Development Kit (AWS CDK) scripts para automatizar o padrão.

Ferramentas

Serviços da AWS

- AWS CLIé uma ferramenta unificada para gerenciamento Serviços da AWS e recursos usando comandos em seu shell de linha de comando.
- O Lambda é um serviço de computação que permite executar código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- O API Gateway serve AWS service (Serviço da AWS) para criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- O Amazon S3 é um serviço de armazenamento de objetos que permite armazenar e recuperar qualquer quantidade de informações a qualquer momento, de qualquer lugar na web.
- OpenSearch O Service é um serviço totalmente gerenciado que facilita a implantação, a proteção e a execução do Elasticsearch de maneira econômica e em grande escala.

Código

O anexo fornece arquivos de amostra para esse padrão. Isso inclui:

- `index_lambda_package.zip`— A função Lambda para indexar dados no OpenSearch Service usando o modelo de pool.
- `search_lambda_package.zip`— A função Lambda para pesquisar dados no OpenSearch Service.
- `Tenant-1-data`: amostra de dados brutos (não indexados) para o Tenant-1.
- `Tenant-2-data`: amostra de dados brutos (não indexados) para o Tenant-2.

> **Important**
>
> As histórias desse padrão incluem exemplos de AWS CLI comandos formatados para Unix, Linux e macOS. Para Windows, substitua o caractere de continuação Unix de barra invertida (\) no final de cada linha por um circunflexo (^).

> **Note**
>
> Nos AWS CLI comandos, substitua todos os valores dentro dos colchetes angulares (**<>**) pelos valores corretos.

Épicos

Criação e configuração de um bucket do S3

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Crie um bucket S3 no seu Região da AWS. Esse bucket conterá os dados não indexados do inquilino para o aplicativo de amostra. Certifique-se de que o nome do bucket do S3 seja globalmente exclusivo, pois o namespace é compartilhado por todos. Contas da AWS Para criar um bucket do S3, você pode usar o comando AWS CLI create-bucket da seguinte forma: `aws s3api create-bucket \ --bucket <tenantrawdata> \ --region <your-AWS-Region>` onde `tenantrawdata` é o nome do bucket do S3. (Você pode usar qualquer nome	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	exclusivo que siga as diretrizes de nomenclatura do bucket.)	

Criar e configurar um cluster Elasticsearch

Tarefa	Descrição	Habilidades necessárias

Crie um domínio OpenSearch de serviço.	Execute o AWS CLI create-elasticsearch-domaincomando para criar um domínio OpenSearch de serviço:
	`aws es create-elasticsearch-domain \`
	`  --domain-name vpc-cli-example \`
	`  --elasticsearch-version 7.10 \`
	`  --elasticsearch-cluster-config InstanceType=t3.medium.elasticsearch,InstanceCount=1 \`
	`  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=10 \`
	`  --domain-endpoint-options "{\"EnforceHTTPS\": true}" \`
	`  --encryption-at-rest-options "{\"Enabled\": true}" \`
	`  --node-to-node-encryption-options "{\"Enabled\": true}" \`
	`  --advanced-security-options "{\"Enabl`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	ed\": true, \"Interna lUserDatabaseEnabled \": true, \ \"MasterUserOption s\": {\"MasterUserName \": \"KibanaUser\", \ \"MasterUserPasswo rd\": \"NewKiba naPassword@123\"}}" \ --vpc-options "{\"SubnetIds\": [\"<subnet-id>\"], \"SecurityGroupIds\": [\"<sg-id>\"]}" \ --access-policies "{\"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect\": \"Allow\", \ \"Principal\": {\"AWS\": \"*\" }, \"Action\":\"es:*\", \ \"Resource\": \"arn:aws:es:<regi on>:<account-id>:d omain\/vpc-cli-exa mple\/*\" }] }" A contagem de instâncias é definida como 1 porque o domínio é para fins de teste. Você precisa ativar o controle de acesso refinado usando o `advanced-security-options` parâmetro, pois os detalhes não podem ser	

Tarefa	Descrição	Habilidades necessárias
	alterados após a criação do domínio. Esse comando cria um nome de usuário principal (`KibanaUser`) e uma senha que você usará para fazer login no console do Kibana. Como o domínio faz parte de uma nuvem privada virtual (VPC), você precisa garantir que possa acessar a instância do Elasticsearch especific ando a política de acesso a ser usada. Para obter mais informaçõ es, consulte Lançamento de seus domínios do Amazon OpenSearch Service em uma VPC na AWS documentação.	

Tarefa	Descrição	Habilidades necessárias

Configurar um bastion host.	Configure uma instância Windows da Amazon Elastic Compute Cloud (Amazon EC2) como bastion host para acessar o console Kibana. O grupo de segurança do Elasticsearch deve permitir o tráfego do grupo de EC2 segurança da Amazon. Para obter instruções, consulte a postagem do blog Como controlar o acesso à rede às EC2 instâncias usando um servidor Bastion.
	
	Quando o bastion host tiver sido configurado e você tiver o grupo de segurança associado à instância disponível, use o AWS CLI authorize-security-group-ingresscomando para adicionar permissão ao grupo de segurança do Elasticsearch para permitir a porta 443 do grupo de segurança Amazon EC2 (bastion host).
	
	`aws ec2 authorize-security-group-ingress \`
	`  --group-id <SecurityGroupIdfElasticSearch> \`
	`  --protocol tcp \`
	`  --port 443 \`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	`--source-group <SecurityGroupIdfBashionHostEC2>`	

Criar e configurar a função do Lambda de índice

Tarefa	Descrição	Habilidades necessárias

Criar o perfil de execução do Lambda	Execute o comando AWS CLI create-role para conceder acesso e recursos à função de índice Lambda: Serviços da AWS
	`aws iam create-role \ --role-name index-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	onde `lambda_assume_role.json` está um documento JSON que concede `AssumeRole` permissões para a função Lambda, da seguinte forma:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	"Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }] }	

Tarefa	Descrição	Habilidades necessárias

Anexe as políticas gerenciadas à função do Lambda.	Execute o AWS CLI attach-role-policy comando para anexar políticas gerenciadas à função criada na etapa anterior. Essas duas políticas dão à função permissões para criar uma interface de rede elástica e gravar CloudWatch registros em Logs.
	
	`aws iam attach-role-policy \`
	`  --role-name index-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	
	`aws iam attach-role-policy \`
	`  --role-name index-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

Criar uma política para dar permissão à função de índice Lambda para ler os objetos do S3.	Execute o comando AWS CLI create-policy para dar `s3:GetObject` permissão à função de índice Lambda para ler os objetos no bucket do S3:
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3-policy.json`
	O arquivo `s3-policy.json` é um documento JSON mostrado abaixo que concede `s3:GetObject` permissões para permitir acesso de leitura aos objetos do S3. Se você usou um nome diferente ao criar o bucket do S3, forneça o nome correto do bucket na `Resource` seção:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::<tenantrawdata>/*" }`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	``
	    ]
	}
	``	

Anexar a política de permissões do Amazon S3 ao perfil de execução do Lambda.	Execute o AWS CLI attach-role-policycomando para anexar a política de permissão do Amazon S3 que você criou na etapa anterior à função de execução do Lambda:
	``
	aws iam attach-role-policy \
	  --role-name index-lambda-role \
	  --policy-arn <PolicyARN>
	``
	onde `PolicyARN` é o nome de recurso da nome do recurso da Amazon (ARN) da política de permissões do Amazon S3. É possível obter esse valor na saída do comando anterior.
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

Criar a função do Lambda de índice.	Execute o comando AWS CLI create-function para criar a função de índice Lambda, que acessará o Service: OpenSearch
	
	`aws lambda create-function \`
	`  --function-name index-lambda-function \`
	`  --zip-file fileb://index_lambda_package.zip \`
	`  --handler lambda_index.lambda_handler \`
	`  --runtime python3.9 \`
	`  --role "arn:aws:iam::account-id:role/index-lambda-role" \`
	`  --timeout 30 \`
	`  --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \`
	`  \"SecurityGroupIds\": [\"<sg-1>\"]}"`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Permitir que o Amazon S3 chame a função de índice Lambda.	Execute o comando AWS CLI add-permission para dar ao Amazon S3 a permissão de chamar a função de índice Lambda: `aws lambda add-permission \ --function-name index-lambda-function \ --statement-id s3-permissions \ --action lambda:InvokeFunction \ --principal s3.amazonaws.com \ --source-arn "arn:aws:s3:::<tenantrawdata>" \ --source-account "<account-id>"`	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Adicionar um gatilho Lambda para o evento Amazon S3.	Execute o AWS CLI put-bucket-notification-configuration comando para enviar notificações para a função de índice do Lambda quando o evento do Amazon S3 `ObjectCreated` for detectado. A função de índice é executada sempre que um objeto é carregado no bucket do S3. `aws s3api put-bucket-notification-configuration \ --bucket <tenantrawdata> \ --notification-configuration file://s3-trigger.json` O arquivo `s3-trigger.json` é um documento JSON na pasta atual que adiciona a política de recursos à função do Lambda quando ocorre o evento Amazon S3 `ObjectCreated`.	Arquiteto de nuvem, administrador de nuvem

Criar e configurar a função do Lambda de pesquisa

Tarefa	Descrição	Habilidades necessárias
Criar o perfil de execução do Lambda	Execute o comando AWS CLI create-role para conceder	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	acesso e recursos à função de pesquisa do Lambda: Serviços da AWS
	
	`aws iam create-role \ --role-name search-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	
	onde `lambda_assume_role.json` é um documento JSON na pasta atual que concede `AssumeRole` permissões para a função do Lambda, da seguinte forma:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }`	

Tarefa	Descrição	Habilidades necessárias

Anexe as políticas gerenciadas à função do Lambda.	Execute o AWS CLI attach-role-policy comando para anexar políticas gerenciadas à função criada na etapa anterior. Essas duas políticas dão à função permissões para criar uma interface de rede elástica e gravar CloudWatch registros em Logs.
	
	`aws iam attach-role-policy \`
	`  --role-name search-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	
	`aws iam attach-role-policy \`
	`  --role-name search-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar a função do Lambda de pesquisa.	Execute o comando AWS CLI create-function para criar a função de pesquisa do Lambda, que acessará o Serviço: OpenSearch `aws lambda create-function \ --function-name search-lambda-function \ --zip-file fileb://search_lambda_package.zip \ --handler lambda_search.lambda_handler \ --runtime python3.9 \ --role "arn:aws:iam::account-id:role/search-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Arquiteto de nuvem, administrador de nuvem

Criar e configurar funções de inquilino

Tarefa	Descrição	Habilidades necessárias
Crie o perfil do IAM de inquilino.	Execute o comando AWS CLI create-role para criar duas funções de inquilino que serão usadas para testar a funcionalidade de pesquisa:	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	`aws iam create-role \ --role-name Tenant-1-role \ --assume-role-policy-document file://assume-role-policy.json`	
	`aws iam create-role \ --role-name Tenant-2-role \ --assume-role-policy-document file://assume-role-policy.json`	
	O arquivo `assume-role-policy.json` é um documento JSON na pasta atual que concede `AssumeRole` permissões para o perfil de execução do Lambda:	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "<Lambda execution role for index function>", "AWS": "<Lambda execution role for search function>" }, `	

Tarefa	Descrição	Habilidades necessárias

	<pre>"Action":
	"sts:AssumeRole"
	}
	]
	}</pre>	

Tarefa	Descrição	Habilidades necessárias

Criar uma nova política do IAM	Execute o comando AWS CLI create-policy para criar uma política de locatário que conceda acesso às operações do Elasticsearch:
	`aws iam create-policy \ --policy-name tenant-policy \ --policy-document file://policy.json`
	O arquivo `policy.json` é um documento JSON na pasta atual que concede permissões no Elasticsearch:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpDelete", "es:ESHttpGet", "es:ESHttpHead", "es:ESHttpPost", "es:ESHttpPut", "es:ESHttpPatch" ],`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	<pre>"Resource": ["<ARN of Elasticsearch domain created earlier>"] }] }</pre>	

Anexar a política do IAM do inquilino às funções do inquilino.	Execute o AWS CLI attach-role-policycomando para anexar a política do IAM do inquilino às duas funções de inquilino que você criou na etapa anterior:
	<pre>aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/tenant-policy \ --role-name Tenant-1-role
	
	aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/tenant-policy \ --role-name Tenant-2-role</pre>
	A ARN da política vem da saída na etapa anterior.
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

Criar uma política do IAM para conceder permissões ao Lambda para assumir a função.	Execute o comando AWS CLI create-policy para criar uma política para que o Lambda assuma a função de locatário:
	`aws iam create-policy \ --policy-name assume-tenant-role-policy \ --policy-document file://lambda_policy.json`
	O arquivo `lambda_policy.json` é um documento JSON na pasta atual que concede permissões para o `AssumeRole` :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<ARN of tenant role created earlier>" } ] }`
	Pois`Resource`, você pode usar um caractere curinga para evitar a criação de
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	uma nova política para cada inquilino.	

Criar uma política do IAM para conceder à função do índice do Lambda a permissão para acessar o Amazon S3.	Execute o comando AWS CLI create-policy para dar permissão à função do índice Lambda para acessar os objetos no bucket do S3:
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3_lambda_policy.json`
	O arquivo `s3_lambda_policy.json` é o seguinte documento de política JSON na pasta atual:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::tenantrawdata/*" } ] }`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

Anexar a política a um perfil de execução do Lambda.	Execute o AWS CLI attach-role-policycomando para anexar a política criada na etapa anterior ao índice Lambda e às funções de execução de pesquisa que você criou anteriormente:
	`aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \ --role-name index-lambda-role`
	`aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \ --role-name search-lambda-role`
	`aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/s3-permission-policy \ --role-name index-lambda-role`
	A ARN da política vem da saída na etapa anterior.
		Arquiteto de nuvem, administrador de nuvem

Criar e configurar uma API de pesquisa

Tarefa	Descrição	Habilidades necessárias
Criar uma API REST do API Gateway.	Execute o AWS CLI create-rest-api comando para criar um recurso da API REST: `aws apigateway create-rest-api \ --name Test-Api \ --endpoint-configuration "{ \"types\": [\"REGIONAL\"] }"` Para o tipo de configuração de endpoint, você pode especificar `EDGE` em vez de `REGIONAL` usar locais de borda em vez de um determinado Região da AWS. Anote o valor do campo `id` na saída do comando. Esse é o ID da API que você usará nos comandos subsequentes.	Arquiteto de nuvem, administrador de nuvem
Criar um recurso para a API de pesquisa.	O recurso da API de pesquisa inicia a função de pesquisa do Lambda com o nome do recurso. `search` (Você não precisa criar uma API para a função de índice do Lambda, porque ela é executada automaticamente quando os objetos são carregados no bucket do S3.)	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	1. Execute o comando AWS CLI get-resources para obter o ID principal do caminho raiz:
	
	`aws apigateway get-resources \ --rest-api-id <API-ID>`
	
	Observe o valor do campo ID. Você usará esse ID pai no próximo comando.
	
	`{ "items": [ { "id": "zpsri964ck", "path": "/" } ] }`
	
	2. Execute o comando AWS CLI create-resource para criar um recurso para a API de pesquisa. Para `parent-id`, especifique o ID do comando anterior.
	
	`aws apigateway create-resource \ --rest-api-id <API-ID> \ --parent-id <Parent-ID> \`	

Tarefa	Descrição	Habilidades necessárias
	`--path-part search`	
Criar um método GET para a API de pesquisa.	Execute o comando AWS CLI put-method para criar um `GET` método para a API de pesquisa: `aws apigateway put-method \ --rest-api-id <API-ID> \ --resource-id <ID from the previous command output> \ --http-method GET \ --authorization-type "NONE" \ --no-api-key-required` Para `resource-id`, especificar o ID da saída do `create-resource` comando.	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar um método de resposta para a API de pesquisa.	Execute o AWS CLI put-method-responsecomando para adicionar uma resposta de método para a API de pesquisa: `aws apigateway put-method-response \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --status-code 200 \ --response-models "{\"application/json\": \"Empty\"}"` Para`resource-id` , especifique o ID da saída do `create-resource` comando anterior.	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Configurar uma integração de proxy Lambda para a API de pesquisa.	Execute o comando AWS CLI put-integration para configurar uma integração com a função de pesquisa do Lambda: `aws apigateway put-integration \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --type AWS_PROXY \ --integration-http-method GET \ --uri arn:aws:apigateway:region:lambda:path/2015-03-31/functions/arn:aws:lambda:<region>:<account-id>:function:<function-name>/invocations`  Para `resource-id`, especifique o ID do `create-resource` comando anterior.	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Conceder permissão para que o API Gateway possa invocar a função do Lambda.	Execute o comando AWS CLI add-permission para dar permissão ao API Gateway para usar a função de pesquisa: `aws lambda add-permission \ --function-name <function-name> \ --statement-id apigateway-get \ --action lambda:InvokeFunction \ --principal apigateway.amazonaws.com \ --source-arn "arn:aws:execute-api:<region>:<account-id>:api-id/*/GET/search"` Alterar o `source-arn` caminho se você usou um nome de recurso de API diferente em vez de `search`.	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

Implantar a API de pesquisa.	Execute o comando AWS CLI create-deployment para criar um recurso de estágio chamado: `dev`
	
	`aws apigateway create-deployment \`
	`  --rest-api-id <API-ID> \`
	`  --stage-name dev`
	
	Se você atualizar a API, poderá usar o mesmo AWS CLI comando para reimplantá-la no mesmo estágio.
		Arquiteto de nuvem, administrador de nuvem

Criar e configurar funções do Kibana

Tarefa	Descrição	Habilidades necessárias
Fazer login no console do Kibana.	1. Encontre o link para o Kibana no painel do seu domínio no console de OpenSearch serviços. O URL está no formato:`<domain-endpoint>/_plugin/kibana/` . 2. Use o bastion host que você configurou no primeiro épico para acessar o console Kibana. 3. Faça login no console do Kibana usando o nome de	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	usuário principal e a senha da etapa anterior, quando você criou o domínio do OpenSearch Serviço. 4. Quando solicitado a escolher um inquilino, escolha Privado.	

Tarefa	Descrição	Habilidades necessárias
Criar e configurar perfis do Kibana	Para fornecer isolamento de dados e garantir que um inquilino não possa recuperar os dados de outro inquilino, você precisa usar a segurança de documentos, que permite que os inquilinos acessem somente documentos que contenham sua ID de inquilino . 1. No console do Kibana, no painel de navegação , escolha Segurança, Função. 2. Criar um novo perfil de inquilino. 3. Defina permissões de cluster como`indices_all` , o que dá permissões de criação, leitura, atualização e exclusão (CRUD) no índice OpenSearch de serviços. 4. Restringir as permissões do `tenant-data` índice ao índice. (O nome do índice deve corresponder ao nome nas funções de pesquisa e indexação do Lambda.) 5. Definir permissões de índice como`indices_all` , para permitir que os usuários realizem todas	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	as operações relacionadas ao índice. (Você pode restringir as operações para obter um acesso mais granular, dependendo de suas necessidades.) 6. Para segurança em nível de documento, use a política a seguir para filtrar documentos por ID de inquilino, para fornecer isolamento de dados para inquilinos em um índice compartilhado: `{ "bool": { "must": { "match": { "TenantId": "Tenant-1" } } } }` O nome, as propriedades e os valores do índice diferenciam maiúsculas de minúsculas.	

Tarefa	Descrição	Habilidades necessárias
Mapear usuários para funções.	1. Escolher a guia Usuários mapeados para a função e, em seguida, escolha Mapear usuários. 2. Na seção Funções de backend, especifique o ARN da função de inquilino do IAM que você criou anteriormente e escolha Mapa. Isso mapeia a função de inquilino do IAM para a função Kibana para que a pesquisa específica do inquilino retorne dados somente desse inquilino. Por exemplo, se o nome do perfil do IAM para Tenant-1 for`Tenant-1-Role` , especifique o ARN para `Tenant-1-Role` (do épico Criar e configurar funções de inquilino) na caixa Funções de backend para a função Tenant-1 Kibana. 3. Repetir as etapas 1 e 2 para o Locatário-2. Recomendamos automatizar a criação das funções de inquilino e Kibana no momento da integração do inquilino.	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar o índice de dados do inquilino.	No painel de navegação, em Gerenciamento, escolha Dev Tools e execute o seguinte comando. Esse comando cria o `tenant-data` índice para definir o mapeamento da `TenantId` propriedade. `PUT /tenant-data { "mappings": { "properties": { "TenantId": { "type": "keyword"} } } }`	Arquiteto de nuvem, administrador de nuvem

Crie endpoints VPC para o Amazon S3 e AWS STS

Tarefa	Descrição	Habilidades necessárias
Crie uma política de endpoint da VPC para o Amazon S3.	Execute o AWS CLI create-vpc-endpointcomando para criar um VPC endpoint para o Amazon S3. O endpoint permite que a função de índice Lambda na VPC acesse o Amazon S3. `aws ec2 create-vpc-endpoint \ --vpc-id <VPC-ID> \ --service-name com.amazonaws.us-east-1.s3 \`	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	`--route-table-ids <route-table-ID>` Para `vpc-id`, especificar a VPC que você está usando para a função de índice Lambda. Para `service-name`, use a URL correta para o endpoint do Amazon S3. Para `route-table-ids`, especifique a tabela de rotas associada ao endpoint da VPC.	

Tarefa	Descrição	Habilidades necessárias

Crie um VPC endpoint para. AWS STS	Execute o AWS CLI create-vpc-endpointcomando para criar um VPC endpoint para AWS Security Token Service ().AWS STS O endpoint permite que as funções de indexação e pesquisa do Lambda na VPC acessem. AWS STS As funções são usadas AWS STS quando assumem a função do IAM.
	
	`aws ec2 create-vpc-endpoint \`
	`  --vpc-id <VPC-ID> \`
	`  --vpc-endpoint-type Interface \`
	`  --service-name com.amazonaws.us-east-1.sts \`
	`  --subnet-id <subnet-ID> \`
	`  --security-group-id <security-group-ID>`
	
	Para`vpc-id`, especificar a VPC que você está usando para a função do Lambda de índice e pesquisa. Para`subnet-id` , fornecer a sub-rede na qual esse endpoint deve ser criado. Para`security-group-id`, especifique o grupo de segurança ao qual associar esse endpoint. (Pode ser
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	o mesmo que o grupo de segurança que o Lambda usa.)	

Testar a multilocação e o isolamento de dados

Tarefa	Descrição	Habilidades necessárias
Atualizar os arquivos Python para as funções de índice e pesquisa.	1. No `index_lambda_package.zip` arquivo, edite o `lamba_index.py` arquivo para atualizar o Conta da AWS ID e as informações do endpoint do Elasticsearch. Região da AWS 2. No `search_lambda_package.zip` arquivo, edite o `lambda_search.py` arquivo para atualizar o Conta da AWS ID e as informações do endpoint do Elasticsearch. Região da AWS Você pode obter o endpoint do Elasticsearch na guia Visão geral do console de serviços. OpenSearch Ele tem o formato `<AWS-Regi`	Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	on>.es.amazonaws.com .	

Criar o código do Lambda.	Use o AWS CLI update-function-codecomando para atualizar o código Lambda com as alterações feitas nos arquivos Python:
	`aws lambda update-function-code \`
	`  --function-name index-lambda-function \`
	`  --zip-file fileb://index_lambda_package.zip`
	
	`aws lambda update-function-code \`
	`  --function-name search-lambda-function \`
	`  --zip-file fileb://search_lambda_package.zip`
		Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

Fazer upload do arquivo de dados brutos em um bucket do S3.	Use o comando AWS CLI cp para carregar dados dos objetos Tenant-1 e Tenant-2 no `tenantrawdata` bucket (especifique o nome do bucket do S3 que você criou para essa finalidade):
	`aws s3 cp tenant-1-data s3://tenantrawdata`
	`aws s3 cp tenant-2-data s3://tenantrawdata`
	O bucket do S3 é configurado para executar a função de índice do Lambda sempre que os dados são carregados para que o documento seja indexado no Elasticsearch.
		Arquiteto de nuvem, administrador de nuvem

Pesquisar dados no console Kibana.	No console do Kibana, execute a seguinte consulta: `GET tenant-data/_search` Essa consulta exibe todos os documentos indexados no Elasticsearch. Nesse caso, você deve ver dois documentos separados para o Locatário-1 e o Locatário-2.	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

Testar a API de pesquisa do API Gateway.	1. No console do API Gateway, abra a API de pesquisa, escolha o `GET` método dentro do recurso de pesquisa e escolha Testar.
	2. Na janela de teste, forneça a seguinte sequência de caracteres de consulta (com distinção entre maiúsculas e minúsculas) para o ID do inquilino e escolha Testar.
	`TenantId=Tenant-1`
	A função Lambda envia uma consulta ao OpenSearch Service que filtra o documento do locatário com base na segurança em nível do documento. O método retorna o documento que pertence ao Tenant-1.
	3. Alterar a string de consulta para:
	`TenantId=Tenant-2`
	Essa consulta retorna o documento que pertence ao Tenant-2.
		Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Para ver ilustrações de tela, consulte a seção Informações adicionais.	
Limpar recursos.	Limpe todos os recursos que você criou para evitar cobranças adicionais em sua conta.	AWS DevOps, arquiteto de nuvem, administrador de nuvem

Recursos relacionados

- AWS SDK for Python (Boto)
- AWS Lambda documentação
- Documentação do API Gateway
- Documentação do Amazon S3
- Documentação OpenSearch do Amazon Service
  - Controle de acesso refinado no Amazon Service OpenSearch
  - Criação de um aplicativo de pesquisa com o Amazon OpenSearch Service
  - Lançamento de seus domínios OpenSearch do Amazon Service em uma VPC

Mais informações

Modelos de particionamento de dados

Existem três modelos comuns de particionamento de dados usados em sistemas multilocatários: silo, pool e híbrido. O modelo escolhido depende das necessidades de conformidade, vizinhança ruidosa, operações e isolamento do seu ambiente.

Modelo de silo

No modelo de silo, os dados de cada inquilino são armazenados em uma área de armazenamento distinta, onde não há mistura de dados do inquilino. Você pode usar duas abordagens para implementar o modelo de silo com o OpenSearch Service: domínio por inquilino e índice por inquilino.

- Domínio por inquilino — Você pode usar um domínio de OpenSearch serviço separado (sinônimo de um cluster do Elasticsearch) por locatário. Colocar cada inquilino em seu próprio domínio oferece todos os benefícios associados a ter dados em uma estrutura independente. No entanto, essa abordagem apresenta desafios de gerenciamento e agilidade. Sua natureza distribuída torna mais difícil agregar e avaliar a saúde operacional e a atividade dos inquilinos. Essa é uma opção cara que exige que cada domínio de OpenSearch serviço tenha, no mínimo, três nós principais e dois nós de dados para cargas de trabalho de produção.

- Índice por inquilino — Você pode colocar os dados do inquilino em índices separados dentro de um OpenSearch cluster de serviços. Com essa abordagem, você usa um identificador de inquilino ao criar e nomear o índice, anexando o identificador de inquilino ao nome do índice. A abordagem de índice por inquilino ajuda você a atingir suas metas de silo sem introduzir um cluster completamente separado para cada inquilino. No entanto, você pode enfrentar pressão de memória se o número de índices aumentar, porque essa abordagem requer mais fragmentos e o nó principal precisa lidar com mais alocação e rebalanceamento.

Isolamento no modelo de silo: no modelo de silo, você usa políticas do IAM para isolar os domínios ou índices que contêm os dados de cada inquilino. Essas políticas impedem que um inquilino acesse os dados de outro inquilino. Para implementar seu modelo de isolamento de silo, você pode criar uma política baseada em recursos que controle o acesso ao seu recurso de inquilino. Geralmente, essa é uma política de acesso ao domínio que especifica quais ações um principal pode realizar nos sub-recursos do domínio, incluindo índices do Elasticsearch e. APIs Com as políticas baseadas em identidade do IAM, você pode especificar ações permitidas ou negadas no domínio, nos índices ou no Serviço. APIs OpenSearch O `Action` elemento de uma política do IAM descreve a ação ou ações específicas que são permitidas ou negadas pela política, e o `Principal` elemento especifica as contas, os usuários ou os papéis afetados.

O exemplo de política a seguir concede ao Tenant-1 acesso total (conforme especificado por`es:*`) somente aos sub-recursos no `tenant-1` domínio. O `/*` no elemento `Resource` à direita é significativo e indica que as políticas se aplicam aos sub-recursos do domínio, e não ao próprio domínio. Quando essa política está em vigor, os inquilinos não têm permissão para criar um novo domínio ou modificar as configurações em um domínio existente.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::<aws-account-id>:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:<Region>:<account-id>:domain/tenant-1/*"
      }
   ]
}
```

Para implementar o modelo de silo de inquilino por índice, você precisaria modificar esse exemplo de política para restringir ainda mais o Tenant-1 ao índice ou índices especificados, especificando o nome do índice. O exemplo de política a seguir restringe o Tenant-1 ao índice. `tenant-index-1`

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:<Region>:<account-id>:domain/test-domain/tenant-
index-1/*"
      }
   ]
}
```

Modelo de piscina

No modelo de pool, todos os dados do inquilino são armazenados em um índice dentro do mesmo domínio. O identificador do inquilino é incluído nos dados (documento) e usado como chave de partição, para que você possa determinar quais dados pertencem a qual inquilino. Esse modelo reduz a sobrecarga de gerenciamento. Operar e gerenciar o índice agrupado é mais fácil e eficiente do que gerenciar vários índices. No entanto, como os dados do inquilino são misturados no mesmo

índice, você perde o isolamento natural do inquilino que o modelo de silo fornece. Essa abordagem também pode degradar o desempenho devido ao efeito de vizinhança ruidosa.

Isolamento do inquilino no modelo do pool: em geral, o isolamento do inquilino é um desafio de implementar no modelo do pool. O mecanismo do IAM usado com o modelo de silo não permite que você descreva o isolamento com base na ID do inquilino armazenada em seu documento.

Uma abordagem alternativa é usar o suporte de controle de acesso refinado (FGAC) fornecido pela Open Distro for Elasticsearch. O FGAC permite controlar permissões em um nível de índice, documento ou campo. Com cada solicitação, o FGAC avalia as credenciais do usuário e autentica o usuário ou nega o acesso. Se o FGAC autenticar o usuário, ele obterá todas as funções mapeadas para esse usuário e usará o conjunto completo de permissões para determinar como lidar com a solicitação.

Para obter o isolamento necessário no modelo agrupado, você pode usar a segurança em nível de documento, que permite restringir uma função a um subconjunto de documentos em um índice. O exemplo de função a seguir restringe as consultas ao Tenant-1. Ao aplicar essa função ao Tenant-1, você pode obter o isolamento necessário.

```
{
   "bool": {
     "must": {
       "match": {
         "tenantId": "Tenant-1"
       }
     }
   }
 }
```

Modelo híbrido

O modelo híbrido usa uma combinação dos modelos de silo e piscina no mesmo ambiente para oferecer experiências únicas para cada nível de inquilino (como níveis gratuito, padrão e premium). Cada camada segue o mesmo perfil de segurança usado no modelo de pool.

Isolamento do inquilino no modelo híbrido: no modelo híbrido, você segue o mesmo perfil de segurança do modelo de pool, em que o uso do modelo de segurança do FGAC no nível

do documento proporcionou o isolamento do inquilino. Embora essa estratégia simplifique o gerenciamento de clusters e ofereça agilidade, ela complica outros aspectos da arquitetura. Por exemplo, seu código exige complexidade adicional para determinar qual modelo está associado a cada inquilino. Você também precisa garantir que as consultas de um único inquilino não saturem o domínio inteiro e prejudiquem a experiência de outros locatários.

Teste no API Gateway

Janela de teste para consulta Tenant-1

Janela de teste para consulta Tenant-2

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Implante aplicativos de várias pilhas usando o AWS CDK com TypeScript

Criado pelo Dr. Rahul Sharad Gaikwad (AWS)

Resumo

Esse padrão fornece uma step-by-step abordagem para implantação de aplicativos na Amazon Web Services (AWS) usando o AWS Cloud Development Kit (AWS CDK) com TypeScript. Como exemplo, o padrão implanta um aplicativo de análise em tempo real com tecnologia sem servidor.

O padrão cria e implanta aplicativos de pilha aninhados. A pilha principal da AWS chama a CloudFormation pilha secundária, ou aninhada, de pilhas. Cada pilha secundária cria e implanta os recursos da AWS que estão definidos na pilha. CloudFormation O AWS CDK Toolkit, o comando da interface de linha de comando (CLI)`cdk`, é a interface principal das pilhas. CloudFormation

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Nuvem privada virtual (VPC) e sub-redes existentes
- AWS CDK Toolkit instalado e configurado
- Um usuário com permissões de administrador e um conjunto de chaves de acesso.
- Node.js
- AWS Command Line Interface (AWS CLI)

Limitações

- Como o AWS CDK usa a AWS CloudFormation, os aplicativos do AWS CDK estão sujeitos a cotas de CloudFormation serviço. Para obter mais informações, consulte as CloudFormation cotas da AWS.

Versões do produto

Esse padrão foi criado e testado usando as seguintes ferramentas e versões.

- Kit de ferramentas do AWS CDK 1.83.0
- Node.js 14.13.0

- npm 7.0.14

O padrão deve funcionar com qualquer versão do AWS CDK ou npm. Observe que as versões 13.0.0 a 13.6.0 do Node.js não são compatíveis com o AWS CDK.

Arquitetura

Pilha de tecnologias de destino

- AWS Amplify Console
- Amazon API Gateway
- AWS CDK
- Amazon CloudFront
- Amazon Cognito
- Amazon DynamoDB
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)

Arquitetura de destino

O diagrama a seguir mostra a implantação de aplicativos em várias pilhas usando o AWS CDK com. TypeScript

O diagrama a seguir mostra a arquitetura do exemplo de aplicação em tempo real com tecnologia sem servidor.

Ferramentas

Ferramentas

- O AWS Amplify Console é o centro de controle para implantações completas de aplicativos móveis e web na AWS. O host do Amplify Console fornece um fluxo de trabalho baseado em git para

hospedar aplicativos web fullstack com tecnologia sem servidor com implantação contínua. A UI Admin é uma interface visual para desenvolvedores web e móveis frontend criarem e gerenciarem backends de aplicativos fora do console da AWS.

- O Amazon API Gateway é um serviço da AWS para criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- O AWS CDK Toolkit é um kit de desenvolvimento em nuvem de linha de comando que ajuda você a interagir com seu aplicativo AWS CDK. O comando `cdk` CLI é a principal ferramenta para interagir com seu aplicativo AWS CDK. Ele executa seu aplicativo, interroga o modelo de aplicativo que você definiu e produz e implanta os CloudFormation modelos da AWS gerados pelo CDK da AWS.
- CloudFrontA Amazon é um serviço web que acelera a distribuição de conteúdo web estático e dinâmico, como arquivos.html, .css, .js e imagens. CloudFront entrega seu conteúdo por meio de uma rede mundial de data centers chamados de pontos de presença para menor latência e melhor desempenho.
- O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para seus aplicativos Web e móveis. Seus usuários podem fazer login diretamente ou por meio de terceiros.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade integrada.
- O Amazon Data Firehose é um serviço totalmente gerenciado para fornecer dados de streaming em tempo real para destinos como Amazon S3, Amazon Redshift, OpenSearch Amazon Service, Splunk e qualquer endpoint HTTP personalizado ou endpoints HTTP de propriedade de provedores de serviços terceirizados compatíveis.
- O Amazon Kinesis Data Streams é um serviço para coleta e processamento de grandes fluxos de registros de dados em tempo real.
- O AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Código

O código desse padrão está anexado.

Épicos

Instale o AWS CDK Toolkit

Tarefa	Descrição	Habilidades necessárias
Instale o AWS CDK Toolkit.	Para instalar o AWS CDK Toolkit globalmente, execute o comando a seguir. `npm install -g aws-cdk`	DevOps
Verificar a versão.	Para verificar a versão do AWS CDK Toolkit, execute o comando a seguir. `cdk --version`	DevOps

Configurar credenciais da AWS

Tarefa	Descrição	Habilidades necessárias

Configurar credenciais.	Para configurar as credencia is, execute o comando `aws configure` e siga as instruções.
	`$aws configure`
	`AWS Access Key ID`
	`[None]:`
	`AWS Secret Access Key`
	`[None]: your_secr`
	`et_access_key`
	`Default region name`
	`[None]:`
		DevOps

Tarefa	Descrição	Habilidades necessárias
	`Default output format [None]:`	

Baixe o código do projeto

Tarefa	Descrição	Habilidades necessárias
Baixe o código do projeto em anexo.	Para obter mais informações sobre a estrutura de diretórios e arquivos, consulte a seção Informações adicionais.	DevOps

Faça o bootstrap do ambiente do AWS CDK

Tarefa	Descrição	Habilidades necessárias
Faça o bootstrap do ambiente.	Para implantar o CloudFormation modelo da AWS na conta e na região da AWS que você deseja usar, execute o comando a seguir. `cdk bootstrap <account>/<Region>` Para obter mais informações, consulte a documentação da AWS.	DevOps

Crie e implante o projeto

Tarefa	Descrição	Habilidades necessárias
Crie o projeto.	Para construir o código do projeto, execute o comando `npm run build`.	DevOps
Implante o projeto.	Para implantar o código do projeto, execute o comando `cdk deploy`.	

Verificar as saídas

Tarefa	Descrição	Habilidades necessárias
Verifique a criação da pilha.	No AWS Management Console, escolha CloudFormation. Nas pilhas do projeto, verifique se uma pilha principal e duas pilhas secundárias foram criadas.	DevOps

Teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Enviar dados ao Kinesis Data Streams.	Configure sua conta da AWS para enviar dados para o Kinesis Data Streams usando o Amazon Kinesis Data Generator (KDG). Para obter mais informações, consulte Amazon Kinesis Data Generator.	DevOps

Tarefa	Descrição	Habilidades necessárias
Crie um usuário do Amazon Cognito.	Para criar um usuário do Amazon Cognito, baixe o CloudFormation modelo cognito-setup.json na seção Criar um usuário do Amazon Cognito na página de ajuda do Kinesis Data Generator. Inicie o modelo e, em seguida, insira seu nome de usuário e senha do Amazon Cognito. A guia Outputs (Saídas) lista o URL do Kinesis Data Generator.	DevOps
Faça o login no Kinesis Data Generator	Para fazer login no KDG, use as credenciais do Amazon Cognito que você forneceu e o URL do Kinesis Data Generator.	DevOps
Testar o aplicativo.	No KDG, em Modelo de registro, Modelo 1, cole o código de teste na seção Informações adicionais e selecione Enviar dados.	DevOps
Teste o API Gateway.	Depois que os dados forem ingeridos, teste o API Gateway usando o método `GET` para recuperar dados.	DevOps

Recursos relacionados

Referências

- Nuvem AWS Development Kit
- AWS CDK em GitHub
- Trabalhar com pilhas aninhadas
- Exemplo de exemplo da AWS – Análise em tempo real com tecnologia sem servidor

Mais informações

Detalhes do diretório e do arquivo

Esse padrão configura as três pilhas a seguir.

- `parent-cdk-stack.ts`: essa pilha atua como pilha principal e chama os dois aplicativos secundários de pilhas aninhadas.
- `real-time-analytics-poc-stack.ts`: essa pilha aninhada contém a infraestrutura e o código do aplicativo.
- `real-time-analytics-web-stack.ts`: essa pilha aninhada contém somente o código estático do aplicativo web.

Arquivos importantes e suas funcionalidades

- `bin/real-time-analytics-poc.ts`: ponto de entrada do aplicativo AWS CDK. Ele carrega todas as pilhas definidas em `lib/`.
- `lib/real-time-analytics-poc-stack.ts`: definição da pilha (`real-time-analytics-poc`) do aplicativo AWS CDK.
- `lib/real-time-analytics-web-stack.ts`: definição da pilha (`real-time-analytics-web-stack`) do aplicativo AWS CDK.
- `lib/parent-cdk-stack.ts`: definição da pilha (`parent-cdk`) do aplicativo AWS CDK.
- `package.json`: manifesto do módulo npm, que inclui o nome, a versão e as dependências do aplicativo.
- `package-lock.json`: mantido pelo npm.
- `cdk.json`: kit de ferramentas para executar o aplicativo.
- `tsconfig.json`— A TypeScript configuração do projeto.
- `.gitignore`: lista de arquivos que o Git deve excluir do controle de origem.
- `node_modules`: mantido pelo npm; inclui as dependências do projeto.

A seção de código a seguir na pilha principal chama os aplicativos secundários como pilhas de CDK aninhadas da AWS.

```
import * as cdk from '@aws-cdk/core';
import { Construct, Stack, StackProps } from '@aws-cdk/core';
import { RealTimeAnalyticsPocStack } from './real-time-analytics-poc-stack';
import { RealTimeAnalyticsWebStack } from './real-time-analytics-web-stack';


export class CdkParentStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);


    new RealTimeAnalyticsPocStack(this, 'RealTimeAnalyticsPocStack');
    new RealTimeAnalyticsWebStack(this, 'RealTimeAnalyticsWebStack');
  }
}
```

Código para teste

```
session={{date.now('YYYYMMDD')}}|sequence={{date.now('x')}}|
reception={{date.now('x')}}|instrument={{random.number(9)}}|
l={{random.number(20)}}|price_0={{random.number({"min":10000,
 "max":30000})}}|price_1={{random.number({"min":10000, "max":30000})}}|
price_2={{random.number({"min":10000, "max":30000})}}|
price_3={{random.number({"min":10000, "max":30000})}}|
price_4={{random.number({"min":10000, "max":30000})}}|
price_5={{random.number({"min":10000, "max":30000})}}|
price_6={{random.number({"min":10000, "max":30000})}}|
price_7={{random.number({"min":10000, "max":30000})}}|
price_8={{random.number({"min":10000, "max":30000})}}|
```

Teste o API Gateway

No console do API Gateway, teste o API Gateway usando o método `GET`.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Automatize a implantação de aplicativos aninhados usando o AWS SAM

Criado pelo Dr. Rahul Sharad Gaikwad (AWS), Dmitry Gulin (AWS), Ishwar Chauthaiwale (AWS) e Tabby Ward (AWS)

Resumo

Na Amazon Web Services (AWS), o AWS Serverless Application Model (AWS SAM) é uma estrutura de código aberto que fornece sintaxe abreviada para expressar APIs funções, bancos de dados e mapeamentos de fontes de eventos. Com apenas algumas linhas para cada recurso, você pode definir o aplicativo desejado e modelá-lo usando YAML. Durante a implantação, o SAM transforma e expande a sintaxe do SAM na sintaxe da AWS CloudFormation , que você pode usar para criar aplicativos sem servidor com mais rapidez.

O AWS SAM simplifica o desenvolvimento, a implantação e o gerenciamento de aplicativos com tecnologia sem servidor na plataforma da AWS. Ele fornece uma estrutura padronizada, implantação mais rápida, recursos de teste locais, gerenciamento de recursos, integração perfeita com ferramentas de desenvolvimento e uma comunidade de apoio. Esses recursos o tornam uma ferramenta valiosa para criar aplicativos com tecnologia sem servidor de forma eficiente e eficaz.

Esse padrão usa modelos do AWS SAM para automatizar a implantação de aplicativos aninhados. Um aplicativo aninhado é um aplicativo dentro de outro aplicativo. Os aplicativos principais chamam os aplicativos secundários. Esses são componentes com acoplamento fraco de uma arquitetura com tecnologia sem servidor.

Usando aplicativos aninhados, você pode criar rapidamente arquiteturas com tecnologia sem servidor altamente sofisticadas reutilizando serviços ou componentes criados e mantidos de forma independente, mas compostos usando o AWS SAM e o Serverless Application Repository. Os aplicativos aninhados ajudam você a criar aplicativos mais poderosos, evitar a duplicação de trabalho e garantir a consistência e as melhores práticas em suas equipes e organizações. Para demonstrar aplicativos aninhados, o padrão implanta um exemplo de aplicativo de carrinho de compras com tecnologia sem servidor da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) e sub-redes existentes

- Um ambiente de desenvolvimento integrado, como o Visual Studio Code (para obter mais informações, consulte Ferramentas para criar na AWS)
- Biblioteca Python wheel instalada usando pip install wheel, se ainda não estiver instalada

Limitações

- O número máximo de aplicativos que podem ser aninhados em um aplicativo com tecnologia sem servidor é 200.
- O número máximo de parâmetros para um aplicativo aninhado pode ter 60.

Versões do produto

- Essa solução foi criada na interface de linha de comando do AWS SAM (AWS SAM CLI) versão 1.21.1, mas essa arquitetura deve funcionar com versões posteriores da CLI do AWS SAM.

Arquitetura

Pilha de tecnologias de destino

- Amazon API Gateway
- AWS SAM
- Amazon Cognito
- Amazon DynamoDB
- AWS Lambda
- Fila do Amazon Simple Queue Service (Amazon SQS)

Arquitetura de destino

O diagrama a seguir mostra como as solicitações dos usuários são feitas aos serviços de compras por meio de chamadas APIs. A solicitação do usuário, incluindo todas as informações necessárias, é enviada ao Amazon API Gateway e ao autorizador do Amazon Cognito, que executa mecanismos de autenticação e autorização para o. APIs

Quando um item é adicionado, excluído ou atualizado no DynamoDB, um evento é colocado no DynamoDB Streams, que por sua vez inicia uma função do Lambda. Para evitar a exclusão imediata

de itens antigos como parte de um fluxo de trabalho síncrono, as mensagens são colocadas em uma fila SQS, que inicia uma função de trabalho para excluir as mensagens.

Nessa configuração da solução, a CLI do AWS SAM serve como interface para pilhas da AWS CloudFormation . Os modelos do AWS SAM implantam automaticamente aplicativos aninhados. O modelo principal do SAM chama os modelos secundários e a pilha principal implanta as CloudFormation pilhas secundárias. Cada pilha secundária cria os recursos da AWS que são definidos nos modelos do AWS SAM CloudFormation .

1. Compile e implante as pilhas.
2. A CloudFormation pilha Auth contém o Amazon Cognito.
3. A CloudFormation pilha de produtos contém uma função Lambda e o Amazon API Gateway
4. A CloudFormation pilha de compras contém uma função Lambda, o Amazon API Gateway, a fila SQS e o banco de dados Amazon DynamoDB.

Ferramentas

Ferramentas

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para suas aplicações Web e móveis.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Serverless Application Model (AWS SAM) é uma estrutura de código aberto que ajuda na criação de aplicativos com tecnologia sem servidor na Nuvem AWS.

- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.

Código

O código desse padrão está disponível no repositório GitHub AWS SAM Nested Stack Sample.

Épicos

Instalar a AWS SAM CLI

Tarefa	Descrição	Habilidades necessárias
Instale a AWS SAM CLI.	Para instalar a CLI do AWS SAM, consulte as instruções na documentação do AWS SAM.	DevOps engenheiro

Configurar credenciais da AWS.	Para definir as credenciais da AWS para que a CLI do AWS SAM possa fazer chamadas para os serviços da AWS em seu nome, execute o comando `aws configure` e siga as instruções.
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: your_secret_access_key`
	`Default region name [None]:`
	`Default output format [None]:`
	Para obter mais informações sobre como configurar
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	suas credenciais e autentica ção, consulte Credenciais de autenticação e acesso.	

Inicialize o projeto AWS SAM

Tarefa	Descrição	Habilidades necessárias

Clone o repositório de códigos do AWS SAM.	1. Clone o repositório de amostra aws sam nested stack para esse padrão digitando o comando a seguir.
	`git clone https://github.com/aws-samples/aws-sam-nested-stack-sample.git`
	2. Navegue até o diretório clonado inserindo o comando a seguir.
	`cd aws-sam-nested-stack-sample`
		DevOps engenheiro

Implante modelos para inicializar o projeto.	Para inicializar o projeto, execute o comando `SAM init`. Quando solicitado a escolher uma origem de modelo, escolha `Custom Template Location`.	DevOps engenheiro

Compile e crie o código do modelo SAM

Tarefa	Descrição	Habilidades necessárias
Analise os modelos de aplicativos do AWS SAM.	Analise os modelos dos aplicativos aninhados. Este exemplo usa os seguintes modelos de aplicativos aninhados: • `auth.yaml` : esse modelo configura recursos relacionados à autenticação, como o Amazon Cognito e o AWS Systems Manager Parameter Store. • `product-mock.yaml` : esse modelo implanta recursos relacionados ao produto, como funções do Lambda e Amazon API Gateway. • `shoppingcart-service.yaml` : esse modelo configura recursos relacionados ao carrinho de compras, como AWS Identity and Access Management (IAM), tabelas do DynamoDB e funções do Lambda.	DevOps engenheiro
Analise o modelo principal.	Analise o modelo que invocará os modelos de aplicativos aninhados. Neste exemplo, o modelo principal é `template.yml` . Todos os aplicativos separados estão	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	aninhados no modelo pai único `template.yml` .	
Compile e crie o código do modelo do AWS SAM.	Usando a AWS SAM CLI, execute o comando a seguir. `sam build`	DevOps engenheiro

Implante o modelo AWS SAM

Tarefa	Descrição	Habilidades necessárias
Implante os aplicativos.	Para iniciar o código do modelo SAM que cria as CloudFormation pilhas de aplicativos aninhadas e implanta o código no ambiente da AWS, execute o comando a seguir. `sam deploy --guided --stack-name shopping-cart-nested-stack --capabilities CAPABILITY_IAM CAPABILITY_AUTO_EXPAND` O comando exibirá algumas perguntas. Responda a todas as perguntas com `y`.	DevOps engenheiro

Verificar a implantação

Tarefa	Descrição	Habilidades necessárias
Verificar as pilhas.	Para analisar as CloudFormation pilhas e os recursos da AWS que foram definidos nos modelos do AWS SAM, faça o seguinte: 1. Faça login no AWS Management Console e navegue até o CloudFormationconsole. 2. Verifique se as pilhas principal e secundária estão listadas. Neste exemplo, `sam-shopping-cart` é a pilha principal que chama as pilhas aninhadas de Auth, Product e Shopping. A pilha de produtos fornece o link URL do Product API Gateway como saída.	DevOps engenheiro

Recursos relacionados

Referências

- AWS Serverless Application Model (AWS SAM)
- AWS SAM ativado GitHub
- Microsserviço de carrinho de compras com tecnologia sem servidor (exemplo de aplicativo da AWS)

Tutoriais e vídeos

- Crie um aplicativo com tecnologia sem servidor
- Palestras técnicas on-line da AWS: criação e implantação de aplicativos com tecnologia sem servidor com o AWS SAM

Mais informações

Depois que todo o código estiver pronto, o exemplo tem a seguinte estrutura de diretórios:

- sam_stacks: essa pasta contém a camada `shared.py`. Uma camada é um arquivo que contém bibliotecas, um runtime personalizado ou outras dependências. Com camadas, você pode usar as bibliotecas na sua função sem a necessidade de incluí-las em um pacote de implantação.
- product-mock-service— Essa pasta contém todas as funções e arquivos do Lambda relacionados ao produto.
- shopping-cart-service— Essa pasta contém todas as funções e arquivos do Lambda relacionados a compras.

Implementar o isolamento de inquilinos SaaS para o Amazon S3 usando uma máquina de venda automática de tokens AWS Lambda

Criado por Tabby Ward (AWS), Sravan Periyathambi (AWS) e Thomas Davis (AWS)

Resumo

Os aplicativos SaaS multilocação devem implementar sistemas para garantir que o isolamento dos inquilinos seja mantido. Quando você armazena dados de inquilinos no mesmo recurso da Amazon Web Services (AWS), como vários inquilinos armazenando dados no mesmo bucket do Amazon Simple Storage Service (Amazon S3), você deve garantir que o acesso entre inquilinos não ocorra. As máquinas de venda automática de tokens (TVMs) são uma forma de fornecer isolamento de dados do inquilino. Essas máquinas fornecem um mecanismo para obter tokens e, ao mesmo tempo, abstrair a complexidade de como esses tokens são gerados. Os desenvolvedores podem usar uma TVM sem ter conhecimento detalhado de como ela produz tokens.

Este padrão implementa uma TVM usando o AWS Lambda. A TVM gera um token que consiste em credenciais temporárias de serviço de token de segurança (STS) que limitam o acesso aos dados de um único inquilino SaaS em um bucket S3.

TVMse o código fornecido com esse padrão são normalmente usados com declarações derivadas de JSON Web Tokens (JWTs) para associar solicitações de recursos da AWS a uma política do AWS Identity and Access Management (IAM) com escopo de locatário. Você pode usar o código deste padrão como base para implementar um aplicativo SaaS que gera credenciais STS temporárias e com escopo com base nas declarações fornecidas em um token JWT.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) versão 1.19.0 ou superior, instalada e configurada no macOS, Linux ou Windows. Como alternativa, você pode usar a AWS CLI versão 2.1 ou superior.

Limitações

- Este código é executado em Java e atualmente não oferece suporte a outras linguagens de programação.

- O aplicativo de exemplo não inclui suporte entre regiões ou recuperação de desastres (DR) da AWS.
- Este padrão demonstra como uma TVM do Lambda para um aplicativo SaaS pode fornecer acesso de inquilino com escopo definido. Não se destina a ser usado em ambientes de produção.

Arquitetura

Pilha de tecnologias de destino

- AWS Lambda
- Amazon S3
- IAM
- AWS Security Token Service (AWS STS)

Arquitetura de destino

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Security Token Service (AWS STS) ajuda você a solicitar credenciais temporárias com privilégios limitados para os usuários.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Código

O código-fonte deste padrão está disponível como anexo e inclui os seguintes arquivos:

- `s3UploadSample.jar` fornece o código-fonte para uma função do Lambda que carrega um documento JSON em um bucket do S3.
- `tvm-layer.zip` oferece uma biblioteca Java reutilizável que fornece um token (credenciais temporárias STS) para que a função do Lambda acesse o bucket do S3 e faça o upload do documento JSON.
- `token-vending-machine-sample-app.zip` fornece o código-fonte usado para criar esses artefatos e instruções de compilação.

Para usar esses arquivos, siga as instruções da próxima seção.

Épicos

Determinar os valores das variáveis

Tarefa	Descrição	Habilidades necessárias
Determinar os valores das variáveis.	A implementação deste padrão inclui vários nomes de variáveis que devem ser usados de forma consisten te. Determine os valores que devem ser usados para cada variável e forneça esse valor quando solicitado nas etapas subsequentes. <AWS Account ID> – O ID da conta de 12 dígitos associado à conta da AWS na qual você está implementando este padrão. Para obter informaçõ es sobre como localizar o número da sua conta da AWS, consulte O ID da sua	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	conta da AWS e seu alias na documentação do IAM. <AWS Region> – A região da AWS na qual você está implementando este padrão. Para obter mais informaçõ es sobre regiões da AWS, consulte Regiões e zonas de disponibilidade no site da AWS. < sample-tenant-name > – O nome de um inquilino a ser usado no aplicativo. Recomendamos que você use somente caracteres alfanuméricos neste valor para simplificar, mas você pode usar qualquer nome válido para uma chave de objeto do S3. < sample-tvm-role-name > – O nome da função do IAM associada à função Lambda que executa o TVM e o aplicativo de amostra. O nome do perfil é uma string que consiste em caractere s alfanuméricos maiúsculos e minúsculos sem espaços. Você também pode incluir os seguintes caracteres: sublinhado (_), sinal de mais (+), sinal de igual (=), vírgula	

Tarefa	Descrição	Habilidades necessárias
	(,), ponto (.), arroba (@) e hífen (-). O nome da função deve ser exclusivo na conta. **< sample-app-role-name >** – O nome da função do IAM que é assumida pela função Lambda quando ela gera credenciais STS temporárias e com escopo definido. O nome do perfil é uma string que consiste em caracteres alfanuméricos maiúsculos e minúsculos sem espaços. Você também pode incluir os seguintes caracteres: sublinhado (_), sinal de mais (+), sinal de igual (=), vírgula (,), ponto (.), arroba (@) e hífen (-). O nome da função deve ser exclusivo na conta. **< sample-app-function-name >** – O nome da função Lambda. É uma string com até 64 caracteres. **< sample-app-bucket-name >** – O nome de um bucket do S3 que deve ser acessado com permissões que têm como escopo um locatário específico. Os nomes do bucket do S3: • Devem conter entre 3 e 63 caracteres.	

Tarefa	Descrição	Habilidades necessárias
	• Devem consistir em apenas letras minúsculas, números, pontos (.) e hifens (-). • Deve iniciar e terminar com uma letra ou um número. • Não devem ser formatados como um endereço IP (por exemplo, 192.168.5.4). • Deve ser exclusivo em uma partição. Uma partição é um grupo de regiões. Atualmente, a AWS tem três partições: `aws` (regiões padrão), `aws-cn` (regiões da China) e `aws-us-gov` (regiões da AWS GovCloud [EUA]).	

Criar um bucket do S3.

Tarefa	Descrição	Habilidades necessárias
Criar um ambiente do bucket do S3 para o aplicativo de exemplo.	Usar o comando da AWS CLI a seguir para criar o bucket do S3. Forneça o valor **<** sample-app-bucket-name **>** no trecho de código: `aws s3api create-bucket --bucket <sample-app-bucket-name>` O aplicativo de exemplo Lambda carrega arquivos JSON nesse bucket.	Administrador de nuvem

Criar uma política e um perfil do TVM do IAM

Tarefa	Descrição	Habilidades necessárias

Criar um perfil TVM.	Use um dos comandos da AWS CLI a seguir para criar um perfil do IAM. Forneça o valor < sample-tvm-role-name > no comando.
	
	Para shells no macOS ou Linux:
	
	`aws iam create-role \ --role-name <sample-tvm-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ]}'`
	
	Para a linha de comando do Windows:
	
	`aws iam create-role ^ --role-name <sample-tvm-role-name> ^`
		Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	`--assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Principal\": {\"Service\": \"lambda.amazonaws.com\"}, \"Action\": \"sts:AssumeRole\"}]}"` O aplicativo de exemplo do Lambda assume essa função quando o aplicativo é invocado. A capacidade de assumir o perfil do aplicativo com uma política de escopo fornece ao código permissões mais amplas para acessar o bucket do S3.	

Tarefa	Descrição	Habilidades necessárias

Criar uma política de função de TVM em linha.	Use um dos comandos da AWS CLI a seguir para criar uma política do IAM. Forneça os <AWS Account ID>valores < sample-tvm-role-name sample-app-role-name >, e < > no comando.
	
	Para shells no macOS ou Linux:
	
	`aws iam put-role-policy \`
	`--role-name <sample-tvm-role-name> \`
	`--policy-name assume-app-role \`
	`--policy-document '{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Effect": "Allow",`
	`"Action": "sts:AssumeRole",`
	`"Resource": "arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>"`
	`}`
	`]}'`
	
	Para a linha de comando do Windows:
	
	`aws iam put-role-policy ^`
		Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	`--role-name <sample-tvm-role-name> ^ --policy-name assume-app-role ^ --policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\", \"Resource\": \"arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>\"}]}"` Esta política é anexada à função da TVM. Dá ao código a capacidade de assumir o perfil do aplicativo que possui permissões mais amplas para acessar o bucket do S3.	

Tarefa	Descrição	Habilidades necessárias

Anexar a política gerenciada do Lambda.	Use um dos comandos da AWS CLI a seguir para anexar uma política do IAM `AWSLambdaBasicExecutionRole`. Forneça o valor **<** sample-tvm-role-name **>** no comando:
	`aws iam attach-role-policy \ --role-name <sample-tvm-role-name> \ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Para a linha de comando do Windows:
	`aws iam attach-role-policy ^ --role-name <sample-tvm-role-name> ^ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Essa política gerenciada é anexada à função TVM para permitir que o Lambda envie registros para a Amazon. CloudWatch
		Administrador de nuvem

Criar uma política e um perfil do aplicativo IAM

Tarefa	Descrição	Habilidades necessárias
Criar o perfil do aplicativo.	Use um dos comandos da AWS CLI a seguir para criar um perfil do IAM. Forneça os <AWS Account ID>valores < sample-app-role-name sample-tvm-role-name >, e < > no comando. Para shells no macOS ou Linux: `aws iam create-role \ --role-name <sample-app-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>" }, "Action": "sts:AssumeRole" } ]}'` Para a linha de comando do Windows:	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	`aws iam create-role ^ --role-name <sample-app-role-name> ^ --assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\",\"Principal\": {\"AWS\": \"arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>\"},\"Action\": \"sts:AssumeRole\" }]}"` O aplicativo de exemplo Lambda assume essa função com uma política de escopo para obter acesso baseado em inquilinos a um bucket do S3.	

Tarefa	Descrição	Habilidades necessárias
Criar uma política de função de aplicativo embutida.	Use um dos comandos da AWS CLI a seguir para criar uma política do IAM. Forneça os valores **<** sample-app-role-name sample-app-bucket-name **>** e **< >** no comando. Para shells no macOS ou Linux: `aws iam put-role-policy \ --role-name <sample-app-role-name> \ --policy-name s3-bucket-access \ --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"], "Resource": "arn:aws:s3:::<sample-app-bucket-name>/*" }, { "Effect": "Allow",`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	<pre>"Action":
	["s3:ListBucket"],
	"Resource
	": "arn:aws:s3:::<sam
	ple-app-bucket-name>"
	}
	]}'</pre>
	Para a linha de comando do Windows:
	<pre>aws iam put-role-policy
	^
	--role-name <sample-a
	pp-role-name> ^
	--policy-name s3-bucket
	-access ^
	--policy-documen
	t "{\"Version\":
	\"2012-10-17\",
	\"Statement\":
	[{\"Effect\": \"Allow
	\", \"Action\":
	[\"s3:PutObject\",
	\"s3:GetObject\",
	\"s3:DeleteObject\
	"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-na
	me>/*\"}, {\"Effect\":
	\"Allow\", \"Action\
	": [\"s3:ListBucket
	\"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-name>
	\"}]}"</pre>
	Esta política é anexada ao perfil do aplicativo. Ela fornece amplo acesso aos objetos	

Tarefa	Descrição	Habilidades necessárias
	no bucket do S3. Quando o aplicativo de exemplo assume o perfil, essas permissões são atribuídas a um inquilino específico com a política gerada dinamicamente pela TVM.	

Crie o aplicativo de exemplo Lambda com a TVM

Tarefa	Descrição	Habilidades necessárias
Baixe os arquivos de origem compilados.	Baixe os arquivos `s3UploadSample.jar` e `tvm-layer.zip`, que estão incluídos como anexos. O código-fonte usado para criar esses artefatos e instruções de compilação são fornecidos em `token-vending-machine-sample-app.zip`.	Administrador de nuvem
Criar a camada do Lambda.	Use o seguinte comando da AWS CLI para criar uma camada do Lambda, o que torna a TVM acessível ao Lambda. **Note** Se você não estiver executando esse comando a partir do local em que fez o download `tvm-`	Administrador da nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	`layer.zip` , forneça o caminho correto `tvm-layer.zip` no `--zip-file` parâmetro.
	
	`aws lambda publish-layer-version \ --layer-name sample-token-vending-machine \ --compatible-runtimes java11 \ --zip-file fileb://tvm-layer.zip`
	
	Para a linha de comando do Windows:
	
	`aws lambda publish-layer-version ^ --layer-name sample-token-vending-machine ^ --compatible-runtimes java11 ^ --zip-file fileb://tvm-layer.zip`
	
	Esse comando cria uma camada Lambda que contém a biblioteca TVM reutilizável.	

Tarefa	Descrição	Habilidades necessárias
Criar a função do Lambda.	Use o comando da AWS CLI a seguir para criar a função do Lambda. Forneça os <AWS Account ID><AWS Region>valores < sample-app-functio n-name sample-tvm-role-na me >,,, < sample-app-bucket-name >, < sample-app-role-na me > e < > no comando. **Note** Se você não estiver executando esse comando a partir do local em que fez o download `s3UploadS ample.jar` , forneça o caminho correto `s3UploadS ample.jar` no `--zip-file` parâmetro. `aws lambda create-fu nction \ --function-name <sample-app-function-name> \ --timeout 30 \ --memory-size 256 \ --runtime java11 \ --role arn:aws:i am::<AWS Account`	Administrador da nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	ID>:role/<sample-tvm-role-name> \ --handler com.amazon.aws.s3UploadSample.App \ --zip-file fileb://s3UploadSample.jar \ --layers arn:aws:lambda:<AWS Region>:<AWS Account ID>:layer:sample-token-vending-machine:1 \ --environment "Variables={S3_BUCKET=<sample-app-bucket-name>, ROLE=arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>}" Para a linha de comando do Windows: aws lambda create-function ^ --function-name <sample-app-function-name> ^ --timeout 30 ^ --memory-size 256 ^ --runtime java11 ^ --role arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name> ^ --handler com.amazon.aws.s3UploadSample.App ^ --zip-file fileb://s3UploadSample.jar ^	

Tarefa	Descrição	Habilidades necessárias

	`--layers arn:aws:lambda:<AWS Region>:<AWS Account ID>:layer:sample-token-vending-machine:1 ^`
	`--environment "Variables={S3_BUCKET=<sample-app-bucket-name>,ROLE=arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>}"`
	
	Esse comando cria uma função do Lambda com o código do aplicativo de exemplo e a camada TVM anexada. Ele também define duas variáveis de ambiente: `S3_BUCKET` e `ROLE`. O aplicativo de exemplo usa essas variáveis para determinar a função a ser assumida e o bucket do S3 para o qual carregar documentos JSON.	

Testar o aplicativo de exemplo e a TVM

Tarefa	Descrição	Habilidades necessárias
Invocar o aplicativo de exemplo do Lambda.	Use um dos comandos da AWS CLI a seguir para iniciar o aplicativo de exemplo do Lambda com o payload esperado. Forneça os valores	Administrador da nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	< sample-app-function-name sample-tenant-name > e < > no comando.
	
	Para shells no macOS ou Linux:
	
	`aws lambda invoke \ --function <sample-app-function-name> \ --invocation-type RequestResponse \ --payload '{"tenant": "<sample-tenant-name>"}' \ --cli-binary-format raw-in-base64-out response.json`
	
	Para a linha de comando do Windows:
	
	`aws lambda invoke ^ --function <sample-app-function-name> ^ --invocation-type RequestResponse ^ --payload "{\"tenant\": \"<sample-tenant-name>\"}" ^ --cli-binary-format raw-in-base64-out response.json`
	
	Esse comando chama a função do Lambda e retorna o resultado em um documento `response.json` . Em muitos	

Tarefa	Descrição	Habilidades necessárias
	sistemas baseados em Unix, você pode alterar `response.json` para `/dev/stdout` para enviar os resultados diretamente para o shell sem criar outro arquivo. **Note** Alterar o valor < sample-tenant-name > em invocações subsequentes dessa função Lambda altera a localização do documento JSON e as permissões que o token fornece.	
Visualizar o bucket do S3 para ver os objetos criados.	Navegue até o bucket do S3 (< sample-app-bucket-name >) que você criou anteriormente. Esse bucket contém um prefixo de objeto do S3 com o valor < > sample-tenant-name. Sob esse prefixo, você encontrará um documento JSON chamado com um UUID. Invocar o aplicativo de exemplo várias vezes adiciona mais documentos JSON.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Visualizar os logs do Cloudwatch para o aplicativo de exemplo.	Visualize os registros do Cloudwatch associados à função Lambda chamada < >. sample-app-function-name Para obter instruções, consulte Como acessar CloudWatch os logs da Amazon para o AWS Lambda na documentação do AWS Lambda. Você pode visualizar a política com escopo de inquilino gerada pela TVM nesses logs. Essa política com escopo de locatário concede permissões para o aplicativo de amostra para o Amazon S3,,, e PutObjectGetObject DeleteObjectListBucket APIs, mas somente para o prefixo de objeto associado a < >. sample-tenant-name Nas invocações subsequentes do aplicativo de amostra, se você alterar < sample-tenant-name >, o TVM atualizará a política de escopo para corresponder ao inquilino fornecido na carga de invocação. Essa política gerada dinamicamente mostra como o acesso com escopo de inquilino pode ser mantido com uma TVM em aplicativos SaaS.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	A funcionalidade da TVM é fornecida em uma camada Lambda para que possa ser anexada a outras funções do Lambda usadas por um aplicativo sem precisar replicar o código. Para obter uma ilustração da política gerada dinamicam ente, consulte a seção Informações adicionais.	

Recursos relacionados

- Isolar inquilinos com políticas do IAM geradas dinamicamente (publicação do blog)
- Aplicar políticas de isolamento geradas dinamicamente no ambiente SaaS (publicação do blog)
- AWS SaaS Boost (um ambiente de referência de código aberto que ajuda você a mover sua oferta de SaaS para a AWS)

Mais informações

O seguinte log do Amazon Cloudwatch mostra a política gerada dinamicamente produzida pelo código da TVM nesse padrão. Nesta captura de tela, o < sample-app-bucket-name > é `DOC-EXAMPLE-BUCKET` e o < sample-tenant-name > é `test-tenant-1`. As credenciais STS retornadas por essa política de escopo não conseguem realizar nenhuma ação em objetos no bucket do S3, exceto os objetos associados ao prefixo da chave do objeto `test-tenant-1`.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Implementar o padrão de saga com tecnologia sem servidor usando o AWS Step Functions

Criado por Tabby Ward (AWS), Joe Kern (AWS) e Rohan Mehta (AWS)

Resumo

Em uma arquitetura de microsserviços, o objetivo principal é criar componentes desacoplados e independentes para promover agilidade, flexibilidade e menor tempo de comercialização de seus aplicativos. Como resultado do desacoplamento, cada componente de microsserviço tem sua própria camada de persistência de dados. Em uma arquitetura distribuída, as transações comerciais podem abranger vários microsserviços. Como esses microsserviços não podem usar uma única transação de atomicidade, consistência, isolamento e durabilidade (ACID), você pode acabar com transações parciais. Nesse caso, alguma lógica de controle é necessária para desfazer as transações que já foram processadas. O padrão de saga distribuída é normalmente usado para essa finalidade.

O padrão saga é um padrão de gerenciamento de falhas que ajuda a estabelecer a consistência em aplicativos distribuídos e coordena as transações entre vários microsserviços para manter a consistência de dados. Quando você usa o padrão de saga, cada serviço que realiza uma transação publica um evento que aciona serviços subsequentes para realizar a próxima transação na cadeia. Isso continua até que a última transação na cadeia seja concluída. Se uma transação comercial falhar, a saga orquestra uma série de transações compensatórias que desfazem as alterações feitas pelas transações anteriores.

Esse padrão demonstra como automatizar a configuração e a implantação de um aplicativo de amostra (que lida com reservas de viagens) com tecnologias sem servidor, como AWS Step Functions, AWS Lambda e Amazon DynamoDB. O aplicativo de amostra também usa o Amazon API Gateway e o Amazon Simple Notification Service (Amazon SNS) para implementar um coordenador de execução da saga. O padrão pode ser implantado com uma estrutura de infraestrutura como código (IaC), como o AWS Cloud Development Kit (AWS CDK), o AWS Serverless Application Model (AWS SAM) ou o Terraform.

Para obter mais informações sobre o padrão da saga e outros padrões de persistência de dados, consulte o guia Habilitar a persistência de dados em microsserviços no site de Recomendações da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões para criar uma CloudFormation pilha da AWS. Para obter mais informações, consulte Controle de acesso na CloudFormation documentação.
- Estrutura de IaC de sua escolha (AWS CDK, AWS SAM ou Terraform) configurada com sua conta da AWS para que você possa usar a CLI da estrutura para implantar o aplicativo.
- NodeJS, usado para criar o aplicativo e executá-lo localmente.
- Um editor de código de sua escolha (como Visual Studio Code, Sublime ou Atom).

Versões do produto

- NodeJS versão 14
- AWS CDK versão 2.37.1
- AWS SAM versão 1.71.0
- Terraform versão 1.3.7

Limitações

O fornecimento de eventos é uma forma natural de implementar o padrão de orquestração da saga em uma arquitetura de microsserviços em que todos os componentes estão com acoplamento fraco e não têm conhecimento direto uns dos outros. Se sua transação envolver um pequeno número de etapas (três a cinco), o padrão da saga pode ser uma ótima opção. No entanto, a complexidade aumenta com o número de microsserviços e o número de etapas.

Testar e depurar podem se tornar difíceis quando você usa esse design, porque você precisa ter todos os serviços em execução para simular o padrão da transação.

Arquitetura

Arquitetura de destino

A arquitetura proposta usa o AWS Step Functions para criar um padrão de saga para reservar voos, reservar aluguéis de carros e processar pagamentos de férias.

O diagrama de fluxo de trabalho a seguir ilustra o fluxo típico do sistema de reserva de viagens. O fluxo de trabalho consiste em reservar viagens aéreas (“ReserveFlight”), reservar um carro (“ReserveCarRental”), processar pagamentos (“ProcessPayment”), confirmar reservas de voos (“ConfirmFlight”) e confirmar aluguéis de carros (“”), seguido por uma notificação de sucesso quando

essas etapas forem concluídas. ConfirmCarRental No entanto, se o sistema encontrar algum erro na execução de qualquer uma dessas transações, ele começará a falhar para trás. Por exemplo, um erro no processamento do pagamento (“ProcessPayment”) aciona um reembolso (“RefundPayment”), que então aciona o cancelamento do carro e do voo alugados (“CancelRentalReservation” e “CancelFlightReservation”), finalizando toda a transação com uma mensagem de falha.

Esse padrão implanta funções do Lambda separadas para cada tarefa destacada no diagrama, bem como três tabelas do DynamoDB para voos, aluguel de carros e pagamentos. Cada função do Lambda cria, atualiza ou exclui as linhas nas respectivas tabelas do DynamoDB, dependendo se uma transação é confirmada ou revertida. O padrão usa o Amazon SNS para enviar mensagens de texto (SMS) aos assinantes, notificando-os sobre transações fracassadas ou bem-sucedidas.

Automação e escala

Você pode criar a configuração para essa arquitetura usando uma das estruturas do IaC. Para se conectar no IaC de sua preferência, use um dos links a seguir.

- Implemente com o AWS CDK
- Implemente com o AWS SAM
- Implemente com o Terraform

Ferramentas

Serviços da AWS

- O AWS Step Functions é um serviço de orquestração de tecnologia sem servidor que permite combinar funções do AWS Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios. A partir do console gráfico do Step Functions, você vê o fluxo de trabalho do seu aplicativo como uma série de etapas orientadas por eventos.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade integrada. Use o DynamoDB para criar uma tabela do banco de dados que possa armazenar e recuperar qualquer quantidade de dados e atender qualquer nível de tráfego solicitado.
- O AWS Lambda é um serviço de computação que permite que você execute o código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.

- O Amazon API Gateway é um serviço da AWS para criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- O Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens de publicadores para assinantes.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software para definir seus recursos de aplicativos em nuvem usando linguagens de programação conhecidas TypeScript, como Python JavaScript, Java e C#/.Net.
- O AWS Serverless Application Model (AWS SAM) é uma estrutura de código aberto para a criação de aplicativos com tecnologia sem servidor. Ele fornece sintaxe abreviada para expressar funções APIs, bancos de dados e mapeamentos de fontes de eventos.

Código

O código de um aplicativo de amostra que demonstra o padrão da saga, incluindo o modelo IaC (AWS CDK, AWS SAM ou Terraform), as funções do Lambda e as tabelas do DynamoDB, pode ser encontrado nos links a seguir. Siga as instruções no primeiro épico para instalá-los.

- Implemente com o AWS CDK
- Implemente com o AWS SAM
- Implemente com o Terraform

Épicos

Instale pacotes, compile e crie

Tarefa	Descrição	Habilidades necessárias
Instale os pacotes NPM.	Crie um novo diretório, navegue até esse diretório em um terminal e clone o GitHub repositório de sua escolha na seção Código anterior nesse padrão. Na pasta raiz que contém o arquivo `package.json` ,	Desenvolvedor e arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	execute o comando a seguir para baixar e instalar todos os pacotes do Node Package Manager (NPM): `npm install`	
Compile scripts.	Na pasta raiz, execute o comando a seguir para instruir o TypeScript transpilador a criar todos os arquivos necessários: JavaScript `npm run build`	Desenvolvedor e arquiteto de nuvem
Observe as alterações e recompile.	Na pasta raiz, execute o comando a seguir em uma janela de terminal separada para observar as alteraçõe s no código e compilar o código quando detectar uma alteração: `npm run watch`	Desenvolvedor e arquiteto de nuvem
Execute testes de unidade (somente AWS CDK).	Se você estiver usando o AWS CDK, na pasta raiz, execute o seguinte comando para realizar os testes de unidade do Jest: `npm run test`	Desenvolvedor e arquiteto de nuvem

Implante recursos na conta da AWS de destino

Tarefa	Descrição	Habilidades necessárias

Implante a pilha de demonstração na AWS.	**Important**
	O aplicativo é independente da região da AWS. Se você usar um perfil, deverá declarar a região explicitamente no perfil da AWS Command Line Interface (AWS CLI) ou por meio de variáveis de ambiente da AWS CLI.
	
	Na pasta raiz, execute o comando a seguir para criar um conjunto de implantação e implantá-lo na conta e região padrão da AWS.
	
	AWS CDK:
	
	`cdk bootstrap`
	`cdk deploy`
	
	AWS SAM:
	
	`sam build`
	`sam deploy --guided`
	
	Terraform:
		Desenvolvedor e arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

	`terraform init`
	`terraform apply`
	
	Esta etapa pode demorar vários minutos para que seja concluída. Esse comando usa as credenciais padrão que foram configuradas para a AWS CLI.
	
	Observe o URL do API Gateway que é exibida no console após a conclusão da implantação. Você precisará dessas informações para testar o fluxo de execução da saga.	

Tarefa	Descrição	Habilidades necessárias

Compare a pilha implantada com o estado atual.	Na pasta raiz, execute o comando a seguir para comparar a pilha implantada com o estado atual depois de fazer alterações no código-fonte:
	AWS CDK:
	`cdk diff`
	AWS SAM:
	`sam deploy`
	Terraform:
	`terraform plan`
		Desenvolvedor e arquiteto de nuvem

Teste o fluxo de execução

Tarefa	Descrição	Habilidades necessárias
Teste o fluxo de execução da saga.	Navegue até o URL do API Gateway que você anotou na etapa anterior, ao implantar a pilha. Esse URL aciona a inicialização da máquina de estado. Para obter mais informações sobre como manipular o fluxo da máquina de estado passando parâmetros de URL diferentes,	Desenvolvedor e arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	consulte a seção Informações adicionais. Para ver os resultados, faça login no Console de Gerenciamento da AWS e navegue até o console do Step Functions. Aqui, você pode ver cada passo da máquina de estado da saga. Você também pode visualizar a tabela do DynamoDB para ver os registros inseridos, atualizados ou excluídos. Se você atualizar a tela com frequência, poderá observar a mudança do status da transação de `pending` para `confirmed` . Você pode assinar o tópico do SNS atualizando o código no arquivo `stateMachine.ts` com seu número de telefone celular para receber mensagens SMS em caso de reservas bem-sucedidas ou malsucedidas. Para obter mais informações, consulte Amazon SNS na seção Informações adicionais.	

Limpeza

Tarefa	Descrição	Habilidades necessárias

Limpar os recursos.	Para limpar os recursos implantados para esse aplicativo, você pode usar um dos seguintes comandos.
	
	AWS CDK:
	
	`cdk destroy`
	
	AWS SAM:
	
	`sam delete`
	
	Terraform:
	
	`terraform destroy`
		Desenvolvedor de aplicativos, arquiteto de nuvem

Recursos relacionados

Artigos técnicos

- Implementação de microsserviços na AWS
- Perspectiva de aplicativos com tecnologia sem servidor
- Habilitar a persistência de dados em microsserviços

Documentação do serviço da AWS

- Conceitos básicos do AWS CDK
- Conceitos básicos do AWS SAM
- AWS Step Functions
- Amazon DynamoDB

- AWS Lambda
- Amazon API Gateway
- Amazon SNS

Tutoriais

- Workshops práticos sobre computação com tecnologia sem servidor

Mais informações

Código

Para fins de teste, esse padrão implanta o API Gateway e uma função do Lambda de teste que aciona a máquina de estado Step Functions. Com o Step Functions, você pode controlar a funcionalidade do sistema de reserva de viagens passando um `run_type` parâmetro para simular falhas em “ReserveFlight,” “ReserveCarRental,” “ProcessPayment,” “ConfirmFlight” e “”ConfirmCarRental.

A função do Lambda `saga` (`sagaLambda.ts`) recebe a entrada dos parâmetros de consulta no URL do API Gateway, cria o seguinte objeto JSON e o passa para o Step Functions para execução:

```
let input = {
"trip_id": tripID, //  value taken from query parameter, default is AWS request ID
"depart_city": "Detroit",
"depart_time": "2021-07-07T06:00:00.000Z",
"arrive_city": "Frankfurt",
"arrive_time": "2021-07-09T08:00:00.000Z",
"rental": "BMW",
"rental_from": "2021-07-09T00:00:00.000Z",
"rental_to": "2021-07-17T00:00:00.000Z",
"run_type": runType // value taken from query parameter, default is "success"
};
```

Você pode experimentar diferentes fluxos da máquina de estado Step Functions passando os seguintes parâmetros de URL:

- Execução bem-sucedida – https://{api gateway url}
- Falha no voo de reserva – https://{api gateway url}? Tipo de execução = failFlightsReservation

- Confirme a falha do voo – https://{api gateway url}? Tipo de execução = failFlightsConfirmation
- Falha na reserva do aluguel de carros – https://{api gateway url}? RunType= Reserva failCarRental
- Confirme a falha no aluguel do carro – https://{api gateway url}? RunType= Confirmação failCarRental
- Falha no processo de pagamento – https://{api gateway url}?runType=failPayment
- Passe um ID de viagem – https://{api gateway url}?tripID={por padrão, o ID da viagem será o ID da solicitação da AWS}

Modelos IaC

Os repositórios vinculados incluem modelos de IaC que você pode usar para criar toda a amostra do aplicativo de reserva de viagens.

- Implemente com o AWS CDK
- Implemente com o AWS SAM
- Implemente com o Terraform

Tabelas do DynamoDB

Aqui estão os modelos de dados para as tabelas de voos, aluguéis de carros e pagamentos.

```
Flight Data Model:
 var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: flightReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: flightReservationID},
        'depart_city' : {S: event.depart_city},
        'depart_time': {S: event.depart_time},
        'arrive_city': {S: event.arrive_city},
        'arrive_time': {S: event.arrive_time},
        'transaction_status': {S: 'pending'}
      }
    };

Car Rental Data Model:
var params = {
```

```
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: carRentalReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: carRentalReservationID},
        'rental': {S: event.rental},
        'rental_from': {S: event.rental_from},
        'rental_to': {S: event.rental_to},
        'transaction_status': {S: 'pending'}
      }
    };

Payment Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: paymentID},
        'trip_id' : {S: event.trip_id},
        'id': {S: paymentID},
        'amount': {S: "750.00"}, // hard coded for simplicity as implementing any
 monetary transaction functionality is beyond the scope of this pattern
        'currency': {S: "USD"},
        'transaction_status': {S: "confirmed"}
      }
    };
```

Funções do Lambda

As seguintes funções serão criadas para suportar o fluxo e a execução da máquina de estado no Step Functions:

- Reservar voos: insere um registro na tabela de voos do DynamoDB com um `transaction_status` de `pending`, para reservar um voo.
- Confirmar voo: atualiza o registro na tabela de voos do DynamoDB, para definir `transaction_status` como `confirmed`, para confirmar o voo.
- Cancelar reserva de voos: exclui o registro da tabela de voos do DynamoDB para cancelar o voo pendente.
- Reserve locações de veículos: insere um registro na tabela do CarRentals DynamoDB com `transaction_status` um de, para reservar um aluguel `pending` de carro.

- Confirmar aluguel de carros: atualiza o registro na tabela do CarRentals DynamoDB, para `transaction_status` definir como, `confirmed` para confirmar o aluguel do carro.
- Cancelar reserva de aluguel de carro: exclui o registro da tabela do CarRentals DynamoDB para cancelar o aluguel de carro pendente.
- Processar pagamento: insere um registro na tabela de pagamentos do DynamoDB para o pagamento.
- Cancelar pagamento: exclui o registro do pagamento da tabela de pagamentos do DynamoDB.

Amazon SNS

O aplicativo de amostra cria o tópico e a assinatura a seguir para enviar mensagens SMS e notificar o cliente sobre reservas bem-sucedidas ou malsucedidas. Se você quiser receber mensagens de texto enquanto testa o aplicativo de amostra, atualize a assinatura de SMS com seu número de telefone válido no arquivo de definição da máquina de estado.

Trecho do AWS CDK (adicione o número de telefone na segunda linha do código a seguir):

```
const topic = new  sns.Topic(this, 'Topic');
topic.addSubscription(new subscriptions.SmsSubscription('+11111111111'));
const snsNotificationFailure = new tasks.SnsPublish(this ,'SendingSMSFailure', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation Failed'),
});

const snsNotificationSuccess = new tasks.SnsPublish(this ,'SendingSMSSuccess', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation is Successful'),
});
```

Trecho do AWS SAM (substitua as strings +1111111111 pelo seu número de telefone válido):

```
  StateMachineTopic11111111111:
    Type: 'AWS::SNS::Subscription'
    Properties:
      Protocol: sms
      TopicArn:
        Ref: StateMachineTopic
      Endpoint: '+11111111111'
```

```
    Metadata:
      'aws:sam:path': SamServerlessSagaStack/StateMachine/Topic/+11111111111/Resource
```

Trecho do Terraform (substitua a string +111111111 pelo seu número de telefone válido):

```
resource "aws_sns_topic_subscription" "sms-target" {
  topic_arn = aws_sns_topic.topic.arn
  protocol  = "sms"
  endpoint  = "+11111111111"
}
```

Reservas bem-sucedidas

O fluxo a seguir ilustra uma reserva bem-sucedida com “ReserveFlight,” “ReserveCarRental,” e “ProcessPayment” seguidos por “ConfirmFlight” e “”ConfirmCarRental. O cliente é notificado sobre a reserva bem-sucedida por meio de mensagens SMS enviadas ao assinante do tópico do SNS.

Reservas malsucedidas

Esse fluxo é um exemplo de falha no padrão da saga. Se, após a reserva de voos e aluguel de carros, “ProcessPayment” falhar, as etapas serão canceladas na ordem inversa. As reservas são liberadas e o cliente é notificado da falha por meio de mensagens SMS que são enviadas ao assinante do tópico do SNS.

Gerencie aplicativos de contêineres on-premises configurando o Amazon ECS Anywhere com o AWS CDK

Criado pelo Dr. Rahul Sharad Gaikwad (AWS)

Resumo

O Amazon ECS Anywhere é uma extensão do Amazon Elastic Container Service (Amazon ECS). Você pode usar o ECS Anywhere para implantar tarefas nativas do Amazon ECS em um ambiente on-premises ou gerenciado pelo cliente. Esse atributo ajuda a reduzir custos e mitigar operações e orquestrações complexas de contêineres locais. Você pode usar o ECS Anywhere para implantar e executar aplicativos de contêiner em ambientes on-premises e na nuvem. Isso elimina a necessidade de sua equipe aprender vários domínios e conjuntos de habilidades ou gerenciar softwares complexos por conta própria.

Esse padrão demonstra as etapas para configurar o ECS Anywhere usando pilhas do AWS Cloud Development Kit (AWS CDK);

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI), instalada e configurada. (Consulte Instalar, atualizar e desinstalar a AWS CLI na documentação da AWS CLI.)
- AWS CDK Toolkit, instalado e configurado. (Consulte o AWS CDK Toolkit na documentação do AWS CDK e siga as instruções para instalar a versão 2 globalmente.)
- Gerenciador de pacotes Node (npm), instalado e configurado para o AWS CDK em. TypeScript (Consulte Como baixar e instalar o Node.js e o npm na documentação do npm.)

Limitações

- Para limitações e considerações, consulte Instâncias externas (Amazon ECS Anywhere) na documentação do Amazon ECS.

Versões do produto

- Kit de ferramentas do AWS CDK versão 2

- npm versão 7.20.3 ou superior
- Node.js versão 16.6.1 ou superior

Arquitetura

Pilha de tecnologias de destino

- AWS CloudFormation
- AWS CDK
- Amazon ECS Anywhere
- AWS Identity and Access Management (IAM)

Arquitetura de destino

O diagrama a seguir ilustra uma arquitetura de sistema de alto nível da configuração do ECS Anywhere usando o AWS CDK com TypeScript, conforme implementado por esse padrão.

1. Quando você implanta a pilha de CDK da AWS, ela cria uma CloudFormation pilha na AWS.
2. A CloudFormation pilha provisiona um cluster do Amazon ECS e recursos relacionados da AWS.
3. Para registrar uma instância externa com um cluster do Amazon ECS, você deve instalar o AWS Systems Manager Agent (SSM Agent) na sua máquina virtual (VM) e registrar a VM como uma instância gerenciada do AWS Systems Manager.
4. Você deve instalar o agente de contêiner do Amazon ECS e o Docker na sua VM para registrá-la como instância externa com o cluster do Amazon ECS.
5. Quando a instância externa é registrada e configurada com o cluster Amazon ECS, ela pode executar vários contêineres na sua VM, que é registrada como uma instância externa.

Automação e escala

O GitHub repositório fornecido com esse padrão usa o AWS CDK como uma ferramenta de infraestrutura como código (IaC) para criar a configuração dessa arquitetura. O AWS CDK ajuda você a orquestrar recursos e configurar o ECS Anywhere.

Ferramentas

- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

Código

O código-fonte desse padrão está disponível no GitHub repositório Amazon ECS Anywhere CDK Samples. Para clonar e usar o repositório, siga as instruções na próxima seção.

Épicos

Verifique a configuração do AWS CDK

Tarefa	Descrição	Habilidades necessárias
Verifique a versão do AWS CDK.	Verifique a versão do AWS CDK Toolkit executando o seguinte comando: `cdk --version` Esse padrão requer a versão 2 do AWS CDK. Se você tiver uma versão anterior do AWS CDK, siga as instruções na documentação do AWS CDK para atualizá-la.	DevOps engenheiro
Configure as credenciais da AWS.	Para configurar as credencia is, execute o comando `aws configure` e siga as instruções: `$aws configure`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`AWS Access Key ID [None]: <your-access-key-ID>`
	`AWS Secret Access Key [None]: <your-secret-access-key>`
	`Default region name [None]: <your-Region-name>`
	`Default output format [None]:`	

Faça o bootstrap do ambiente do AWS CDK

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de códigos do AWS CDK.	Clone o repositório de GitHub código desse padrão usando o comando: `git clone https://github.com/aws-samples/amazon-ecs-anywhere-cdk-samples.git`	DevOps engenheiro
Faça o bootstrap do ambiente.	Para implantar o CloudFormation modelo da AWS na conta e na região da AWS que você deseja usar, execute o seguinte comando: `cdk bootstrap <account-number>/<Region>`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es, consulte Inicialização na documentação do AWS CDK.	

Crie e implante o projeto

Tarefa	Descrição	Habilidades necessárias

Instale as dependências do pacote e compile TypeScript os arquivos.	Instale as dependências do pacote e compile os TypeScrip t arquivos executando os seguintes comandos:
	`$cd amazon-ecs-anywher e-cdk-samples`
	`$npm install`
	`$npm fund`
	Esses comandos instalam todos os pacotes do repositór io de exemplo.
	Important
	Se você receber algum erro sobre pacotes ausentes, use um dos seguintes comandos:
	`$npm ci`
	—ou—
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`$npm install -g @aws-cdk/<package_name>` Para obter mais informações, consulte npm ci e npm install na documentação do npm.	
Crie o projeto.	Para construir o código do projeto, execute o comando: `npm run build` Para obter mais informações sobre como criar e implantar o projeto, consulte Seu primeiro aplicativo da AWS CDK na documentação do AWS CDK.	DevOps engenheiro
Implante o projeto.	Para implantar o código do projeto, execute o comando: `cdk deploy`	DevOps engenheiro
Verifique a criação e a saída da pilha.	Abra o CloudFormation console da AWS em https://console.aws.amazon.com/cloudformation e escolha a pilha. `EcsAnywhereStack` A guia Saídas mostra os comandos a serem executados em sua VM externa.	DevOps engenheiro

Configurar uma máquina on-premises

Tarefa	Descrição	Habilidades necessárias
Configure sua VM usando o Vagrant.	Para fins de demonstração, você pode usar o HashiCorp Vagrant para criar uma VM. O Vagrant é um utilitário de código aberto para criar e manter ambientes portáteis de desenvolvimento de software virtual. Crie uma VM Vagrant executando o comando `vagrant up` a partir do diretório raiz em que o Vagrantfile está colocado. Para obter mais informações, consulte a documentação do Vagrant.	DevOps engenheiro
Registre sua VM como uma instância externa.	1. Faça login na VM Vagrant usando o comando `vagrant ssh`. Para obter mais informações, consulte a documentação do Vagrant. 2. Crie um código de ativação e um ID que você possa usar para registrar sua VM no AWS Systems Manager e ativar sua instância externa. A saída desse comando inclui os valores `ActivationId` e `ActivationCode` : `aws ssm create-activation --iam-role EcsAnywhereInstanc`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`eRole | tee ssm-activ ation.json`
	
	3. Exporte a ID de ativação e os valores do código:
	
	`export ACTIVATIO N_ID=<activation-ID> export ACTIVATIO N_CODE=<activation- code>`
	
	4. No servidor on-premises ou na máquina virtual (VM), baixe o script de instalação:
	
	`curl -o "ecs-anywhere- install.sh" "https:// amazon-ecs-agent.s 3.amazonaws.com/ec s-anywhere-install -latest.sh" && sudo chmod +x ecs-anywhere- install.sh`
	
	5. No servidor on-premises ou na máquina virtual (VM), execute o script de instalação:
	
	`sudo ./ecs-anywhere-ins tall.sh \ --cluster test-ecs- anywhere \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <Region>`	

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es sobre como configurar e registrar sua VM, consulte Registro de uma instância externa em um cluster na documentação do Amazon ECS.	

Verifique o status do ECS Anywhere e da VM externa.	Para verificar se sua caixa virtual está conectada ao ambiente de gerenciam ento do Amazon ECS e em execução, use os seguintes comandos:
	`aws ssm describe-instance-information`
	`aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps engenheiro

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpe e exclua recursos.	Depois de percorrer esse padrão, você deve remover os recursos criados para evitar cobranças adicionais. Para limpar, execute o comando: `cdk destroy`	DevOps engenheiro

Recursos relacionados

- Documentação do Amazon ECS Anywhere
- Demonstração do Amazon ECS Anywhere
- Exemplos de workshops do Amazon ECS Anywhere

Modernize aplicativos ASP.NET Web Forms na AWS

Criado por Vijai Anand Ramalingam (AWS) e Sreelaxmi Pai (AWS)

Resumo

Esse padrão descreve as etapas para modernizar um aplicativo antigo e monólito do ASP.NET Web Forms, portando-o para o ASP.NET Core na AWS.

A portabilidade de aplicativos ASP.NET Web Forms para o ASP.NET Core ajuda você a aproveitar o desempenho, a redução de custos e o ecossistema robusto do Linux. No entanto, pode ser um esforço manual significativo. Nesse padrão, o aplicativo herdado é modernizado de forma incremental usando uma abordagem em fases e, em seguida, conteinerizado na Nuvem AWS.

Considere um aplicativo monolítico antigo para um carrinho de compras. Vamos supor que ele foi criado como um aplicativo ASP.NET Web Forms e consiste em páginas.aspx com um arquivo code-behind (`aspx.cs`). O processo de modernização consiste em três etapas:

1. Divida o monólito em microsserviços usando os padrões de decomposição apropriados. Para obter mais informações, consulte o guia Decomposição de monólitos em microsserviços no site de Recomendações da AWS.
2. Porte seu aplicativo antigo ASP.NET Web Forms (.NET Framework) para o ASP.NET Core no.NET 5 ou superior. Nesse padrão, você usa o Assistente de Portabilidade para .NET para verificar seu aplicativo ASP.NET Web Forms e identificar incompatibilidades com o ASP.NET Core. Isso reduz o esforço de portabilidade manual.
3. Redesenvolva a camada de interface do usuário do Web Forms usando o React. Esse padrão não abrange a remodelação da interface do usuário. Para obter instruções, consulte Criar um novo aplicativo React na documentação do React.
4. Redesenvolva o arquivo code-behind do Web Forms (interface comercial) como uma API web do ASP.NET Core. Esse padrão usa NDepend relatórios para ajudar a identificar os arquivos e dependências necessários.
5. Atualize projetos compartilhados/comuns, como Business Logic e Data Access, em seu aplicativo herdado para o.NET 5 ou superior usando o Assistente de Portabilidade para .NET.
6. Adicione serviços da AWS para complementar seu aplicativo. Por exemplo, você pode usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar os registros do seu aplicativo, e o AWS Systems Manager para armazenar as configurações do seu aplicativo.

7. Coloque o aplicativo ASP.NET Core modernizado em contêiner. Esse padrão cria um arquivo Docker que tem como destino o Linux no Visual Studio e usa o Docker Desktop para testá-lo localmente. Essa etapa pressupõe que seu aplicativo legado já esteja sendo executado em uma instância local ou no Amazon Elastic Compute Cloud (Amazon EC2) Windows. Para obter mais informações, consulte o padrão Executar um contêiner Docker da API web ASP.NET Core em uma instância do Amazon EC2 Linux.
8. Implantar o aplicativo ASP.NET core modernizado no Amazon Elastic Container Service (Amazon ECS). Esse padrão não abrange a etapa de implantação. Para obter instruções, consulte o Workshop do Amazon ECS.

> **Note**
>
> Esse padrão não abrange as etapas de desenvolvimento da interface do usuário, modernização do banco de dados ou implantação de contêineres.

Pré-requisitos e limitações

Pré-requisitos

- Visual Studio ou Visual Studio Code, baixado e instalado.
- Acesso a uma conta da AWS usando o Console de Gerenciamento da AWS e a AWS Command Line Interface (AWS CLI), versão 2. (Consulte Instruções para configurar a AWS CLI.)
- AWS Toolkit for Visual Studio (consulte instruções de configuração).
- Docker Desktop, baixado e instalado.
- .NET SDK, baixado e instalado.
- NDepend ferramenta, baixada e instalada. Para instalar a NDepend extensão para o Visual Studio, execute `NDepend.VisualStudioExtension.Installer` (consulte as instruções). Você pode selecionar o Visual Studio 2019 ou 2022, dependendo dos seus requisitos.
- Assistente de Portabilidade para .NET, baixado e instalado.

Arquitetura

Modernizando o aplicativo do carrinho de compras

O diagrama a seguir ilustra o processo de modernização de um aplicativo antigo de carrinho de compras ASP.NET.

Arquitetura de destino

O diagrama a seguir ilustra a arquitetura do aplicativo de carrinho de compras modernizado na AWS. O ASP.NET Core web APIs é implantado em um cluster Amazon ECS. Os serviços de registro e configuração são fornecidos pela Amazon CloudWatch Logs e pelo AWS Systems Manager.

Ferramentas

Serviços da AWS

- Amazon ECS: o Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido para execução, interrupção e gerenciamento de contêineres em um cluster. Você pode executar tarefas e serviços em uma infraestrutura com tecnologia gerenciada pelo AWS Fargate. Como alternativa, para ter mais controle sobre sua infraestrutura, você pode executar suas tarefas e serviços em um cluster de EC2 instâncias que você gerencia.
- Amazon CloudWatch Logs — O Amazon CloudWatch Logs centraliza os registros de todos os seus sistemas, aplicativos e serviços da AWS que você usa. Você pode visualizar e monitorar os logs, pesquisá-los em busca de códigos de erro ou padrões específicos, filtrá-los com base em campos específicos ou arquivá-los com segurança para análise futura.
- AWS Systems Manager – O AWS Systems Manager é um serviço da AWS que você pode usar para visualizar e controlar sua infraestrutura na AWS. Usando o console do Systems Manager, você pode visualizar dados operacionais de vários serviços da AWS e automatizar tarefas operacionais nos recursos da AWS. O Systems Manager ajuda você a manter a segurança e a conformidade verificando suas instâncias gerenciadas e gerando relatórios (ou tomando medidas corretivas) sobre quaisquer violações de políticas detectadas.

Ferramentas

- Visual Studio ou Visual Studio Code — Ferramentas para criar aplicativos.NET APIs, web e outros programas.
- AWS Toolkit for Visual Studio: uma extensão do Visual Studio que ajuda a desenvolver, depurarem e implantarem aplicações .NET que usam os serviços da AWS.

- Docker Desktop: uma ferramenta que simplifica a criação e a implantação de aplicativos em contêineres.
- NDepend— Um analisador que monitora o código.NET em busca de dependências, problemas de qualidade e alterações no código.
- Assistente de Portabilidade para .NET: uma ferramenta de análise que escaneia o código .NET para identificar incompatibilidades com o.NET Core e estimar o esforço de migração.

Épicos

Porte seu aplicativo herdado para o.NET 5 ou versão posterior

Tarefa	Descrição	Habilidades necessárias
Atualize seu aplicativo herdado do .NET Framework para o .NET 5.	Você pode usar o Assistente de Portabilidade para .NET para converter seu aplicativo herdado ASP.NET Web Forms em .NET 5 ou superior. Siga as instruções na documentação do Assistente de Portabilidade para .NET.	Desenvolvedor de aplicativos
Gere NDepend relatórios.	Ao modernizar seu aplicativo ASP.NET Web Forms decompondo-o em microsserviços, talvez você não precise de todos os arquivos.cs do aplicativo herdado. Você pode usar NDepend para gerar um relatório para qualquer arquivo code-behind (.cs), para obter todos os chamadores e chamadores. Esse relatório ajuda você a identificar e usar somente os	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	arquivos necessários em seus microsserviços. Depois de instalar NDepend (consulte a seção Pré-requisitos), abra a solução (arquivo.sln) para seu aplicativo legado no Visual Studio e siga estas etapas: 1. Crie o aplicativo herdado no Visual Studio. 2. Na barra de menu do Visual Studio NDepend, escolha Anexar novo NDepend projeto à solução VS atual. 3. Escolha Analisar conjuntos do .NET. 4. Quando a análise estiver concluída, navegue até o projeto no Solution Explorer. Clique com o botão direito do mouse em qualquer arquivo code-behind (por exemplo,`listprodu cts.aspx.cs`) para o qual você deseja gerar o relatório e escolha Mostrar no gráfico de dependências. 5. Na barra de navegação , escolha Chamadores e chamados e, em seguida,	

Tarefa	Descrição	Habilidades necessárias
	escolha Editar consulta de código. 6. No painel painel Editar consultas e regras, escolha a seta de download e escolha Exportar para o Excel. Esse processo gera um relatório para o arquivo code-behind que lista todos os chamadores e chamados. Para obter mais informações sobre o gráfico de dependênc ias, consulte a NDepend documentação.	

Tarefa	Descrição	Habilidades necessárias
Criar uma nova solução .NET 5.	Para criar uma nova estrutura do.NET 5 (ou posterior) para sua web ASP.NET Core modernizada: APIs 1. Abra o Visual Studio. 2. Crie uma solução nova e vazia. 3. Crie novos projetos voltados para o.NET 5 (ou superior), com base em seu aplicativo herdado. Para exemplos de projetos antigos e novos para um aplicativo de carrinho de compras, consulte a seção Informações adicionais. 4. Use o NDepend relatório da etapa anterior para identificar todos os arquivos necessários. Copie esses arquivos do aplicativo que você atualizou anteriorm ente e adicione-os à nova solução. 5. Crie a solução e corrija todos os problemas. Para obter mais informaçõ es sobre como criar projetos e soluções, consulte a documentação do Visual Studio.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Note Ao criar a solução e verificar a funcional idade, você pode identificar vários arquivos adicionais a serem adicionados à solução, além dos arquivos NDepend identificados.	

Atualize seu código de aplicativo.

Tarefa	Descrição	Habilidades necessárias
Implemente a web APIs com o ASP.NET Core.	Vamos supor que um dos microsserviços que você identificou em seu aplicativo antigo de carrinho de compras monolítico seja Produtos. Você criou um novo projeto de API web do ASP.NET Core para Produtos no épico anterior. Nesta etapa, você identifica e moderniza todos os formulários da web (páginas .aspx) relacionados aos Produtos. Vamos supor que os Produtos consistam em quatro formulários da web, conforme ilustrado anteriorm ente na seção Arquitetura:	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	• Listar produtos • Visualizar produto • Adicionar/Editar produto • Excluir produto Você deve analisar cada formulário da web, identificar todas as solicitações enviadas ao banco de dados para realizar alguma lógica e obter respostas. Você pode implementar cada solicitação como um endpoint de API da web. Com base em seus formulários na web, os Produtos podem ter os seguintes endpoints possíveis: • `/api/products` • `/api/products/{id}` • `/api/products/add` • `/api/products/update/{id}` • `/api/products/delete/{id}` Conforme mencionado anteriormente, você também pode reutilizar todos os outros projetos que você atualizou para o .NET 5, incluindo Business Logic, Data Access	

Tarefa	Descrição	Habilidades necessárias
	e projetos compartilhados/comuns.	
Configure o Amazon CloudWatch Logs.	Você pode usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar os registros do seu aplicativo. Você pode registrar dados no Amazon CloudWatch Logs usando um SDK da AWS. Você também pode integrar aplicativos.NET com o CloudWatch Logs usando estruturas de registro do.NET populares NLog, como Log4Net e ASP.NET Core. Para obter mais informações sobre essa etapa, consulte a postagem no blog Amazon CloudWatch Logs and .NET Logging Frameworks.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Configure a AWS Systems Manager Parameter Store.	Você pode usar o AWS Systems Manager Parameter Store para armazenar configurações do aplicativo, como strings de conexão, separadamente do código do seu aplicativo. O NuGet pacote Amazon.Extensions.Configuration.SystemsManager simplifica a forma como seu aplicativo carrega essas configurações do AWS Systems Manager Parameter Store no sistema de configuração.NET Core. Para obter mais informações sobre essa etapa, consulte a postagem no blog Provedor de configuração do .NET Core para o AWS Systems Manager.	Desenvolvedor de aplicativos

Adicione autenticação e autorização

Tarefa	Descrição	Habilidades necessárias
Use um cookie compartilhado para autenticação.	Modernizar um aplicativo monolítico herdado é um processo iterativo e exige que o monólito e sua versão modernizada coexistam. Você pode usar um cookie compartilhado para obter uma	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	autenticação perfeita entre as duas versões. O aplicativo ASP.NET herdado continua validando as credenciais do usuário e emite o cookie, enquanto o aplicativo ASP.NET Core modernizado valida o cookie. Para obter instruções e exemplos de código, consulte o GitHub projeto de amostra.	

Compilar e executar o contêiner localmente

Tarefa	Descrição	Habilidades necessárias
Criar uma imagem do Docker usando o Visual Studio.	Nesta etapa, você cria um arquivo Docker usando a API web do Visual Studio for .NET Core. 1. Abra o Visual Studio. 2. No Solution Explorer, no menu de contexto (clique com o botão direito do mouse) do projeto, escolha Add, Docker Support. 3. Selecione Linux como o sistema operacional de destino. O Visual Studio cria um arquivo Docker para seu	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	projeto. Para obter um exemplo de arquivo Docker, consulte Visual Studio Container Tools for Docker no site da Microsoft.	

Tarefa	Descrição	Habilidades necessárias

Crie e execute o contêiner usando o Docker Desktop.	Agora você pode compilar, criar e executar o contêiner no Docker Desktop.
	
	1. Abra a janela Command Prompt (Prompt de comando). Navegue até a pasta da solução em que o arquivo Docker está localizado. Execute o seguinte comando para criar a imagem do Docker:
	
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	
	2. Execute o comando a seguir para visualizar todas as imagens do Docker:
	
	`docker images`
	
	3. Execute o comando a seguir para criar e executar um contêiner:
	
	`docker run -d -p 8080:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
	
	4. Abra o Docker Desktop e escolha Contêineres/Aplicativos. Você pode ver um novo contêiner chamado
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`aspnetcorewebapicontainer` running.	

Recursos relacionados

- Execute um contêiner Docker da API web ASP.NET Core em uma instância Amazon EC2 Linux (AWS Prescriptive Guidance)
- Workshop do Amazon ECS
- Execute implantações azul/verde do ECS usando a CodeDeploy AWS (documentação da AWS) CloudFormation CloudFormation
- Começando com NDepend (NDepend documentação)
- Assistente de Portabilidade para .NET

Mais informações

As tabelas a seguir fornecem exemplos de projetos para um aplicativo antigo de carrinho de compras e os projetos equivalentes em seu aplicativo ASP.NET Core modernizado.

Solução antiga:

Nome do projeto	Modelo de projeto	Estrutura de destino
Interface de negócios	Biblioteca de classes	NET Framework
BusinessLogic	Biblioteca de classes	NET Framework
WebApplication	Aplicativo Web do ASP.NET Framework	NET Framework
UnitTests	NUnit Projeto de teste	NET Framework
Compartilhado ->Comum	Biblioteca de classes	NET Framework
Compartilhado ->Estrutura	Biblioteca de classes	NET Framework

Nova solução:

Nome do projeto	Modelo de projeto	Estrutura de destino
BusinessLogic	Biblioteca de classes	.NET 5.0
<WebAPI>	API Web do ASP.NET Core	.NET 5.0
<WebAPI>. UnitTests	NUnit 3 Projeto de teste	.NET 5.0
Compartilhado ->Comum	Biblioteca de classes	.NET 5.0
Compartilhado ->Estrutura	Biblioteca de classes	.NET 5.0

Executar workloads agendadas e orientadas por eventos em grande escala com o AWS Fargate

Criado por HARI OHM PRASATH RAJAGOPAL (AWS)

Resumo

Aviso: CodeCommit A AWS não está mais disponível para novos clientes. Os clientes atuais da AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão descreve como executar workloads agendadas e orientadas por eventos em grande escala na Nuvem da Amazon Web Services (AWS) usando o AWS Fargate.

No caso de uso configurado por esse padrão, o código é escaneado em busca de informações confidenciais da AWS, como o número da conta e as credenciais da AWS, sempre que uma solicitação pull é enviada. O solicitação pull inicia uma função do Lambda. A função do Lambda invoca uma tarefa do Fargate que cuida da verificação do código. O Lambda é inicializado sempre que uma nova solicitação pull é gerada. Se o escaneamento encontrar alguma informação confidencial, o Amazon Simple Notification Service (Amazon SNS) enviará os resultados do escaneamento em uma mensagem de e-mail.

Esse padrão é útil nos seguintes casos de uso comercial:

- Se sua empresa precisar executar muitas workloads agendadas e orientadas por eventos que não conseguem ser executadas pelo AWS Lambda devido a limitações em relação ao runtime (um limite de 15 minutos) ou à memória
- Se você quiser que a AWS gerencie as instâncias provisionadas para essas workloads

Ao usar esse padrão, você tem a opção de criar uma nova nuvem privada virtual (VPC). Esse padrão também usa AWS CodeCommit.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS CodeCommit para hospedar a base de código e criar pull requests
- AWS Command Line Interface (AWS CLI) versão 1.7 ou mais recente, instalada e configurada no macOS, Linux ou Windows

- Workloads em execução em contêineres
- Apache Maven executável e configurado no classpath

Arquitetura

Este fluxo geral inclui as seguintes etapas.

1. Sempre que uma nova pull request é enviada CodeCommit, uma função Lambda é iniciada. A função Lambda escuta o evento por `CodeCommit Pull Request State Change` meio da Amazon. EventBridge
2. A função do Lambda envia uma nova tarefa do Fargate com os seguintes parâmetros de ambiente para verificar o código e digitalizá-lo.

   ```
   RUNNER # <<TaskARN>>
   SNS_TOPIC # <<SNSTopicARN>>
   SUBNET # <<Subnet in which Fargate task gets launched>>
   ```

   Se o escaneamento encontrar informações confidenciais no código, Fargate envia uma nova mensagem para o tópico do Amazon SNS.
3. Um assinante do SNS lê a mensagem do tópico e envia uma mensagem de e-mail.

Tecnologia

- AWS CodeCommit
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon EventBridge
- AWS Fargate
- AWS Lambda
- Amazon SNS
- Docker

Ferramentas

Ferramentas

- AWS CLI: a interface de linha de comandos (CLI) é uma ferramenta unificada para gerenciar os serviços da AWS.
- AWS CodeCommit — CodeCommit A AWS é um serviço de controle de origem totalmente gerenciado que hospeda repositórios seguros baseados em Git. Usando CodeCommit, as equipes podem colaborar no código em um ambiente seguro e altamente escalável.
- Amazon ECR: o Amazon Elastic Container Registry (Amazon ECR) é um registro totalmente gerenciado que os desenvolvedores podem usar para armazenar, gerenciar e implantar imagens de contêiner do Docker.
- Amazon ECS: o Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente rápido e escalável. Você pode usar o Amazon ECS para executar, interromper e gerenciar contêineres em um cluster.
- AWS Fargate — O AWS Fargate é uma tecnologia que você pode usar com o Amazon ECS para executar contêineres sem precisar gerenciar servidores ou clusters de instâncias da Amazon. EC2
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens de editores para assinantes (também conhecido como produtores e consumidores). Os publicadores se comunicam de maneira assíncrona com os assinantes produzindo e enviando mensagens para um tópico, que é um canal de comunicação e um ponto de acesso lógico. Os clientes que assinaram o tópico SNS recebem mensagens publicadas usando um protocolo compatível, como Lambda, e-mail, notificações push móveis e mensagens de texto móveis (SMS).
- Docker: o Docker ajuda você a compilar, testar e entregar aplicativos em pacotes chamados contêineres.
- Cliente Git: ferramenta de linha de comando ou desktop para verificar os artefatos necessários
- Maven: o Apache Maven é uma ferramenta de gerenciamento de projetos para gerenciar centralmente a compilação, os relatórios e a documentação de um projeto.

Épicos

Configurar o repositório local

Tarefa	Descrição	Habilidades necessárias
Baixe o código.	Na seção Anexos, baixe o arquivo .zip e extraia os arquivos.	Desenvolvedor, administrador de sistemas da AWS
Configure o repositório.	Execute `mvn clean install` na pasta raiz.	Desenvolvedor, administrador de sistemas da AWS

Crie uma imagem do Amazon ECR e envie a imagem

Tarefa	Descrição	Habilidades necessárias
Crie um repositório do Amazon ECR e faça o login.	Abra o console do Amazon ECR. No painel de navegação , selecione Repositórios e, em seguida, Criar repositór io. Para obter ajuda com esse e outros artigos, consulte a seção Recursos relacionados.	Desenvolvedor, administrador de sistemas da AWS
Envie a imagem do seu contêiner.	Abra o repositório, escolha Exibir comandos push e registre no Docker. Depois de fazer login, execute os comandos, com as substitui ções necessárias, que estão em Enviar a imagem do contêiner na seção Informaçõ es adicionais. Isso carrega a imagem do contêiner do Docker que é usada para realizar o escaneamento de	Desenvolvedor, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	código. Quando o upload estiver concluído, copie o URL da compilação mais recente no repositório do Amazon ECR.	

Crie o CodeCommit repositório

Tarefa	Descrição	Habilidades necessárias
Crie o CodeCommit repositór io.	Para criar um novo CodeCommit repositório da AWS, execute o comando em Criar o CodeCommit repositór io na seção Informações adicionais.	Desenvolvedor, administrador de sistemas da AWS

Crie a VPC (opcional)

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	Se você quiser usar uma nova VPC em vez de uma existente , execute os comandos em Criar uma VPC na seção Informações adicionais. O script do AWS Cloud Development Kit (AWS CDK) produzirá a IDs VPC e a sub-rede que foram criadas.	Desenvolvedor, administrador de sistemas da AWS

Crie o cluster do Amazon ECS e a tarefa Fargate

Tarefa	Descrição	Habilidades necessárias
Crie o cluster e a tarefa.	Para criar um cluster do Amazon ECS e uma definição de tarefa do Fargate, execute os comandos em Criar o cluster e a tarefa na seção Informações adicionais. Certifique-se de que o ID da VPC e o URI do repositório Amazon ECR corretos sejam passados como um parâmetro ao executar o script de shell. O script cria uma definição de tarefa do Fargate que aponta para a imagem do Docker (responsável pela digitaliz ação). Em seguida, o script cria um trabalho e um perfil de execução associada.	Desenvolvedor, administrador de sistemas da AWS
Verifique o cluster do Amazon ECS.	Abra o console do Amazon ECS. No painel de navegação , escolha Clusters e escolha o cluster recém-criado do Amazon ECS chamado Fargate-Job-Cluster. Depois disso, escolha Definição de tarefa no painel de navegação e confirme se há uma nova definição de tarefa com o prefixo `awscdkfar gateecsTaskDef` .	Desenvolvedor, administrador de sistemas da AWS

Crie o tópico e o assinante do SNS

Tarefa	Descrição	Habilidades necessárias
Criar um tópico do SNS.	Para criar um tópico do SNS, execute o comando em Criar o tópico do SNS na seção Informações adicionais. Depois que a criação for bem-sucedida, observe o `SNS ARN`, que será usado na próxima etapa.	Desenvolvedor, administrador de sistemas da AWS
Crie o assinante do SNS.	Para criar um assinante de e-mail para o tópico do SNS, execute o comando em Criar o tópico do SNS na seção Informações adicionais. Certifique-se de substituir `TopicARN` e `Email address` usados no comando CLI. Para receber notificações por e-mail, confirme o endereço de e-mail usado como assinante.	Desenvolvedor, administrador de sistemas da AWS

Crie a função Lambda e acione CodeCommit

Tarefa	Descrição	Habilidades necessárias
Crie a função e o trigger.	Para criar uma função Lambda com um CodeCommit gatilho, execute o comando em Função Lambda e CodeCommit acione na seção Informações adicionai	Desenvolvedor, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
	s. Certifique-se de substituir os parâmetros pelos valores correspondentes antes de executar o comando. O script cria a função do Lambda e a configura para ser invocada quando uma nova solicitação pull é feita.	

Teste o aplicativo

Tarefa	Descrição	Habilidades necessárias
Testar o aplicativo.	Se você inserir qualquer informação confidencial da AWS no CodeCommit repositório, a função Lambda deverá ser iniciada. A função do Lambda inicia a tarefa Fargate, que escaneia o código e envia os resultados da verificação em uma notificação por e-mail.	Desenvolvedor, administrador de sistemas da AWS

Recursos relacionados

- Criação de um repositório do Amazon ECR
- Enviar por push as imagens do Docker para o Amazon ECR

Mais informações

Empurre a imagem do contêiner

```
> cd 1-ecr-image-push
```

```
> ./run.sh <<ecr-repository>>
```

Crie o CodeCommit repositório

```
aws codecommit create-repository --repository-name test-repo --repository-description
 "My Test repository"
```

Criar uma VPC

```
> cd 2-create-vpc
> ./run.sh
```

Saída

```
aws-batch-cdk-vpc-efs-launch-template.privatesubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.publicsubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.vpcid = vpc-<<id>>
```

Crie o cluster e a tarefa

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 3-create-ecs-task
> ./run.sh <<vpc-id>> <<ecr-repo-uri>>
```

Saída

```
aws-cdk-fargate-ecs.CLUSTERNAME = Fargate-Job-Cluster
aws-cdk-fargate-ecs.ClusterARN = <<cluster_arn>>
aws-cdk-fargate-ecs.ContainerARN = Fargate-Container
aws-cdk-fargate-ecs.TaskARN = <<task_arn>>
aws-cdk-fargate-ecs.TaskExecutionRole = <<execution_role_arn>>
aws-cdk-fargate-ecs.TaskRole = <<task_role_arn>>
```

Criar o tópico do SNS

```
aws sns create-topic --name code-commit-topic
```

Crie o assinante do SNS

```
aws sns subscribe \
    --topic-arn <<topic_arn>> \
    --protocol email \
    --notification-endpoint <<email_address>>
```

Função e gatilho Lambda CodeCommit

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 5-Lambda-CodeCommit-Trigger
> ./run.sh <<taskarn>> <<snstopicarn>> subnet-<<id>> <<codecommitarn>>
```

Saída

```
aws-cdk-fargate-lambda-event.Cloudwatchrule = <<cloudwatchrule>>
aws-cdk-fargate-lambda-event.CodeCommitLambda = AWS-Code-Scanner-Function
aws-cdk-fargate-lambda-event.LambdaRole = <<lambdaiamrole>>
```

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Integração de locatários na arquitetura de SaaS para o modelo de silo usando C# e o AWS CDK

Criado por Tabby Ward (AWS), Susmitha Reddy Gankidi (AWS) e Vijai Anand Ramalingam (AWS)

Resumo

Os aplicativos de software como serviço (SaaS) podem ser criados com uma variedade de modelos arquitetônicos diferentes. O modelo de silo se refere a uma arquitetura em que os locatários recebem recursos dedicados.

Os aplicativos SaaS dependem de um modelo simples para introduzir novos locatários em seu ambiente. Isso geralmente requer a orquestração de vários componentes para provisionar e configurar com êxito todos os elementos necessários para criar um novo locatário. Esse processo, na arquitetura SaaS, é chamado de integração de locatários. A integração deve ser totalmente automatizada para cada ambiente SaaS, utilizando a infraestrutura como código em seu processo de integração.

Esse padrão orienta você por meio de um exemplo de criação de um locatário e provisionamento de uma infraestrutura básica para o locatário na Amazon Web Services (AWS). O padrão usa C# e o AWS Cloud Development Kit (AWS CDK).

Como esse padrão cria um alarme de faturamento, recomendamos implantar a pilha na região da AWS do Leste dos EUA (Norte da Virgínia) ou us-east-1. Para obter mais informações, consulte a documentação da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma entidade principal do Identity and Access Management (IAM) da AWS com acesso suficiente ao IAM para criar recursos da AWS para esse padrão. Para obter mais informações, consulte os perfis do IAM.
- Instale a Amazon Command Line Interface (AWS CLI) e configure a AWS CLI para realizar a implantação do AWS CDK.
- Visual Studio 2022 baixado e instalado ou Visual Studio Code baixado e instalado.
- Configuração do AWS Toolkit for Visual Studio.

- .NET Core 3.1 ou superior (exigido para aplicativos C# AWS CDK)
- Amazon.Lambda.Tools instalado.

Limitações

- O AWS CDK usa a AWS CloudFormation, então os aplicativos do AWS CDK estão sujeitos às cotas de CloudFormation serviço. Para obter mais informações, consulte as CloudFormation cotas da AWS.
- A CloudFormation pilha de inquilinos é criada com uma função CloudFormation de serviço `infra-cloudformation-role` com caracteres curinga nas ações (`sns* esqs*`), mas com recursos restritos ao prefixo. `tenant-cluster` Para um caso de uso de produção, avalie essa configuração e forneça somente o acesso necessário a esse perfil de serviço. A função `InfrastructureProvision` Lambda também usa um caractere curinga (`cloudformation*`) para provisionar a CloudFormation pilha, mas com recursos restritos ao prefixo. `tenant-cluster`
- Este exemplo de código docker usa `--platform=linux/amd64` para forçar imagens baseadas em `linux/amd64`. Isso é para garantir que os artefatos finais da imagem sejam adequados para o Lambda que, por padrão, usa a arquitetura x86-64. Se você precisar alterar a arquitetura Lambda de destino, certifique-se de alterar os códigos do Dockerfiles e do AWS CDK. Para obter mais informações, consulte a publicação do blog Migrar funções do Lambda AWS para processadores AWS Graviton2 baseados em ARM.
- O processo de exclusão da pilha não limpará CloudWatch os registros (grupos de registros e registros) gerados pela pilha. Você deve limpar manualmente os registros por meio do AWS Management Console, CloudWatch console da Amazon ou por meio da API.

Esse padrão é configurado como exemplo. Para uso em produção, avalie as seguintes configurações e faça alterações com base nos requisitos da sua empresa:

- O bucket do AWS Simple Storage Service (Amazon S3) neste exemplo não tem o versionamento habilitado para simplificar. Avalie e atualize a configuração conforme necessário.
- Este exemplo configura os endpoints da API REST do Amazon API Gateway sem autenticação, autorização ou controle de utilização para simplificar. Para uso em produção, recomendamos integrar o sistema à infraestrutura de segurança da empresa. Avalie essa configuração e adicione as configurações de segurança exigidas conforme necessário.
- Para este exemplo de infraestrutura de locatários, o Amazon Simple Notification Service (Amazon SNS) e o Amazon Simple Queue Service (Amazon SQS) têm apenas configurações mínimas. O

AWS Key Management Service (AWS KMS) de cada locatário abre os serviços da Amazon e do Amazon CloudWatch SNS na conta para consumo com base na política de chaves do AWS KMS. A configuração é apenas um exemplo de espaço reservado. Ajuste as configurações conforme necessário com base no seu caso de uso de negócios.

- Toda a configuração, que inclui, mas não se limita a endpoints de API e inquilinos de back-end, provisionamento e exclusão usando a AWS CloudFormation, abrange apenas o caso básico do Happy Path. Avalie e atualize a configuração com a lógica de repetição necessária, a lógica adicional de tratamento de erros e a lógica de segurança com base nas necessidades de sua empresa.
- O código de exemplo é testado com up-to-date cdk-nag para verificar as políticas no momento da redação deste artigo. Novas políticas podem ser aplicadas no futuro. Essas novas políticas podem exigir que você modifique manualmente a pilha com base nas recomendações antes que a pilha possa ser implantada. Revise o código existente para garantir que ele esteja alinhado aos requisitos da sua empresa.
- O código depende do AWS CDK para gerar um sufixo aleatório em vez de depender de nomes físicos atribuídos estáticos para a maioria dos recursos criados. Essa configuração é para garantir que esses recursos sejam exclusivos e não entrem em conflito com outras pilhas. Para obter mais informações, consulte a documentação do AWS CDK. Ajuste isso com base nos requisitos da sua empresa.
- Este código de exemplo empacota artefatos do.NET Lambda em imagens baseadas em Docker e é executado com o Runtime de imagem de contêiner fornecido pelo Lambda. O runtime da imagem do contêiner tem vantagens para mecanismos padrão de transferência e armazenamento (registros de contêiner) e ambientes de teste locais mais precisos (por meio da imagem do contêiner). Você pode mudar o projeto para usar os .NET runtimes fornecidos pelo Lambda para reduzir o tempo de criação das imagens do Docker, mas precisará configurar mecanismos de transferência e armazenamento e garantir que a configuração local corresponda à configuração do Lambda. Ajuste o código de acordo com os requisitos comerciais dos usuários.

Versões do produto

- AWS CDK versão 2.45.0 ou superior
- Visual Studio 2022

Arquitetura

Pilha de tecnologia

- Amazon API Gateway
- AWS CloudFormation
- Amazon CloudWatch
- Amazon DynamoDB
- AWS Identity and Access Management (IAM)
- AWS KMS
- AWS Lambda
- Amazon S3
- Amazon SNS
- Amazon SQS

Arquitetura

O diagrama a seguir mostra o fluxo de criação da pilha de locatários. Para obter mais informações sobre o ambiente de gerenciamento e as pilhas de tecnologia do locatário, consulte a seção Informações adicionais.

Fluxo de criação da pilha de locatários

1. O usuário envia uma solicitação da API POST com a nova carga útil do locatário (nome do locatário, descrição do locatário) em JSON para uma API REST hospedada pelo Amazon API Gateway. O API Gateway processa a solicitação e a encaminha para a função de backend do Lambda Tenant Onboarding. Neste exemplo, não há autorização nem autenticação. Em uma configuração de produção, essa API deve ser integrada ao sistema de segurança da infraestrutura SaaS.
2. A função de integração do locatário verifica a solicitação. Em seguida, ele tenta armazenar o registro do locatário, que inclui o nome do locatário, o identificador único universal (UUID) gerado e a descrição do locatário, na tabela de integração de locatários do Amazon DynamoDB.
3. Depois que o DynamoDB armazena o registro, um stream do DynamoDB inicia a função downstream da Lambda Tenant Infrastructure.

4. A função do Lambda Tenant Infrastructure atua com base no stream recebido do DynamoDB. Se o stream for para o evento INSERT, a função usa a NewImage seção do stream (registro de atualização mais recente, campo Nome do inquilino) para invocar CloudFormation a criação de uma nova infraestrutura de locatário usando o modelo armazenado no bucket do S3. O CloudFormation modelo exige o parâmetro Nome do inquilino.
5. CloudFormation A AWS cria a infraestrutura do locatário com base no CloudFormation modelo e nos parâmetros de entrada.
6. Cada configuração de infraestrutura do inquilino tem um CloudWatch alarme, um alarme de cobrança e um evento de alarme.
7. O evento de alarme se torna uma mensagem para um tópico do SNS, que é criptografado pela chave do AWS KMS do locatário.
8. O tópico do SNS encaminha a mensagem de alarme recebida para a fila do SQS, que é criptografada pelo AWS KMS do locatário para a chave de criptografia.

Outros sistemas podem ser integrados ao Amazon SQS para realizar ações com base nas mensagens na fila. Neste exemplo, para manter o código genérico, as mensagens recebidas permanecem na fila e exigem exclusão manual.

Fluxo de exclusão da pilha de locatários

1. O usuário envia uma solicitação da API DELETE com a nova carga útil do locatário (nome do locatário, descrição do locatário) em JSON para a API REST hospedada pelo Amazon API Gateway, que processará a solicitação e encaminhará para a função de integração do locatário. Neste exemplo, não há autorização nem autenticação. Em uma configuração de produção, essa API será integrada ao sistema de segurança da infraestrutura SaaS.
2. A função de integração do locatário verificará a solicitação e, em seguida, tentará excluir o registro do locatário (nome do locatário) da tabela de integração do locatário.
3. Depois que o DynamoDB exclui o registro com sucesso (o registro existe na tabela e é excluído), um stream do DynamoDB inicia a função downstream do Lambda Tenant Infrastructure.
4. A função do Lambda Tenant Infrastructure atua com base no registro de stream recebido do DynamoDB. Se o stream for para o evento REMOVE, a função usa a OldImage seção do registro (informações do registro e campo Nome do inquilino, antes da última alteração, que é exclusão) para iniciar a exclusão de uma pilha existente com base nas informações desse registro.
5. A AWS CloudFormation exclui a pilha de inquilinos de destino de acordo com a entrada.

Ferramentas

Serviços da AWS

- O Amazon API Gateway ajuda você a criar, publicar, manter, monitorar e proteger REST, HTTP e WebSocket APIs em qualquer escala.
- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- O AWS CDK Toolkit é um kit de desenvolvimento de nuvem de linha de comando que ajuda você a interagir com seu aplicativo AWS Cloud Development Kit (AWS CDK).
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Queue Service (Amazon SQS) oferece uma fila hospedada segura, durável e disponível que permite integrar e desacoplar sistemas de software e componentes distribuídos.
- O AWS Toolkit for Visual Studio é um plug-in para o ambiente de desenvolvimento integrado (IDE) do Visual Studio. O Toolkit for Visual Studio oferece suporte ao desenvolvimento, depuração e implantação de aplicativos.NET que usam serviços da AWS.

Outras ferramentas

- O Visual Studio é um IDE que inclui compiladores, ferramentas de preenchimento de código, designers gráficos e outros atributos que oferecem suporte ao desenvolvimento de software.

Código

O código desse padrão está no repositório de exemplos de integração de locatários na arquitetura SaaS para modelo de silo do APG.

Épicos

Configurar o AWS CDK

Tarefa	Descrição	Habilidades necessárias
Verifique a instalação do Node.js.	Para verificar se o Node.js está instalado em sua máquina local, execute o comando a seguir. `node --version`	Administrador da AWS, AWS DevOps
Instale o AWS CDK Toolkit.	Para instalar o AWS CDK Toolkit em sua máquina local, execute o comando a seguir. `npm install -g aws-cdk` Se o npm não estiver instalado, você poderá instalá-lo no site Node.js.	Administrador da AWS, AWS DevOps
Verifique a versão do AWS CDK Toolkit.	Para verificar se a versão do AWS CDK Toolkit está instalada corretamente em sua máquina, execute o comando a seguir.	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`cdk --version`	

Revise o código do ambiente de gerenciamento de integração do locatário

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Clone o repositório e navegue até a pasta `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example` . Abra a `\src\TenantOnboardingInfra.sln` solução no Visual Studio 2022. Abra o arquivo `TenantOnboardingInfraStack.cs` e revise o código. Os seguintes recursos são criados como parte dessa pilha: • Tabela do DynamoDB • Bucket S3 (faça upload do CloudFormation modelo para o bucket S3.) • Função de execução do Lambda • Função do Lambda • API do API Gateway	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• Fonte do evento para a função do Lambda	
Revise o CloudFormation modelo.	Na `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\template pastainfra.yaml`, abra e revise o CloudFormation modelo. Esse modelo será hidratado com o nome do locatário recuperado da tabela de integração do locatário do DynamoDB. O modelo fornece a infraestrutura específica do locatário. Neste exemplo, ele provisiona a chave do AWS KMS, o Amazon SNS, o Amazon SQS e o alarme. CloudWatch	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Analise a função de integração do locatário.	Abra `Function.cs` e revise o código da função de integração do locatário, que é criada com o modelo do Projeto AWS Lambda do Visual Studio (.NET Core-C#) com o blueprint .NET 6 (Contêiner Image). Abra o `Dockerfile` arquivo e revise o código. `Dockerfile` é um arquivo de texto que consiste em instruções para criar a imagem do contêiner Lambda. Observe que os seguintes NuGet pacotes foram adicionados como dependências ao `TenantOnboardingFunction` projeto: • `Amazon.Lambda.APIGatewayEvents` • `AWSSDK.DynamoDBv2` • `Newtonsoft.Json`	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Revise a InfraProvisioning função de inquilino.	Acesse `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\InfraProvisioningFunction` . Abra `Function.cs` e revise o código da função de integração do locatário, que é criada com o modelo do Projeto AWS Lambda do Visual Studio (.NET Core-C#) com o esquema .NET 6 (Contêiner Image). Abra o `Dockerfile` arquivo e revise o código. Observe que os seguintes NuGet pacotes foram adicionados como dependências ao `InfraProvisioningFunction` projeto: • `Amazon.Lambda.DynamoDBEvents` • `AWSSDK.DynamoDBv2` • `AWSSDK.Cloudformation`	Desenvolvedor de aplicativos, AWS DevOps

Implantar os recursos da AWS

Tarefa	Descrição	Habilidades necessárias
Crie a solução.	Para criar a solução, siga estas etapas: 1. Abra a `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra.sln` solução no Visual Studio 2022. 2. Abra o menu contextual (botão direito do mouse) da solução e escolha Criar solução. **Note** Certifique-se de atualizar o `Amazon.CDK.Lib` `NuGet` pacote para a versão mais recente do `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra`	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	projeto antes de criar a solução.	

Faça o bootstrap do ambiente do AWS CDK.	Abra o prompt de comando do Windows e navegue até a pasta raiz do aplicativo AWS CDK em que o arquivo `cdk.json` está disponível (`\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example`). Execute o comando a seguir para inicializar.
	`cdk bootstrap`
	Se você criou um perfil da AWS para as credenciais, use o comando com seu perfil.
	`cdk bootstrap --profile <profile name>`
		Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Liste as pilhas do AWS CDK.	Para listar todas as pilhas a serem criadas como parte desse projeto, execute o comando a seguir.
	`cdk ls`
	`cdk ls --profile <profile name>`
	Se você criou um perfil da AWS para as credenciais, use o comando com seu perfil.
	`cdk ls --profile <profile name>`
		Administrador da AWS, AWS DevOps

Analise quais recursos da AWS serão criados.	Para analisar todos os recursos da AWS que serão criados como parte desse projeto, execute o comando a seguir.
	`cdk diff`
	Se você criou um perfil da AWS para as credenciais, use o comando com seu perfil.
	`cdk diff --profile <profile name>`
		Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Implante todos os recursos da AWS usando o AWS CDK.	Para implantar todos os recursos da AWS, execute o seguinte comando.
	`cdk deploy --all --require-approval never`
	Se você criou um perfil da AWS para as credenciais, use o comando com seu perfil.
	`cdk deploy --all --require-approval never --profile <profile name>`
	Depois que a implantação for concluída, copie a URL da API da seção de saídas no prompt de comando, que é mostrada no exemplo a seguir.
	`Outputs: TenantOnboardingInfraStack.TenantOnboardingAPIEndpoint42E526D7 = https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/`
		Administrador da AWS, AWS DevOps

Verificação de funcionalidade

Tarefa	Descrição	Habilidades necessárias

Criar um novo locatário.	Para criar o novo locatário, envie a seguinte solicitação curl.
	
	`curl -X POST <TenantOnboardingAPIEndpoint* from CDK Output>tenant -d '{"Name":"Tenant123", "Description":"Stack for Tenant123"}'`
	
	Altere o espaço reservado `<TenantOnboardingAPIEndpoint* from CDK Output>` para o valor real do AWS CDK, conforme mostrado no exemplo a seguir.
	
	`curl -X POST https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant -d '{"Name": "Tenant123", "Description":"test12"}'`
	
	O exemplo a seguir mostra a saída.
	
	`{"message": "A new tenant added - 5/4/2022 7:11:30 AM"}`
		Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Verifique os detalhes do locatário recém-criado no DynamoDB.	Para verificar os detalhes do locatário recém-criado no DynamoDB, execute as etapas a seguir. 1. Abra o Console de Gerenciamento da AWS e navegue até o serviço Amazon DynamoDB. 2. No painel de navegação à esquerda, escolha Explorar itens e escolha a tabela `TenantOnboarding` . **Note** O nome do inquilino será prefixado com. `tenantcluster-` Para obter mais informações, consulte a seção Informações adicionais. 3. Verifique se um novo item foi criado com os detalhes do locatário.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Verifique a criação da pilha para o novo locatário.	Verifique se a nova pilha foi criada e provisionada com sucesso com a infraestrutura para o inquilino recém-criado, de acordo com o modelo. CloudFormation 1. Abra o CloudFormation console. 2. No painel de navegação à esquerda, selecione Pilhas e verifique se uma pilha com o nome do locatário foi criada com sucesso. 3. Escolha a pilha de locatário s recém-criada e depois a guia Recursos. Observe o recurso de alarme e o recurso do Amazon SQS. 4. Abra um novo terminal com as credenciais da AWS configuradas e aponte para a região correta. Para acionar um alarme de teste, digite o código a seguir, substituindo `<alarm resource name>` pelo nome do recurso de alarme anotado na etapa 3. `aws cloudwatch set-alarm-state --alarm-name <alarm resource name> --state-value`	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	ALARM --state-reason 'Test setup' O exemplo a seguir mostra o código com o nome do recurso de alarme. `aws cloudwatch set-alarm-state --alarm-name tenantcluster-tenant123-alarm --state-value ALARM --state-reason 'Test setup'` 5. Abra o console e navegue até o console do Amazon SQS. Escolha o nome do recurso Amazon SQS identificado na etapa 3. Siga as instruções da documentação da AWS para receber e excluir a mensagem de teste do alarme que foi acionado na etapa 4.	

Tarefa	Descrição	Habilidades necessárias

Exclua a pilha de locatários.	Para excluir a pilha de locatários, envie a seguinte solicitação curl.
	`curl -X DELETE <TenantOnboardingAPIEndpoint* from CDK Output>tenant/<Tenant Name from previous step>`
	Altere o espaço reservado `<TenantOnboardingAPIEndpoint* from CDK Output>` para o valor real do AWS CDK e altere `<Tenant Name from previous step>` para o valor real da etapa anterior de criação do locatário, conforme mostrado no exemplo a seguir.
	`curl -X DELETE https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant/Tenant123`
	O exemplo a seguir mostra a saída.
	`{"message": "Tenant destroyed - 5/4/2022 7:14:48 AM"}`
		Desenvolvedor de aplicativos, AWS DevOps, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Verifique a exclusão da pilha para o locatário existente.	Para verificar se a pilha de locatários existente foi excluída, execute as etapas a seguir: 1. Abra o console e navegue até o CloudFormation console. 2. Na navegação à esquerda, verifique se a pilha existente com o nome do inquilino não está mais no console (se o CloudFormation console estiver configurado para mostrar somente pilhas ativas) ou está em processo de exclusão. Se a pilha não estiver mais no CloudFormation console, use a lista suspensa para alterar a configuração do console de Ativo para Excluído para ver a pilha excluída e verificar se a pilha foi excluída com sucesso.	Desenvolvedor de aplicativos, administrador da AWS, AWS DevOps

Limpeza

Tarefa	Descrição	Habilidades necessárias
Destruir o ambiente.	Antes da limpeza da pilha, certifique-se do seguinte:	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	• Todos os registros no DynamoDB são removidos por meio da operação anterior de exclusão de locatários ou por meio do console ou da API do DynamoDB. Cada exclusão do registro do inquilino iniciará a limpeza de sua contraparte da AWS. CloudFormation • Todas as CloudFormation pilhas da AWS baseadas em locatários são limpas (caso a lógica de limpeza do gatilho do DynamoDB falhe) no console da AWS. CloudFormation Após a conclusão do teste, o AWS CDK pode ser usado para destruir todas as pilhas e recursos relacionados executando o comando a seguir. `cdk destroy --all;` Se você criou um perfil da AWS para as credenciais, use o perfil.	

Tarefa	Descrição	Habilidades necessárias
	Confirme a solicitação de exclusão da pilha para excluir a pilha.	
Limpe os Amazon CloudWatch Logs.	O processo de exclusão da pilha não limpará CloudWatch os registros (grupos de registros e registros) que foram gerados pela pilha. Limpe manualmente os CloudWatch recursos usando o CloudWatch console ou a API.	Desenvolvedor de aplicativos, AWS DevOps, administrador da AWS

Recursos relacionados

- Workshop sobre o AWS CDK.NET
- Trabalhar com o AWS CDK em C#
- Referência do CDK.NET

Mais informações

Pilha de tecnologias de ambiente de gerenciamento

O código CDK escrito em.NET é usado para provisionar a infraestrutura do plano de controle, que consiste nos seguintes recursos:

1. API Gateway

   Serve como ponto de entrada da API REST para a pilha do plano de controle.
2. Função do Lambda de integração do locatário

   Essa função do Lambda é iniciada pelo API Gateway usando o método m.

   Uma solicitação de API do método POST resulta na inserção (`tenant name`,`tenant description`) na tabela `Tenant Onboarding` do DynamoDB.

Neste exemplo de código, o nome do locatário também é usado como parte do nome da pilha do locatário e dos nomes dos recursos dentro dessa pilha. Isso é para facilitar a identificação desses recursos. Esse nome de locatário deve ser exclusivo em toda a configuração para evitar conflitos ou erros. A configuração detalhada da validação de entrada é explicada na documentação dos perfis do IAM e na seção Limitações.

O processo de persistência na tabela do DynamoDB só será bem-sucedido se o nome do locatário não for usado em nenhum outro registro na tabela.

O nome do locatário nesse caso é a chave de partição dessa tabela, pois somente a chave de partição pode ser usada como uma expressão da condição `PutItem`.

Se o nome do locatário nunca tiver sido registrado antes, o registro será salvo na tabela com sucesso.

No entanto, se o nome do locatário já for usado por um registro existente na tabela, a operação falhará e iniciará uma exceção do DynamoDB. `ConditionalCheckFailedException` A exceção será usada para retornar uma mensagem de falha (`HTTP BadRequest`) indicando que o nome do locatário já existe.

Uma solicitação de API de método de `DELETE` removerá o registro de um nome de locatário específico da tabela `Tenant Onboardin` g.

A exclusão do registro do DynamoDB neste exemplo será bem-sucedida mesmo que o registro não exista.

Se o registro de destino existir e for excluído, ele criará um registro de stream do DynamoDB. Caso contrário, nenhum registro downstream será criado.

3. Integração de locatários no DynamoDB, com o Amazon DynamoDB Streams habilitado

   Isso registra as informações de metadados do locatário, e qualquer registro salvo ou excluído enviará um stream downstream para a `Tenant Infrastructure` função do Lambda.

4. A Função do Lambda da infraestrutura do locatário

   Essa função do Lambda é iniciada pelo registro de stream do DynamoDB da etapa anterior. Se o registro for de um `INSERT` evento, ele invoca CloudFormation a AWS para criar uma nova infraestrutura de locatários com o CloudFormation modelo armazenado em um bucket do S3. Se

o registro for para `REMOVE`, ele iniciará a exclusão de uma pilha existente com base no campo do registro do stream `Tenant Name`.

5. S3 bucket

   Isso é para armazenar o CloudFormation modelo.

6. Funções do IAM para cada função do Lambda e uma função de serviço para CloudFormation

   Cada função do Lambda tem seu perfil exclusivo do IAM com permissões de privilégio mínimo para realizar sua tarefa. Por exemplo, a função do `Tenant On-boarding` Lambda tem acesso de leitura/gravação ao DynamoDB, e a função do Lambda `Tenant Infrastructure` só pode ler o stream do DynamoDB.

   Uma função CloudFormation de serviço personalizada é criada para o provisionamento da pilha de inquilinos. Essa função de serviço contém permissões adicionais para provisionamento de CloudFormation pilhas (por exemplo, a chave AWS KMS). Isso divide as funções entre o Lambda CloudFormation e evita todas as permissões em uma única função (função do Lambda de infraestrutura).

   As permissões que permitem ações poderosas (como criar e excluir CloudFormation pilhas) são bloqueadas e permitidas somente em recursos que começam com. `tenantcluster-` A exceção é o AWS KMS, devido à sua convenção de nomenclatura de recursos. O nome do locatário ingerido pela API será anexado ao `tenantcluster-`, junto com outras verificações de validação (alfanumérico somente com hífen e limitado a menos de 30 caracteres para caber na maioria dos nomes de recursos da AWS). Isso garante que o nome do locatário não resulte acidentalmente na interrupção das pilhas ou dos recursos da infraestrutura principal.

Pilha de tecnologia para locatários

Um CloudFormation modelo é armazenado no bucket do S3. O modelo provisiona a chave AWS KMS específica do inquilino, um CloudWatch alarme, um tópico do SNS, uma fila do SQS e uma política do SQS.

A chave do AWS KMS é usada para criptografia de dados pelo Amazon SNS e pelo Amazon SQS para suas mensagens. As práticas de segurança para AwsSolutions— SNS2 e AwsSolutions — SQS2 recomendam que você configure o Amazon SNS e o Amazon SQS com criptografia. No entanto, CloudWatch os alarmes não funcionam com o Amazon SNS ao usar uma chave gerenciada pela AWS, então você deve usar uma chave gerenciada pelo cliente nesse caso. Para obter mais informações, consulte o Centro de Conhecimentos da AWS.

A política do SQS é usada na fila do Amazon SQS para permitir que o tópico SNS criado entregue a mensagem à fila. Sem a política do SQS, o acesso será negado. Para obter mais informações, consulte a documentação do Amazon SNS.

Decomponha monólitos em microsserviços usando o CQRS e o fornecimento de eventos

Criado por Rodolfo Jr. Cerrada (AWS), Dmitry Gulin (AWS) e Tabby Ward (AWS)

Resumo

Esse padrão combina dois padrões, usando o padrão de separação de responsabilidade por consulta de comando (CQRS) e o padrão de fornecimento de eventos. O padrão CQRS separa as responsabilidades dos modelos de comando e consulta. O padrão de fornecimento de eventos aproveita a comunicação assíncrona orientada por eventos para melhorar a experiência geral do usuário.

Você pode usar os serviços CQRS e Amazon Web Services (AWS) para manter e escalar cada modelo de dados de forma independente enquanto refatora seu aplicativo monolítico em arquitetura de microsserviços. Em seguida, você pode usar o padrão de fornecimento de eventos para sincronizar dados do banco de dados de comandos com o banco de dados de consulta.

Esse padrão usa um código de exemplo que inclui um arquivo de solução (*.sln) que você pode abrir usando a versão mais recente do Visual Studio. O exemplo contém o código da API Reward para mostrar como o CQRS e o fornecimento de eventos funcionam em aplicativos com tecnologia sem servidor e sem servidor, tradicionais ou on-premises da AWS.

Para saber mais sobre o CQRS e o fornecimento de eventos, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Amazon CloudWatch
- Tabelas do Amazon DynamoDB
- Amazon DynamoDB Streams
- Chave de acesso e chave secreta do AWS Identity and Access Management (IAM); para obter mais informações, acesse o vídeo na seção Recursos relacionados
- AWS Lambda

- Familiaridade com o Visual Studio
- Familiaridade com o AWS Toolkit for Visual Studio; para obter mais informações, consulte o vídeo de demonstração do AWS Toolkit for Visual Studio na seção Recursos relacionados

Versões do produto

- Visual Studio 2019 Community Edition.
- AWS Toolkit for Visual Studio 2019.
- .NET Core 3.1 Esse componente é uma opção na instalação do Visual Studio. Para incluir o .NET Core durante a instalação, selecione Desenvolvimento multiplataforma NET Core.

Limitações

- O código de exemplo para um aplicativo on-premises tradicional (ASP.NET Core Web API e objetos de acesso a dados) não vem com um banco de dados. No entanto, ele vem com o objeto `CustomerData` na memória, que atua como um banco de dados simulado. O código fornecido é suficiente para você testar o padrão.

Arquitetura

Pilha de tecnologia de origem

- Projeto de API Web do ASP.NET Core
- Servidor Web IIS
- Objeto de acesso a dados
- Modelo CRUD

Arquitetura de origem

Na arquitetura de origem, o modelo CRUD contém interfaces de comando e consulta em um aplicativo. Por exemplo, código, consulte `CustomerDA0.cs` (em anexo).

Pilha de tecnologias de destino

- Amazon DynamoDB

- Amazon DynamoDB Streams
- AWS Lambda
- Amazon API Gateway
- (Opcional) Amazon Simple Notification Service (Amazon SNS)

Arquitetura de destino

Na arquitetura de destino, as interfaces de comando e consulta são separadas. A arquitetura mostrada no diagrama a seguir pode ser estendida com o API Gateway e o Amazon SNS. Para obter mais informações, consulte a seção Informações adicionais.

1. As funções de comando do Lambda realizam operações de gravação, como criar, atualizar ou excluir, no banco de dados.
2. As funções de consulta do Lambda realizam operações de leitura, como obter ou selecionar, no banco de dados.
3. Essa função do Lambda processa os fluxos do DynamoDB do banco de dados Comando e atualiza o banco de dados Consulta para as alterações.

Ferramentas

Ferramentas

- Amazon DynamoDB: o Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade integrada.
- Amazon DynamoDB Streams: o Amazon DynamoDB Streams captura uma sequência em ordem temporal de modificações em nível de item em qualquer tabela do Amazon DynamoDB. Esse serviço, então, armazena essas informações em um log por até 24 horas. A criptografia em repouso criptografa os dados em fluxos do DynamoDB.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- Console de Gerenciamento da AWS: o Console de Gerenciamento da AWS é uma aplicação web que compreende uma ampla coleção de consoles de serviço para gerenciar serviços da AWS.

- Visual Studio 2019 Community Edition: o Visual Studio 2019 é um ambiente de desenvolvimento integrado (IDE). A Community Edition é gratuita para colaboradores de código aberto. Nesse padrão, você usará o Visual Studio 2019 Community Edition para abrir, compilar e executar código de exemplo. Somente para visualização, você pode usar qualquer editor de texto ou o Visual Studio Code.
- AWS Toolkit for Visual Studio: o AWS Toolkit for Visual Studio é um plug-in para o Visual Studio IDE. O AWS Toolkit for Visual Studio facilita o desenvolvimento, a depuração e a implantação de aplicativos .NET que usam os serviços AWS.

Código

O código de exemplo está anexado. Para obter instruções sobre como implantar o código de exemplo, consulte a seção Épicos.

Épicos

Abra e crie a solução

Tarefa	Descrição	Habilidades necessárias
Abra a solução.	1. Baixe o código-fonte de exemplo (`CQRS-ES Code.zip`) na seção Anexos e extraia os arquivos. 2. No IDE do Visual Studio, escolha Arquivo, Abrir, Solução do Projeto e navegue até a pasta em que você extraiu o código-fonte. 3. Escolha AWS.APG.CQRSES.sln, e então escolha Abrir. A solução inteira é carregada no Visual Studio.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Crie a solução.	Abra o menu de contexto (clique com o botão direito do mouse) da solução e selecione Criar soluções. Isso criará e compilará todos os projetos na solução. Ele deve ser compilado com sucesso. O Visual Studio Solution Explorer deve mostrar a estrutura de diretórios. • `CQRS On-Premises Code Sample` contém um exemplo de uso do CQRS on-premises. • `CQRS AWS Serverless` contém todo o código de exemplo de CQRS e de fornecimento de eventos usando os serviços com tecnologia sem servidor da AWS.	Desenvolvedor de aplicativos

Crie as tabelas do DynamoDB

Tarefa	Descrição	Habilidades necessárias
Forneça credenciais	Se você ainda não tem uma chave de acesso, assista ao vídeo na seção Recursos relacionados. 1. No Solution Explorer, expanda CQRS AWS	Desenvolvedor de aplicativos, engenheiro de dados, DBA

Tarefa	Descrição	Habilidades necessárias
	Serverless e, em seguida, expanda a pasta da solução Build. 2. Expanda o projeto AwS.APG.CQRSES.Build e exiba o arquivo `Program.cs` . 3. Mova a barra de rolagem até o topo da `Program.cs` e procure por `Program()` . 4. Substitua `YOUR ACCESS KEY` pela chave de acesso à sua conta e substitua `YOUR SECRET KEY` pela chave secreta da sua conta. Observe que, em um ambiente de produção, você não codificaria suas chaves. Em vez disso, você pode usar o AWS Secrets Manager para armazenar e recuperar as credenciais.	
Crie o projeto.	Para criar o projeto, abra o menu de contexto (clique com o botão direito do mouse) para o projeto AwS.APG.CQRSES.Build e selecione Construir.	Desenvolvedor de aplicativos, engenheiro de dados, DBA

Tarefa	Descrição	Habilidades necessárias
Crie e preencha as tabelas.	Para criar as tabelas e preenchê-las com dados iniciais, abra o menu de contexto (clique com o botão direito do mouse) para o projeto AwS.APG.C QRSES.Build e então escolha Depurar, Iniciar nova instância .	Desenvolvedor de aplicativos, engenheiro de dados, DBA
Verifique a construção da tabela e os dados.	Para verificar, navegue até o AWS Explorer e expanda o Amazon DynamoDB. Ele deve exibir as tabelas. Abra cada tabela para exibir os dados de exemplo.	Desenvolvedor de aplicativos, engenheiro de dados, DBA

Execute testes locais

Tarefa	Descrição	Habilidades necessárias
Crie o projeto do CQRS.	1. Abra a solução e navegue até a pasta da Services/ CQRS/Tests solução CQRS AWS. 2. No AWS.APG.CQRSES. CQRSLambda.Testa o projeto, abra BaseFunct ionTest.cs e substitua AccessKeye pelas SecretKeychaves do IAM que você criou. 3. Salve as alterações.	Desenvolvedor de aplicativos, engenheiro de testes

Tarefa	Descrição	Habilidades necessárias
	4. Para compilar e criar o projeto de teste, abra o menu de contexto (clique com o botão direito do mouse) do projeto e selecione Construir.	
Crie o projeto de fornecimento de eventos.	1. Navegue até a pasta da Services/Event Source/Tests solução CQRS AWS. 2. No AWS.APG.CQRSES.EventSourceLambda.Testa o projeto, abra BaseFunctionTest.cs e substitua AccessKeye pelas SecretKeychaves do IAM que você criou. 3. Salve as alterações. 4. Para compilar e criar o projeto de teste, abra o menu de contexto (clique com o botão direito do mouse) do projeto e selecione Construir.	Desenvolvedor de aplicativos, engenheiro de testes
Execute os testes.	Para executar todos os testes, escolha Exibir, Explorador de testes e, em seguida, escolha Executar todos os testes na exibição. Todos os testes devem ser aprovados, o que é indicado por um ícone de marca de seleção verde.	Desenvolvedor de aplicativos, engenheiro de testes

Publique as funções do CQRS Lambda na AWS

Tarefa	Descrição	Habilidades necessárias
Publique a primeira função do Lambda.	1. No Solution Explorer, abra o menu de contexto (clique com o botão direito do mouse) do AWS.APG.CQRSES. CommandCreateLambda projeto e, em seguida, escolha Publicar no AWS Lambda. 2. Selecione o perfil que você deseja usar e a região da AWS em que deseja implantar a função do Lambda e o nome da função. 3. Mantenha os padrões de valores para os campos restantes e escolha Next (Avançar). 4. Na lista suspensa Nome da função, selecione. AWSLambdaFullAccess 5. Para fornecer as chaves da sua conta, escolha Adicionar e insira `AcessKey` como variável e sua chave de acesso como valor. Em seguida, escolha Adicionar novamente, insira `SecretKey` como variável e sua chave secreta como valor.	Desenvolvedor de aplicativos, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	6. Mantenha os padrões de valores para os campos restantes e escolha Upload (Carregar). Depois que a função de teste do Lambda é carregada, ela aparece automaticamente no Visual Studio. 7. Repita as etapas de 1 a 6 para os seguintes projetos: • AWS.APG.CARSES.CommandDeleteLambda • AWS.APG.CARSES.CommandUpdateLambda • AWS.APG.CARSES.CommandAddRewardLambda • AWS.APG.CARSES.CommandRedeemRewardLambda • AWS.APG.CARSES.QueryCustomerListLambda • AWS.APG.CARSES.QueryRewqardLambda	

Tarefa	Descrição	Habilidades necessárias
Verifique o upload da função.	(Opcional) Você pode verificar se a função foi carregada com sucesso navegando até o AWS Explorer e expandindo o AWS Lambda. Para abrir a janela de teste, escolha a função do Lambda (clique duas vezes).	Desenvolvedor de aplicativos, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Testar a função do Lambda.	1. Insira os dados da solicitação ou copie um exemplo de dados de solicitação dos Dados de teste na seção Informações adicionais. Certifique-se de selecionar dados para a função que você está testando. 2. Para executar o teste, escolha Invoke (Invocar). A resposta e quaisquer erros são exibidos na caixa de texto Resposta, e os registros são mostrados na caixa de texto Registros ou em CloudWatch Registros. 3. Para verificar os dados, no AWS Explorer, escolha a tabela do DynamoDB (clique duas vezes). Todos os projetos Lambda do CQRS são encontrados nas pastas de soluções `CQRS AWS Serverless\CQRS\Command Microservice` e `CQRS AWS Serverless\CQRS\Command Microservice`. Para o diretório da solução e os projetos, consulte Diretório de código-fonte na seção Informações adicionais.	Desenvolvedor de aplicativos, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Publique as funções restantes.	Repita as etapas anteriores para os seguintes projetos: • AWS.APG.CARSES. CommandDeleteLambda • AWS.APG.CARSES. CommandUpdateLambda • AWS.APG.CARSES. CommandAddRewardLa mbda • AWS.APG.CARSES. CommandRedeemRewar dLambda • AWS.APG.CARSES. QueryCustomerListLambda • AWS.APG.CARSES. QueryRewqardLambda	Desenvolvedor de aplicativos, DevOps engenheiro

Configure a função do Lambda como um receptor de evento

Tarefa	Descrição	Habilidades necessárias
Publique os manipuladores de eventos Cliente and Recompensa do Lambda.	Para publicar cada manipulad or de eventos, siga as etapas do épico anterior. Os projetos estão sob as pastas de soluções `CQRS AWS Serverless\Event Source\Customer Event` e `CQRS AWS Serverles s\Event Source\Re ward Event` . Para obter mais informações, consulte	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	Diretório de código-fonte na seção Informações adicionais.	

Tarefa	Descrição	Habilidades necessárias
Anexe o receptor de eventos Lambda de fornecimento de eventos.	1. Faça login no Console de Gerenciamento da AWS usando a mesma conta que você usa ao publicar os projetos Lambda. 2. Para a região, selecione Leste dos EUA 1 ou a região em que você implantou as funções do Lambda no épico anterior. 3. Navegue até o serviço Lambda. 4. Selecionar a `EventSourceCustomer` função do Lambda 5. Escolha Add trigger (Adicionar gatilho). 6. Na lista suspensa Configuração do gatilho, selecione DynamoDB. 7. Na lista suspensa da tabela do DynamoDB, selecione. cqrses-customer-cmd 8. Na lista suspensa Iniciando a posição selecione Horizonte de corte. Horizonte de corte significa que o gatilho do DynamoDB começará a ler no último registro do fluxo (não cortado), que é o registro mais antigo no fragmento.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	9. Marque a caixa de seleção Enable trigger (Habilitar gatilho). 10. Mantenha os padrões de valores para os campos restantes e escolha Upload (Carregar). Depois que o receptor for anexado com sucesso à tabela do DynamoDB, ele será exibido na página do designer do Lambda.	
Publique e anexe a EventSourceReward função Lambda.	Para publicar e anexar a função `EventSourceReward` Lambda, repita as etapas nas duas histórias anteriores, selecionando na lista suspensa cqrses-reward-cmdda tabela do DynamoDB.	Desenvolvedor de aplicativos

Teste e valide os fluxos do DynamoDB e o gatilho do Lambda

Tarefa	Descrição	Habilidades necessárias
Teste o fluxo e o acionador do Lambda.	1. No Visual Studio, navegue até o AWS Explorer. 2. Expanda o AWS Lambda e escolha a CommandRedeemRewardfunção (clique duas vezes). Na janela de função que se abre, você pode testar a função.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	3. Na caixa de texto Solicitação, insira os dados da solicitação no formato JavaScript Object Notation (JSON). Para ver um exemplo de solicitação, consulte Dados de teste na seção Informações adicionais. 4. Escolha Invocar o .	
Valide usando a tabela de consulta de recompensas do DynamodDB.	1. Abra a cqrses-reward-querymesa. 2. Confira os pontos do cliente que resgatou a recompensa. Os pontos resgatados devem ser subtraídos do total de pontos agregados do cliente.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Valide usando CloudWatch Logs.	1. Navegue até Grupos de registros CloudWatch e escolha. 2. O grupo/aws/lambda/EventSourceRewardlog contém os registros do `EventSourceReward` acionador. Todas as chamadas do Lambda são registradas, incluindo as mensagens que você inseriu em `context.Logger.LogLine` e `Console.Writeline` no código do Lambda.	Desenvolvedor de aplicativos
Valide o EventSourceCustomer gatilho.	Para validar o `EventSourceCustomer` gatilho, repita as etapas desse épico, usando a respectiva tabela de clientes e CloudWatch registros do `EventSourceCustomer` gatilho.	Desenvolvedor de aplicativos

Recursos relacionados

Referências

- Downloads do Visual Studio 2019 Community Edition
- Download do AWS Toolkit for Visual Studio
- Guia do usuário do AWS Toolkit for Visual Studio
- Tecnologia sem servidor na AWS
- Casos de uso e padrões de design do DynamoDB

- Martin Fowler CQRS
- Fornecimento de eventos de Martin Fowler

Vídeos

- Demo do AWS Toolkit for Visual Studio
- Como faço para criar um ID de chave de acesso para um novo usuário do IAM?

Mais informações

CQRS e fornecimento de eventos

CQRS

O padrão CQRS separa um único modelo de operações conceituais, como um único modelo CRUD (criar, ler, atualizar, excluir) de objeto de acesso a dados, em modelos de operações de comando e consulta. O modelo de comando se refere a qualquer operação, como criar, atualizar ou excluir, que altera o estado. O modelo de consulta se refere a qualquer operação que retorna um valor.

1. O modelo Cliente CRUD inclui as seguintes interfaces:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`

À medida que seus requisitos se tornam mais complexos, você pode abandonar essa abordagem de modelo único. O CQRS usa um modelo de comando e um modelo de consulta para separar a responsabilidade pela gravação e leitura de dados. Dessa forma, os dados podem ser mantidos e gerenciados de forma independente. Com uma separação clara de responsabilidades, os

aprimoramentos em cada modelo não afetam o outro. Essa separação melhora a manutenção e o desempenho e reduz a complexidade do aplicativo à medida que ele cresce.

1. Interfaces no modelo Comando do cliente:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
2. Interfaces no modelo Consulta do cliente:
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`
   - `GetMonthlyStatement()`

Por exemplo de código, consulte Diretório de código-fonte.

O padrão CQRS então separa o banco de dados. Essa dissociação leva à total independência de cada serviço, que é o principal ingrediente da arquitetura de microsserviços.

Usando o CQRS na Nuvem AWS, você pode otimizar ainda mais cada serviço. Por exemplo, você pode definir configurações de computação diferentes ou escolher entre um microsserviço com tecnologia sem servidor ou baseado em contêiner. Você pode substituir seu armazenamento em cache local pela Amazon. ElastiCache Se você tiver um sistema de publicação e assinatura de mensagens on-premises, você pode substituí-lo pelo Amazon Simple Notification Service (Amazon SNS). Além disso, você pode aproveitar os pay-as-you-go preços e a grande variedade de serviços da AWS que você paga somente pelo que usa.

O CQRS inclui os seguintes benefícios:

- Escalabilidade independente: cada modelo pode ter sua estratégia de escalabilidade ajustada para atender aos requisitos e à demanda do serviço. Semelhante aos aplicativos de alto desempenho, a separação de leitura e gravação permite que o modelo seja dimensionado de forma independente

para atender a cada demanda. Você também pode adicionar ou reduzir recursos computacionais para atender à demanda de escalabilidade de um modelo sem afetar o outro.

- Manutenção independente: a separação dos modelos de consulta e comando melhora a capacidade de manutenção dos modelos. Você pode fazer alterações e aprimoramentos no código de um modelo sem afetar o outro.
- Segurança: é mais fácil aplicar as permissões e políticas a modelos separados para leitura e gravação.
- Leituras otimizadas: você pode definir um esquema otimizado para consultas. Por exemplo, você pode definir um esquema para os dados agregados e um esquema separado para as tabelas de fatos.
- Integração: o CQRS se encaixa bem com modelos de programação baseados em eventos.
- Complexidade gerenciada: a separação em modelos de consulta e comando é adequada para domínios complexos.

Ao usar o CQRS, tenha em mente as seguintes advertências:

- O padrão CQRS se aplica somente a uma parte específica de um aplicativo e não a todo o aplicativo. Se implementado em um domínio que não se encaixa no padrão, ele pode reduzir a produtividade, aumentar o risco e introduzir complexidade.
- O padrão funciona melhor para modelos usados com frequência que têm operações de leitura e gravação desequilibradas.
- Para aplicativos que exigem muita leitura, como relatórios grandes que demoram para serem processados, o CQRS oferece a opção de selecionar o banco de dados correto e criar um esquema para armazenar seus dados agregados. Isso melhora o tempo de resposta da leitura e visualização do relatório processando os dados do relatório apenas uma vez e despejando-os na tabela agregada.
- Para aplicativos com muita gravação, você pode configurar o banco de dados para operações de gravação e permitir que o microsserviço de comando seja escalado de forma independente quando a demanda por gravação aumentar. Para ver exemplos, consulte os microsserviços `AWS.APG.CQRSES.CommandRedeemRewardLambda` e `AWS.APG.CQRSES.CommandAddRewardLambda`.

Origens de eventos

A próxima etapa é usar o fornecimento de eventos para sincronizar o banco de dados de consultas quando um comando é executado. Por exemplo, considere os seguintes eventos:

- É adicionado um ponto de recompensa do cliente que exige que os pontos de recompensa totais ou agregados do cliente no banco de dados de consulta sejam atualizados.
- O sobrenome do cliente é atualizado no banco de dados de comandos, o que exige que as informações do cliente substituto no banco de dados de consulta sejam atualizadas.

No modelo CRUD tradicional, você garante a consistência dos dados bloqueando os dados até que a transação seja concluída. No fornecimento de eventos, os dados são sincronizados por meio da publicação de uma série de eventos que serão consumidos por um assinante para atualizar seus respectivos dados.

O padrão de fornecimento de eventos garante e registra uma série completa de ações realizadas nos dados e os publica por meio de uma sequência de eventos. Esses eventos representam um conjunto de alterações nos dados que os assinantes desse evento devem processar para manter seus registros atualizados. Esses eventos são consumidos pelo assinante, sincronizando os dados no banco de dados do assinante. Nesse caso, esse é o banco de dados de consultas.

O diagrama a seguir mostra o fornecimento de eventos usado com o CQRS na AWS.

1. As funções de comando do Lambda realizam operações de gravação, como criar, atualizar ou excluir, no banco de dados.
2. As funções de consulta do Lambda realizam operações de leitura, como obter ou selecionar, no banco de dados.
3. Essa função do Lambda processa os fluxos do DynamoDB do banco de dados Comando e atualiza o banco de dados Consulta para as alterações. Você também pode usar essa função para publicar uma mensagem no Amazon SNS para que seus assinantes possam processar os dados.
4. (Opcional) O assinante do evento Lambda processa a mensagem publicada pelo Amazon SNS e atualiza o banco de dados Consulta.
5. (Opcional) O Amazon SNS envia uma notificação por e-mail sobre a operação de gravação.

Na AWS, o banco de dados de consultas pode ser sincronizado pelo DynamoDB Streams. O DynamoDB captura uma sequência em ordem temporal de modificações em nível de item em uma

tabela do DynamoDB em tempo quase real e armazena de forma durável as informações em 24 horas.

A ativação do DynamoDB Streams permite que o banco de dados publique uma sequência de eventos que possibilita o padrão de fornecimento de eventos. O padrão de fornecimento de eventos adiciona o assinante do evento. O aplicativo de assinante do evento consome o evento e o processa de acordo com a responsabilidade do assinante. No diagrama anterior, o assinante do evento envia as alterações para o banco de dados do Query DynamoDB para manter os dados sincronizados. O uso do Amazon SNS, do agente de mensagens e do aplicativo de assinante de eventos mantém a arquitetura desacoplada.

O fornecimento de eventos inclui os seguintes benefícios:

- Consistência para dados transacionais
- Uma trilha de auditoria confiável e um histórico das ações, que podem ser usados para monitorar as ações realizadas nos dados
- Permite que aplicativos distribuídos, como microsserviços, sincronizem seus dados em todo o ambiente
- Publicação confiável de eventos sempre que o estado mudar
- Reconstruindo ou reproduzindo estados passados
- Entidades fracamente acopladas que trocam eventos para migração de um aplicativo monolítico para microsserviços
- Redução de conflitos causados por atualizações simultâneas; o fornecimento de eventos evita a necessidade de atualizar objetos diretamente no armazenamento de dados
- Flexibilidade e extensibilidade ao desacoplar a tarefa e o evento
- Atualizações externas do sistema
- Gerenciamento de várias tarefas em um único evento

Ao usar o fornecimento de eventos, lembre-se das seguintes ressalvas:

- Como há algum atraso na atualização dos dados entre os bancos de dados dos assinantes de origem, a única maneira de desfazer uma alteração é adicionar um evento compensador ao armazenamento de eventos.
- A implementação do sourcing de eventos tem uma curva de aprendizado devido ao seu estilo diferente de programação.

Dados de teste

Use os dados de teste a seguir para testar a função do Lambda após a implantação bem-sucedida.

CommandCreate Cliente

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Done",  "CompanyName":"AnyCompany",
 "Address": "USA",  "VIP":true }
```

CommandUpdate Cliente

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Doe",  "CompanyName":"Example Corp.",
 "Address": "Seattle, USA",  "VIP":true }
```

CommandDelete Cliente

Insira a ID do cliente como dados da solicitação. Por exemplo, se a ID do cliente for 151, insira 151 como dados da solicitação.

```
151
```

QueryCustomerList

Isso está branco. Quando for invocado, ele retornará todos os clientes.

CommandAddReward

Isso adicionará 40 pontos ao cliente com ID 1 (Richard).

```
{
  "Id":10101,
  "CustomerId":1,
  "Points":40
}
```

CommandRedeemReward

Isso deduzirá 15 pontos para o cliente com ID 1 (Richard).

```
{
  "Id":10110,
  "CustomerId":1,
```

```
  "Points":15
}
```

QueryReward

Insira o ID do cliente. Por exemplo, insira 1 para Richard, 2 para Arnav e 3 para Shirley.

```
2
```

Diretório de código-fonte

Use a tabela a seguir como guia para a estrutura de diretórios da solução Visual Studio.

Diretório de soluções de amostra de código on-premises do CQRS

Modelo CRUD do cliente

Exemplo do código on-premises CQRS\CRUD Model\Projeto AWS.APG.CQRSES.DAL

Versão CQRS do modelo Customer CRUD

- Comando do cliente: projeto `CQRS On-Premises Code Sample\CQRS Model\Command Microservice\AWS.APG.CQRSES.Command`
- Consulta do cliente: projeto `CQRS On-Premises Code Sample\CQRS Model\Query Microservice\AWS.APG.CQRSES.Query`

Microsserviços de comando e consulta

O microsserviço de comando está na pasta da solução `CQRS On-Premises Code Sample\CQRS Model\Command Microservice`:

- O projeto `AWS.APG.CQRSES.CommandMicroservice` ASP.NET Core API atua como o ponto de entrada onde os consumidores interagem com o serviço.
- O projeto `AWS.APG.CQRSES.Command` .NET Core é um objeto que hospeda objetos e interfaces relacionados a comandos.

O microsserviço de consulta está na pasta da solução `CQRS On-Premises Code Sample\CQRS Model\Query Microservice`:

- O projeto `AWS.APG.CQRSES.QueryMicroservice` ASP.NET Core API atua como o ponto de entrada onde os consumidores interagem com o serviço.
- O projeto `AWS.APG.CQRSES.Query` .NET Core é um objeto que hospeda objetos e interfaces relacionados a consultas.

Diretório de soluções de código da tecnologia sem servidor CQRS AWS

Esse código é a versão da AWS do código on-premises usando os serviços com tecnologia sem servidor da AWS.

Em C# .NET Core, cada função do Lambda é representada por um projeto do.NET Core. No código de exemplo desse padrão, há um projeto separado para cada interface nos modelos de comando e consulta.

CQRS usando os serviços da AWS

Você pode encontrar o diretório raiz da solução para o CQRS usando os serviços com tecnologia sem servidor da AWS na pasta `CQRS AWS Serverless\CQRS`. O exemplo inclui dois modelos: Cliente e Recompensa.

As funções de comando do Lambda para Cliente e Recompensa estão nas pastas `CQRS\Command Microservice\Customer` e `CQRS\Command Microservice\Reward`. Eles contêm os seguintes projetos Lambda:

- Comando do cliente: `CommandCreateLambda`, `CommandDeleteLambda`, e `CommandUpdateLambda`
- Comando de recompensa: `CommandAddRewardLambda` e `CommandRedeemRewardLambda`

As funções de consulta do Lambda para Customer e Reward são encontradas nas pastas `CQRS\Query Microservice\Customer` e `CQRS\QueryMicroservice\Reward`. Eles contêm os projetos Lambda `QueryCustomerListLambda` e `QueryRewardLambda`.

Projeto de teste CQRS

O projeto de teste está na pasta `CQRS\Tests`. Este projeto contém um script de teste para automatizar o teste das funções do Lambda do CQRS.

Fornecimento de eventos usando serviços da AWS

Os seguintes manipuladores de eventos do Lambda são iniciados pelos fluxos Cliente e Recompensa do DynamoDB para processar e sincronizar os dados nas tabelas de consulta.

- A função do Lambda `EventSourceCustomer` é mapeada para a tabela Cliente (`cqrses-customer-cmd`) do fluxo do DynamoDB.
- A função do Lambda `EventSourceReward` é mapeada para a tabela Recompensa (`cqrses-reward-cmd`) do fluxo do DynamoDB.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Mais padrões

- Acesse aplicativos de contêineres de forma privada no Amazon EKS usando a AWS PrivateLink e um Network Load Balancer
- Automatizar a adição ou atualização de entradas de registro do Windows usando o AWS Systems Manager
- Automatize o failover e o failback entre regiões usando o DR Orchestrator Framework
- Compilar e implantar automaticamente uma aplicação em Java no Amazon EKS usando um pipeline de CI/CD
- Compile automaticamente pipelines de CI/CD e clusters do Amazon ECS para microsserviços usando o AWS CDK
- Faça backup e arquive dados de mainframe no Amazon S3 usando o BMC AMI Cloud Data
- Crie um PAC de servidor corporativo da Micro Focus com o Amazon EC2 Auto Scaling e o Systems Manager
- Crie uma malha de dados corporativa com a Amazon DataZone, AWS CDK, e AWS CloudFormation
- Reúna os serviços da AWS usando uma abordagem de tecnologia sem servidor
- Containerize workloads de mainframe que foram modernizadas pela Blu Age
- Implemente continuamente um aplicativo web moderno do AWS Amplify a partir de um repositório da AWS CodeCommit
- Converta e descompacte dados EBCDIC em ASCII na AWS usando Python
- Converta arquivos de dados de mainframe com layouts de registro complexos usando o Micro Focus
- Crie um pipeline e uma AMI usando CodePipeline um HashiCorp Packer
- Crie um pipeline e implante atualizações de artefatos em instâncias locais usando EC2 CodePipeline
- Crie um portal para microfrontends usando Angular e AWS Amplify Module Federation
- Implantar e depure clusters do Amazon EKS
- Implantar contêineres usando o Elastic Beanstalk
- Emule o Oracle DR usando um banco de dados global Aurora compatível com PostgreSQL
- Gere insights de dados usando o AWS Mainframe Modernization e o Amazon Q em QuickSight

- Gere insights de dados do Db2 z/OS usando o AWS Mainframe Modernization Amazon Q em QuickSight
- Identifique automaticamente imagens de contêineres duplicadas ao migrar para um repositório Amazon ECR
- Implemente o controle de versão de API baseado em caminhos usando domínios personalizados no Amazon API Gateway
- Migre incrementalmente do Amazon RDS para Oracle para o Amazon RDS para PostgreSQL usando o Oracle SQL Developer e o AWS SCT
- Integre o controlador universal Stonebranch com o AWS Mainframe Modernization
- Gerencie produtos do AWS Service Catalog em várias contas e regiões da AWS
- Migre uma conta membro da AWS do AWS Organizations para o AWS Control Tower
- Migre e replique arquivos VSAM para o Amazon RDS ou o Amazon MSK usando o Connect da Precisely
- Migre do SAP ASE para o Amazon RDS para SQL Server usando o AWS DMS
- Migre tabelas externas da Oracle para a compatibilidade com o Amazon Aurora PostgreSQL
- Modernize o aplicativo de CardDemo mainframe usando AWS Transform
- Modernize as cargas de trabalho de impressão em lote do mainframe AWS usando o Rocket Enterprise Server e o LRS VPSX/MFI
- Modernize as workloads de impressão on-line de mainframe na AWS usando o Micro Focus Enterprise Server e o LRS VPSX/MFI
- Modernize o gerenciamento de saída do mainframe AWS usando o Rocket Enterprise Server e o LRS X PageCenter
- Mova arquivos de mainframe diretamente para o Amazon S3 usando o Transfer Family
- Otimizar imagens do Docker geradas pelo AWS App2Container
- Otimize implantações sem servidor de várias contas usando os fluxos de trabalho e Actions AWS CDK GitHub
- Automatize implantações azul/verdes dos bancos de dados globais Amazon Aurora usando princípios de IaC
- Replique bancos de dados de mainframe para AWS usando o Precisely Connect
- Execute tarefas do Amazon ECS na Amazon WorkSpaces com o Amazon ECS Anywhere
- Envie dados de telemetria de AWS Lambda para OpenSearch para análise e visualização em tempo real

- Configurar um repositório de chart do Helm v3 no Amazon S3
- Configure a detecção de AWS CloudFormation desvios em uma organização multirregional e com várias contas
- Estruture um projeto Python em arquitetura hexagonal usando o AWS Lambda
- Teste a AWS infraestrutura usando LocalStack e Terraform Tests
- Atualize os clusters do SAP Pacemaker de para ENSA1 ENSA2
- Use o Amazon Q Developer como assistente de codificação para aumentar sua produtividade
- Valide o código do Account Factory for Terraform (AFT) localmente

Mainframes

Tópicos

- Acesse Serviços da AWS a partir do IBM z/OS instalando o AWS CLI
- Faça backup e arquive dados de mainframe no Amazon S3 usando o BMC AMI Cloud Data
- Crie programas COBOL Db2 usando e AWS Mainframe ModernizationAWS CodeBuild
- Crie um PAC de servidor corporativo da Micro Focus com o Amazon EC2 Auto Scaling e o Systems Manager
- Crie um visualizador avançado de arquivos de mainframe na Nuvem AWS
- Containerize workloads de mainframe que foram modernizadas pela Blu Age
- Converta e descompacte dados EBCDIC em ASCII na AWS usando Python
- Converta arquivos de mainframe do formato EBCDIC para o formato ASCII delimitado por caracteres no Amazon S3 usando o AWS Lambda
- Converta arquivos de dados de mainframe com layouts de registro complexos usando o Micro Focus
- Implante um ambiente para aplicativos Blu Age conteinerizados usando o Terraform
- Gere insights de dados do Db2 z/OS usando o AWS Mainframe Modernization Amazon Q em QuickSight
- Gere insights de dados usando o AWS Mainframe Modernization e o Amazon Q em QuickSight
- Integre o controlador universal Stonebranch com o AWS Mainframe Modernization
- Migre e replique arquivos VSAM para o Amazon RDS ou o Amazon MSK usando o Connect da Precisely
- Modernize o gerenciamento de saída do mainframe AWS usando o Rocket Enterprise Server e o LRS X PageCenter
- Modernize o aplicativo de CardDemo mainframe usando AWS Transform
- Modernize as cargas de trabalho de impressão em lote do mainframe AWS usando o Rocket Enterprise Server e o LRS VPSX/MFI
- Modernização do mainframe: DevOps iniciada AWS com o Rocket Software Enterprise Suite
- Modernize as workloads de impressão on-line de mainframe na AWS usando o Micro Focus Enterprise Server e o LRS VPSX/MFI
- Mova arquivos de mainframe diretamente para o Amazon S3 usando o Transfer Family

- Proteja e simplifique o acesso de usuários em um banco de dados de federação Db2 na AWS usando contextos confiáveis
- Transferir dados do Db2 z/OS em grande escala para o Amazon S3 em arquivos CSV
- Mais padrões

Acesse Serviços da AWS a partir do IBM z/OS instalando o AWS CLI

Criado por Souma Ghosh (AWS), Phil de Valence (AWS) e Paulo Vitor Pereira (AWS)

Resumo

O AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto para gerenciar vários AWS serviços usando comandos em um shell de linha de comando. Com uma configuração mínima, você pode executar comandos a partir de sessões de linha de comando, como o prompt de comando, o terminal e o shell bash, para implementar uma funcionalidade equivalente à fornecida pelo navegador AWS Management Console.

Todas as funções de administração, gerenciamento e acesso da AWS infraestrutura como serviço (IaaS) no AWS Management Console estão disponíveis na AWS API e. AWS CLI Você pode instalá-lo AWS CLI em um mainframe IBM z/OS para acessar, gerenciar e interagir diretamente a partir do z/OS Serviços da AWS . AWS CLI Isso permite que usuários e aplicativos executem várias tarefas, como:

- Transferência de arquivos ou conjuntos de dados entre o z/OS e o armazenamento de objetos do Amazon Simple Storage Service (Amazon S3) e visualização do conteúdo dos buckets
- Iniciar e interromper AWS recursos diferentes; por exemplo, iniciar um trabalho em lotes em um AWS Mainframe Modernization ambiente
- Chamando uma AWS Lambda função para implementar uma lógica comercial comum
- Integração com inteligência artificial, aprendizado de máquina (IA/ML) e serviços de análise

Esse padrão descreve como instalar, configurar e usar o AWS CLI no z/OS. Você pode instalá-lo globalmente, para que esteja disponível para todos os usuários do z/OS ou em nível de usuário. O padrão também detalha como usar o AWS CLI em uma sessão de linha de comando interativa do z/OS Unix System Services (USS) ou como um trabalho em lotes.

Pré-requisitos e limitações

Pré-requisitos

- Comunicação de rede do z/OS para AWS

  Por padrão, o AWS CLI envia solicitações Serviços da AWS usando HTTPS na porta TCP 443. Para usar o AWS CLI com sucesso, você deve ser capaz de fazer conexões de saída na porta

TCP 443. Você pode usar qualquer um dos seguintes comandos do z/OS USS (alguns deles podem não estar instalados em seu ambiente) para testar a conectividade de rede do z/OS para: AWS

```
ping amazonaws.com
dig amazonaws.com
traceroute amazonaws.com
curl -k https://docs.aws.amazon.com/cli/v1/userguide/cli-chap-welcome.html
```

- AWS credenciais

  Para se comunicar com Nuvem AWS serviços do z/OS, é AWS CLI necessário configurar algumas credenciais com privilégios para acessar o destino. Conta da AWS Para comandos programáticos AWS, você pode usar teclas de acesso, que consistem em um ID de chave de acesso e uma chave de acesso secreta. Se você não tiver chaves de acesso, poderá criá-las usando o AWS Management Console. Como prática recomendada, não use as chaves de acesso do usuário Conta da AWS raiz em nenhuma tarefa, a menos que o usuário raiz seja necessário. Em vez disso, crie um novo usuário administrador do IAM e prepare-se para obter permissões com privilégios mínimos para configurar o usuário com chaves de acesso. Depois de criar o usuário, você pode criar uma ID de chave de acesso e uma chave de acesso secreta para esse usuário.

  > **Warning**
  >
  > AWS Identity and Access Management Os usuários (IAM) têm credenciais de longo prazo que apresentam um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

- IBM Python para z/OS

  AWS CLI Isso requer Python 3.8 ou posterior. A IBM permitiu que o Python fosse executado no z/OS com o IBM Open Enterprise Python for z/OS. O IBM Open Enterprise Python está disponível gratuitamente por meio do Shopz SMP/E, ou você pode baixar o arquivo PAX no site da IBM. Para obter instruções, consulte a documentação de instalação e configuração do IBM Open Enterprise Python for z/OS.

Limitações

- As instruções de instalação fornecidas nesse padrão são aplicáveis somente àAWS CLI versão 1. A versão mais recente do AWS CLI é a versão 2. No entanto, esse padrão usa a versão mais antiga porque os métodos de instalação são diferentes para a versão 2 e os executáveis binários disponíveis para a versão 2 não são compatíveis com o sistema z/OS.

Versões do produto

- AWS CLI versão 1
- Python 3.8 ou posterior

Arquitetura

Pilha de tecnologia

- Mainframe executando z/OS
- Serviços do Sistema UNIX (USS) do Mainframe z/OS
- Mainframe Open MVS (OMVS) — interface de comando do ambiente shell z/OS UNIX
- Disco de mainframe, como um dispositivo de armazenamento de acesso direto (DASD - direct-access storage device)
- AWS CLI

Arquitetura de destino

O diagrama a seguir mostra uma AWS CLI implantação no IBM z/OS. Você pode invocar o a AWS CLI partir de uma sessão de usuário interativa, como SSH e sessões de telnet. Você também pode invocá-la a partir de um trabalho em lotes usando a linguagem de controle de tarefas (JCL) ou de qualquer programa que possa chamar um comando shell do z/OS Unix.

Ele AWS CLI se comunica com os AWS service (Serviço da AWS) endpoints por meio de uma rede TCP/IP. Essa conexão de rede pode ocorrer pela Internet ou por meio de uma AWS Direct Connect conexão privada do data center do cliente com os data Nuvem AWS centers. A comunicação é autenticada com AWS credenciais e criptografada.

Automação e escala

Você pode explorar os recursos de um AWS service (Serviço da AWS) com o AWS CLI e desenvolver scripts de shell do USS para gerenciar seus AWS recursos a partir do z/OS. Você também pode executar AWS CLI comandos e scripts de shell a partir do ambiente em lotes z/OS e automatizar trabalhos em lotes para execução em um agendamento específico por meio da integração com agendadores de mainframe. AWS CLI comandos ou scripts podem ser codificados dentro de parâmetros (PARMs) e procedimentos (PROCs) e podem ser escalados seguindo a abordagem padrão de chamar o PARM ou o PROC a partir de diferentes trabalhos em lotes com parâmetros diferentes.

Ferramentas

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.

Práticas recomendadas

- Por motivos de segurança, restrinja as permissões de acesso ao diretório do USS onde os detalhes da chave de AWS acesso estão armazenados. Permita o acesso somente aos usuários ou programas que usam AWS CLI o.
- Não use as chaves de acesso do usuário Conta da AWS root para nenhuma tarefa. Em vez disso, crie um novo usuário administrador do IAM para você e configure-o com chaves de acesso.

> **Warning**
>
> Os usuários do IAM têm credenciais de longo prazo que apresentam um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

Épicos

Instale AWS CLI a versão 1 no z/OS USS

Tarefa	Descrição	Habilidades necessárias
Instale o Python 3.8 ou posterior.	1. Faça login na interface do prompt de comando do z/OS USS usando um destes métodos: • Use um comando OMVS da Opção de Compartilhamento de Tempo (TSO) do painel Interactive System Productivity Facility (ISPF) ou • Use SSH ou telnet para se conectar ao IP da partição lógica do mainframe (LPAR). Esse padrão pressupõe que `cliuser` seja o ID de usuário usado para fazer login no ambiente USS e `/u/cliuser/` seja o diretório inicial do usuário. Você pode definir o diretório inicial do usuário de forma diferente em seu ambiente z/OS, dependendo dos requisitos de instalação. 2. Siga o guia de instalação do IBM Open Enterprise Python for z/OS para	Administrador de mainframe z/OS

Tarefa	Descrição	Habilidades necessárias
	instalar o Python 3.8 ou posterior, caso ainda não esteja instalado.	

Tarefa	Descrição	Habilidades necessárias

Defina as variáveis de ambiente do USS.	Adicione variáveis de ambiente ao perfil. Você pode adicioná-los ao `/u/cliuser/.profile` arquivo de um usuário individual (`cliuser`) ou ao `/etc/profile` arquivo de todos os usuários.
	
	Note
	Esse padrão pressupõe que o Python tenha sido instalado no `/u/awscli/python` diretório. Se o diretório de instalação for diferente, atualize o código adequadamente.
	
	`# Python configuration`
	`export BPXKAUTOCVT='ON'`
	`export CEERUNOPTS='FILETAG(AUTOCVT,AUTOTAG) POSIX(ON)'`
	`export TAGREDIR_ERR=txt`
	`export TAGREDIR_IN=txt`
	`export TAGREDIR_OUT=txt`
	
	`# AWS CLI configuration`
		Administrador de mainframe z/OS

Tarefa	Descrição	Habilidades necessárias
	`export PATH=/u/cliuser/python/bin:$PATH` `export PYTHONPATH=/u/cliuser/python:$PYTHONPATH`	
Teste a instalação do Python.	Execute o comando python: `python --version` A saída deve confirmar que você tem o Python 3.8 ou posterior instalado corretamente.	Administrador de mainframe z/OS

Tarefa	Descrição	Habilidades necessárias

Verifique ou instale o pip.	1. O comando pip geralmente é instalado automaticamente quando você instala o Python a partir do site da IBM. Para verificar, execute o comando:
	`pip —-version`
	Se o pip estiver instalado, esse comando deverá mostrar a versão instalada.
	2. Se o comando pip não for encontrado, instale o pip executando o seguinte comando:
	`python -m ensurepip --upgrade`
	Para obter mais opções de instalação, consulte a documentação do pip.
		Administrador de mainframe z/OS

Tarefa	Descrição	Habilidades necessárias

Instale AWS CLI a versão 1.	1. Para instalar o AWS CLI, execute o comando:
	`python -m pip install awscli`
	A saída deve ser semelhante a esta.
	`Successfully installed PyYAML-6.0.1 awscli-1.32.23 botocore-1.34.23 colorama-0.4.4 docutils-0.16 jmespath-1.0.1 pyasn1-0.5.1 python-dateutil-2.8.2 rsa-4.7.2 s3transfer-0.10.0 urllib3-2.0.7`
	2. Altere a permissão do executável aws executando o comando a seguir. Certifique-se de atualizar o diretório de espaço reservado `<python_installation_dir>` com o caminho de instalação do Python.
	`chmod 744 <python_installation_dir>/bin/aws`
		Administrador de mainframe z/OS

Tarefa	Descrição	Habilidades necessárias

	3. Execute o comando a seguir para testar a AWS CLI instalação:
	`aws --version`
	A saída deve mostrar as versões do AWS CLI, Python e botocore, semelhantes às seguintes.
	`aws-cli/1.32.3`
	` Python/3.9.5`
	` OS/390/27.00`
	` botocore/1.34.3`	

Configurar o AWS CLI acesso a partir do z/OS

Tarefa	Descrição	Habilidades necessárias
Configure as chaves de AWS acesso, a região padrão e a saída.	A AWS CLI documentação descreve diferentes opções para configurar o AWS acesso. Você pode escolher uma configuração de acordo com os padrões da sua organização. Este exemplo usa a configuração de credenciais de curto prazo. 1. Configure o AWS CLI com o seguinte comando: `aws configure`	Administrador da AWS, administrador do Mainframe z/OS, desenvolvedor do Mainframe z/OS

Tarefa	Descrição	Habilidades necessárias

	2. Forneça os detalhes dos itens a seguir quando solicitado. Os valores da ID da chave de acesso e da chave de acesso secreta são das chaves que você obteve ao definir AWS as credenciais nas etapas de pré-requisitos.
	`AWS Access Key ID [None]: ASIAIOSFODNN7EXAMPLE`
	`AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
	`Default region name [None]: us-east-1`
	`Default output format [None]:`
	`aws configure set aws_session_token IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE`
	Essa configuração, incluindo as chaves de acesso, é armazenada na `/u/cliuser/.aws` pasta. Por motivos de segurança , restrinja essa pasta para permitir o acesso somente	

Tarefa	Descrição	Habilidades necessárias
	aos usuários ou programas que usam AWS CLI o.	
Teste AWS CLI o.	1. Execute o comando a seguir no prompt de comando para testar o AWS CLI com um comando simples: `aws s3 ls` A saída deve listar todos os buckets do S3 configurados Conta da AWS sem erros. 2. Siga as instruções nos próximos dois épicos para transferir dados do USS para o Amazon S3. É possível escolher apenas uma das duas opções: • Opção 1 (próximo épico): transferir interativamente um arquivo de valores separados por vírgula (CSV) EBCDIC para o Amazon S3 e consultar o arquivo no Amazon Athena. • Opção 2: Transferir um conjunto de dados EBCDIC de tamanho fixo para o Amazon S3 como um trabalho em lotes.	Administrador do Mainframe z/OS, desenvolvedor do Mainframe z/OS

Opção 1 – Transferir dados do USS para o Amazon S3 de forma interativa a partir de uma sessão do USS

Tarefa	Descrição	Habilidades necessárias
Baixe e transfira o arquivo CSV de amostra.	1. Faça o `sales-records.csv` download na seção Anexos. Esse arquivo fornece um exemplo de arquivo CSV com registros de vendas. 2. Transfira o arquivo para o z/OS USS. 3. Verifique se o `/u/cliuser/sales-records.csv` arquivo pode ser lido no formato EBCDIC no USS usando um editor de texto de sua escolha.	Desenvolvedor de aplicativos, desenvolvedor de Mainframe z/OS

Crie um bucket do S3 e faça o upload do arquivo CSV.	1. Crie um bucket do S3 para armazenar o arquivo CSV.
	`aws s3 mb s3://<s3_bucket_name>`
	onde `<s3_bucket_name>` está o nome exclusivo de um bucket; por exemplo:
	`aws s3 mb s3://DOC-EXAMPLE-BUCKET1`
	2. Faça upload do arquivo CSV do z/OS USS para o bucket do S3:
		Desenvolvedor de aplicativos, desenvolvedor de Mainframe z/OS

Tarefa	Descrição	Habilidades necessárias

	`aws s3 cp <csv_file _path> s3://<s3_ bucket_name>`
	
	Por exemplo:
	
	`aws s3 cp /u/cliuser/ sales-records.csv s3://DOC-EXAMPLE-B UCKET1`
	
	3. Liste o conteúdo do bucket do S3 e confirme se ele inclui o arquivo carregado:
	
	`aws s3 ls s3://<s3_ bucket_name>`
	
	Por exemplo:
	
	`aws s3 ls s3://DOC-EXAMPLE-BUCKET1`	

Tarefa	Descrição	Habilidades necessárias
Visualize o bucket do S3 e o arquivo carregado.	1. Faça login no AWS Management Console e abra o console do Amazon S3. 2. Navegue para ver o novo bucket do S3 e o objeto carregado. Para obter mais informações sobre o upload de objetos, consulte Introdução ao Amazon S3 na documentação do Amazon S3.	AWS geral

Tarefa	Descrição	Habilidades necessárias

Execute uma consulta SQL em uma tabela do Amazon Athena.	1. Abra o console do Amazon Athena.
	2. Crie uma nova tabela (por exemplo,`DOC-EXAMPLE-BUCKET`) usando os dados CSV do Amazon S3. Para obter mais informações, consulte Consultar o inventário do Amazon S3 com o Amazon Athena na documentação do Amazon S3.
	3. Execute a `SELECT` consulta na tabela para visualizar os dados.
	`SELECT * FROM <table_name>;`
	Por exemplo:
	`SELECT * FROM DOC-EXAMPLE-BUCKET;`
	A saída da consulta SQL exibirá o conteúdo do seu arquivo CSV.
		AWS geral, desenvolvedor de aplicativos

Opção 2 – Transferir dados do USS para o Amazon S3 usando JCL em lote

Tarefa	Descrição	Habilidades necessárias
Faça o upload do arquivo de amostra.	1. Faça o `sales-records-fixed.txt` download na seção Anexos. Esse é um arquivo de amostra com registros de vendas. Renomeie o arquivo de texto; por exemplo, para `USER.DATA.FIXED` . 2. Transfira o arquivo para o z/OS como um conjunto de dados com bloqueio fixo (FB), comprimento de registro de 256 registros (LRECL) e sequencial físico (PS). 3. Use o utilitário de lista de conjuntos de dados para verificar se o `USER.DATA.FIXED` conjunto de dados pode ser lido no formato EBCDIC na opção 3.4 do ISPF. Consulte a seção Informações adicionais para obter um exemplo de saída.	Desenvolvedor de mainframe z/OS
Crie JCL em lote.	Codifique o JCL em lote da seguinte forma para criar o bucket S3 de destino, fazer o upload do conjunto de dados e listar o conteúdo do bucket. Certifique-se de substituir o	Desenvolvedor de mainframe z/OS

Tarefa	Descrição	Habilidades necessárias

	nome do diretório, os nomes dos arquivos e o nome do bucket pelos seus próprios valores.
	
	`//AWSCLICP JOB`
	` ACTINFO1,'IBMUSER'`
	`,CLASS=A,MSGCLASS=`
	`H,MSGLEVEL=(1,1),`
	`// NOTIFY=&SYSUID,TIM`
	`E=1440`
	`//*--------------`
	`------------------`
	`------------------`
	`-------`
	`//* Sample job for AWS`
	` CLI`
	`//*--------------`
	`------------------`
	`------------------`
	`-------`
	`//USSCMD EXEC PGM=BPXBA`
	`TCH`
	`//STDERR  DD SYSOUT=*`
	`//STDOUT  DD SYSOUT=*`
	`//STDENV  DD *`
	` export PATH=/u/c`
	`liuser/python/bin:`
	`$PATH`
	`//STDPARM DD *`
	`SH`
	` export _BPXK_AUT`
	`OCVT=ON;`
	` aws s3 mb s3://DOC-`
	`EXAMPLE-BUCKET2;`
	` cp "//'USER.DATA.FIXE`
	`D'" /tmp/tmpfile;`
	` aws s3 cp /tmp/tmpf`
	`ile s3://DOC-EXAMPLE-`
	`BUCKET2/USER.DATA.F`
	`IXED;`	

Tarefa	Descrição	Habilidades necessárias
	`rm /tmp/tmpfile; aws s3 ls s3://DOC-EXAMPLE-BUCKET2; /*`	
Envie o trabalho JCL em lote.	1. Envie a tarefa JCL que você codificou na etapa anterior. 2. Verifique o status da tarefa no System Display and Search Facility (SDSF). Se for bem-sucedido, o trabalho deverá terminar com o código de retorno 0. 3. A saída padrão (STDOUT) do registro de tarefas mostra a criação bem-sucedida do bucket, o upload do conjunto de dados e a lista do conteúdo do bucket. Para ver um exemplo de ilustração de tela, consulte a seção Informações adicionais.	Desenvolvedor de mainframe z/OS

Tarefa	Descrição	Habilidades necessárias
Visualize o conjunto de dados carregado no bucket do S3.	1. Faça login no AWS Management Console e abra o console do Amazon S3. 2. Navegue para ver o arquivo carregado no bucket de teste. 3. Você pode processar ainda mais o `USER.DATA.FIXED` arquivo ou analisá-lo usando serviços de análise como o Amazon Redshift.	AWS geral

Recursos relacionados

- AWS CLI documentação da versão 1
- AWS Mainframe Modernization Referência de comandos da CLI
- AWS Mainframe Modernization

Mais informações

USER.DATA.FIXED na opção 3.4 do ISPF (utilitário de lista de conjuntos de dados)

SYSOUT do trabalho em lotes enviado

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Faça backup e arquive dados de mainframe no Amazon S3 usando o BMC AMI Cloud Data

Criado por Santosh Kumar Singh (AWS), Mikhael Liberman (software de mainframe Model9), Gilberto Biondo (AWS) e Maggie Li (AWS)

Resumo

Esse padrão demonstra como fazer backup e arquivar dados do mainframe diretamente no Amazon Simple Storage Service (Amazon S3) e, em seguida, recuperar e restaurar esses dados no mainframe usando o BMC AMI Cloud Data (anteriormente conhecido como Model9 Manager). Se você está procurando uma maneira de modernizar sua solução de backup e arquivamento como parte de um projeto de modernização do mainframe ou para atender aos requisitos de conformidade, esse padrão pode ajudar a atingir essas metas.

Normalmente, as organizações que executam os principais aplicativos de negócios em mainframes usam uma biblioteca virtual de fitas (VTL) para fazer backup de armazenamentos de dados, como arquivos e registros. Esse método pode ser caro porque consome MIPS faturáveis e os dados armazenados em fitas fora do mainframe estão inacessíveis. Para evitar esses problemas, você pode usar o BMC AMI Cloud Data para transferir dados operacionais e históricos do mainframe de forma rápida e econômica diretamente para o Amazon S3. Você pode usar o BMC AMI Cloud Data para fazer backup e arquivar dados por TCP/IP e, ao AWS mesmo tempo, aproveitar os mecanismos IBM z Integrated Information Processor (zIIP) para reduzir custos, paralelismo e tempos de transferência.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- BMC AMI Cloud Data com uma chave de licença válida
- Conectividade TCP/IP entre o mainframe e a AWS
- Uma função AWS Identity and Access Management (IAM) para acesso de leitura/gravação a um bucket do S3
- Acesso ao produto de segurança de mainframe (RACF) no local para executar processos do BMC AMI Cloud

- Um agente BMC AMI Cloud z/OS (Java versão 8 de 64 bits SR5 FP16 ou posterior) que tem portas de rede disponíveis, regras de firewall que permitem acesso aos buckets do S3 e um sistema de arquivos z/FS dedicado
- Requisitos atendidos para o servidor de gerenciamento BMC AMI Cloud

Limitações

- O BMC AMI Cloud Data armazena seus dados operacionais em um banco de dados PostgreSQL que é executado como um contêiner Docker na mesma instância do Amazon Elastic Compute Cloud (EC2Amazon) do servidor de gerenciamento. Atualmente, o Amazon Relational Database Service (Amazon RDS) não é suportado como back-end para BMC AMI Cloud Data. Para obter mais informações sobre as atualizações mais recentes do produto, consulte O que há de novo? na documentação da BMC.
- Esse padrão faz backup e arquiva somente os dados do mainframe z/OS. O BMC AMI Cloud Data faz backup e arquiva somente arquivos de mainframe.
- Esse padrão não converte dados em formatos abertos padrão, como JSON ou CSV. Use um serviço de transformação adicional, como o BMC AMI Cloud Analytics (anteriormente conhecido como Model9 Gravity) para converter os dados em formatos abertos padrão. Aplicativos nativos da nuvem e ferramentas de análise de dados podem acessar os dados depois que eles são gravados na nuvem.

Versões do produto

- BMC AMI Cloud Data versão 2.x

Arquitetura

Pilha de tecnologia de origem

- Mainframe executando z/OS
- Arquivos de mainframe, como conjuntos de dados e arquivos z/OS UNIX System Services (USS)
- Disco de mainframe, como um dispositivo de armazenamento de acesso direto (DASD - direct-access storage device)
- Fita de mainframe (biblioteca de fitas virtuais ou físicas)

Pilha de tecnologias de destino

- Amazon S3
- EC2 Instância da Amazon em uma nuvem privada virtual (VPC)
- AWS Direct Connect
- Amazon Elastic File System (Amazon EFS)

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura de referência em que os agentes do software BMC AMI Cloud Data em um mainframe conduzem os processos legados de backup e arquivamento de dados que armazenam os dados no Amazon S3.

O diagrama mostra o seguinte fluxo de trabalho:

1. Os agentes do software BMC AMI Cloud Data são executados em partições lógicas de mainframe (). LPARs Os agentes de software leem e gravam dados do mainframe do DASD ou da fita diretamente no Amazon S3 via TCP/IP.
2. AWS Direct Connect configura uma conexão física isolada entre a rede local e. AWS Para aumentar a segurança, use uma site-to-site VPN na parte superior AWS Direct Connect para criptografar dados em trânsito.
3. O bucket do S3 armazena arquivos do mainframe como dados de armazenamento de objetos, e os agentes do BMC AMI Cloud Data se comunicam diretamente com os buckets do S3. Os certificados são usados para criptografia HTTPS de todas as comunicações entre o agente e o Amazon S3. A criptografia de dados do Amazon S3 é usada para criptografar e proteger os dados em repouso.
4. Os servidores de gerenciamento de dados do BMC AMI Cloud são executados como contêineres Docker em EC2 instâncias. As instâncias se comunicam com agentes em execução no mainframe LPARs e nos buckets do S3.
5. O Amazon EFS é montado em EC2 instâncias ativas e passivas para compartilhar o armazenamento do Network File System (NFS). Isso é para garantir que os metadados relacionados a uma política criada no servidor de gerenciamento não sejam perdidos no caso de um failover. No caso de um failover do servidor ativo, o servidor passivo pode ser acessado sem perda de dados. Se o servidor passivo falhar, o servidor ativo poderá ser acessado sem perda de dados.

Ferramentas

Serviços da AWS

- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados no Nuvem AWS.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado em nuvem que ajuda você a armazenar, proteger e recuperar praticamente qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.
- AWS Direct Connectconecta sua rede interna a um AWS Direct Connect local por meio de um cabo de fibra óptica Ethernet padrão. Com essa conexão, você pode criar interfaces virtuais diretamente para AWS serviços públicos, ignorando os provedores de serviços de Internet em seu caminho de rede.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.

Ferramentas BMC

- O servidor de gerenciamento BMC AMI Cloud é um aplicativo de GUI que é executado como um contêiner Docker em uma Amazon Linux Amazon Machine Image (AMI) para Amazon. EC2 O servidor de gerenciamento fornece a funcionalidade para gerenciar as atividades do BMC AMI Cloud, como emissão de relatórios, criação e gerenciamento de políticas, execução de arquivos e realização de backups, recuperações e restaurações.
- O agente BMC AMI Cloud é executado em uma LPAR de mainframe local que lê e grava arquivos diretamente no armazenamento de objetos usando TCP/IP. Uma tarefa iniciada é executada em uma LPAR de mainframe e é responsável por ler e gravar dados de backup e arquivamento de e para o Amazon S3.
- A interface de linha de comando do BMC AMI Cloud Mainframe (M9CLI) fornece um conjunto de comandos para realizar ações do BMC AMI Cloud diretamente do TSO/E ou em operações em lote, sem a dependência do servidor de gerenciamento.

Épicos

Crie um bucket do S3 e uma política do IAM

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Crie um bucket S3 para armazenar os arquivos e volumes dos quais você deseja fazer backup e arquivar do seu ambiente de mainframe.	AWS geral
Crie uma política do IAM.	Todos os servidores e agentes de gerenciamento do BMC AMI Cloud exigem acesso ao bucket do S3 que você criou na etapa anterior. Para conceder o acesso necessário, crie a seguinte política do IAM: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Listfolder", "Action": [ "s3:ListBucket", "s3:GetBucketLocation", "s3:ListBucketVersions" ],`	AWS geral

Tarefa	Descrição	Habilidades necessárias
	"Effect": "Allow", "Resource": ["arn:aws:s3:::<Bucket Name>"] }, { "Sid": "Objectaccess", "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObjectAcl", "s3:GetObject", "s3:DeleteObjectVersion", "s3:DeleteObject", "s3:PutObjectAcl", "s3:GetObjectVersion"], "Resource": ["arn:aws:s3:::<Bucket Name>/*"] }] }	

Obtenha a licença do software BMC AMI Cloud e faça o download do software

Tarefa	Descrição	Habilidades necessárias
Obtenha uma licença do software BMC AMI Cloud.	Para obter uma chave de licença de software, entre em contato com a equipe do BMC AMI Cloud. A saída do comando `D M=CPU` z/OS é necessária para gerar uma licença.	Crie um lead
Baixe o software e a chave de licença do BMC AMI Cloud.	Obtenha os arquivos de instalação e a chave de licença seguindo as instruções na documentação da BMC.	Administrador de infraestrutura de mainframe

Instale o agente de software BMC AMI Cloud no mainframe

Tarefa	Descrição	Habilidades necessárias
Instale o agente de software BMC AMI Cloud.	1. Antes de iniciar o processo de instalação, verifique se os requisitos mínimos de software e hardware do agente foram atendidos. 2. Para instalar o agente, siga as instruções na documentação da BMC. 3. Depois que o agente começar a ser executado na LPAR do mainframe, verifique a mensagem `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` no spool.	Administrador de infraestrutura de mainframe

Tarefa	Descrição	Habilidades necessárias
	Verifique se a conectividade foi estabelecida com sucesso entre o agente e o bucket do S3 procurando a `Object store connectivity has been established successfully` mensagem no STDOUT do agente.	

Configurar um servidor de gerenciamento do BMC AMI Cloud em uma instância EC2

Tarefa	Descrição	Habilidades necessárias
Crie instâncias EC2 do Amazon Linux 2.	Execute duas instâncias do Amazon EC2 Linux 2 em diferentes zonas de disponibilidade seguindo as instruções da Etapa 1: Inicie uma instância na EC2 documentação da Amazon. A instância deve atender aos seguintes requisitos recomendados de hardware e software: • CPU – Mínimo de 4 núcleos • RAM - mínimo 8 GB • Unidade – 40 GB • EC2 Instância recomendada — C5.xlarge • SO – Linux	Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	• Software – Docker, unzip, VI/Vim • Largura de banda de rede — Mínimo de 1 GB Para obter mais informações, consulte a documentação da BMC.	
Criar um sistema de arquivos do Amazon EFS.	Crie um sistema de arquivos do Amazon EFS seguindo as instruções da Etapa 1: Crie seu sistema de arquivos do Amazon EFS na documenta ção do Amazon EFS. Ao criar o sistema de arquivos, faça o seguinte: • Escolha a classe de armazenamento padrão. • Escolha a mesma VPC que você usou para iniciar suas EC2 instâncias.	Administrador de nuvem, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

Instale o Docker e configure o servidor de gerenciamento.	Conecte-se às suas EC2 instâncias:
	
	Conecte-se às suas EC2 instâncias seguindo as instruções em Conecte-se à sua instância Linux na EC2 documentação da Amazon.
	
	Configure suas EC2 instâncias:
	
	Para cada EC2 instância, faça o seguinte:
	
	1. Para instalar o Docker, execute o comando:
	
	`sudo yum install docker`
	
	2. Para iniciar o Docker, execute o comando:
	
	`sudo service docker start`
	
	3. Para validar o status do Docker, execute o comando:
	
	`sudo service docker status`
	
	4. Na `/etc/selinux` pasta, altere o arquivo `config` para `SELINUX=permissive` .
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	5. Faça upload dos `VerificationScripts.zip` arquivos `model9-v2.x.y_build_build-id-server.zip` e (que você baixou anteriormente) em uma pasta temporária em uma das EC2 instâncias (por exemplo, na `/var/tmp` pasta da sua instância).
	6. Para ir até a `tmp` pasta, execute o comando:
	`cd/var/tmp`
	7. Para descompactar o script de verificação, execute o comando:
	`unzip VerificationScripts.zip`
	8. Para alterar o diretório, execute o comando:
	`cd /var/tmp/sysutils/PrereqsScripts`
	9. Para executar o script de verificação, execute o comando:
	`./M9VerifyPrereqs.sh`	

Tarefa	Descrição	Habilidades necessárias
	10. Depois que o script de verificação solicitar a entrada, insira o URL e o número da porta do Amazon S3. Em seguida, insira o IP/DNS e o número da porta do z/OS. **Note** O script executa uma verificação para confirmar se a EC2 instância pode se conectar ao bucket e ao agente do S3 em execução no mainframe. Se uma conexão for estabelecida, uma mensagem de sucesso será exibida.	

Tarefa	Descrição	Habilidades necessárias

Instale o software do servidor de gerenciamento.	1. Crie uma pasta e uma subpasta no diretório raiz (por exemplo,`/data/model9`) na EC2 instância em que você planeja tornar o servidor ativo.
	2. Para instalar o `amazon-efs-utils` pacote e montar o sistema de arquivos Amazon EFS criado anteriormente, execute os seguintes comandos:
	`sudo yum install -y amazon-efs-utils`
	`sudo mount -t efs -o tls <File System ID>:/ /data/model9`
	3. Para atualizar o `/etc/fstab` arquivo da EC2 instância com uma entrada para o sistema de arquivos do Amazon EFS (para que o Amazon EFS seja automaticamente remontado quando o Amazon for EC2 reinicial izado), execute o comando:
	`<Amazon-EFS-file-system-id>:/ /data/model9 efs defaults,_netdev 0 0`
		Arquiteto de nuvem, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	4. Para definir o caminho para os arquivos de instalação do BMC AMI Cloud e o local de instalação de destino, execute os seguintes comandos para exportar variáveis:
	`export MODEL9_HOME=/data/model9`
	`export M9INSTALL=/var/tmp`
	Note
	Recomendamos que você adicione esses comandos EXPORT ao seu `.bashrc` script.
	5. Para alterar o diretório, execute comando `cd $MODEL9_HOME` e crie outro subdiretório executando o comando `mkdir diag`.
	6. Para descompactar o arquivo de instalação, execute o comando:
	`unzip $M9INSTALL/model9-<v2.x.y>_build_<build-id>-server.zip`	

Tarefa	Descrição	Habilidades necessárias

	Note
	Substitua `x.y` (a versão) e `build-id` por seus valores.
	7. Para implantar o aplicativo, execute os seguintes comandos:
	`docker load -i $MODEL9_HOME/model9-<v2.x.y>_build_<build-id>.docker`
	`docker load -i $MODEL9_HOME/postgres-12.10-x86.docker.gz`
	Note
	Substitua `v2.x.y` (a versão) e `build-id` por seus valores.
	8. Na pasta `$MODEL9_HOME/conf` , atualize o `model9-local.yml` arquivo.
	Note
	Alguns dos parâmetros têm	

Tarefa	Descrição	Habilidades necessárias

	valores padrão e outros podem ser atualizados conforme necessário. Para obter mais informações, consulte as instruções no arquivo `model9-local.yml` .
	9. Crie um arquivo chamado **`$MODEL9_HOME/conf`** , em seguida, adicione os seguintes parâmetros ao arquivo:
	`TZ=America/New_York`
	`EXTRA_JVM_ARGS=-Xmx2048m`
	10. Para criar uma ponte de rede Docker, execute o comando:
	`docker network create -d bridge model9network`
	11. Para iniciar o contêiner do banco de dados PostgreSQL para o BMC AMI Cloud, execute o seguinte comando:	

Tarefa	Descrição	Habilidades necessárias
	``` docker run -p 127.0.0.1:5432:5432 \ -v $MODEL9_HOME/db/da ta:/var/lib/postgr esql/data:z \ --name model9db -- restart unless-st opped \ --network model9net work \ -e POSTGRES_PASSWORD= model9 -e POSTGRES_ DB=model9 -d postgres:12.10 ```	
	12. Depois que o contêiner do PostgreSQL começar a ser executado, execute o comando a seguir para iniciar o servidor do aplicativo: ``` docker run -d -p 0.0.0.0:443:443 -p 0.0.0.0:80:80 \ --sysctl net.ipv4. tcp_keepalive_time =600 \ --sysctl net.ipv4. tcp_keepalive_intv l=30 \ --sysctl net.ipv4. tcp_keepalive_prob es=10 \ -v $MODEL9_HOME:/mode l9:z -h $(hostname) --restart unless-st opped \ ```	

Tarefa	Descrição	Habilidades necessárias

	`--env-file $MODEL9_HOME/conf/model9.env \`
	`--network model9network \`
	`--name model9-v2.x.y model9:<v2.x.y>.<build-id>`
	
	Note
	Substitua `v2.x.y` (a versão) e `build-id` por seus valores.
	
	13. Para verificar o status de integridade dos dois contêineres, execute o comando:
	
	`docker ps -a`
	
	14. Para instalar um servidor de gerenciamento nas EC2 instâncias passivas, repita as etapas 1—4, 7 e 10—13.
	
	Note
	Para solucionar problemas, acesse os registros armazenados na `/data/model9/logs/` pasta. Para obter mais	

Tarefa	Descrição	Habilidades necessárias
	informações, consulte a documentação da BMC.	

Adicione um agente e defina uma política de backup ou arquivamento no servidor de gerenciamento do BMC AMI Cloud

Tarefa	Descrição	Habilidades necessárias
Adicione um novo agente.	Antes de adicionar um novo agente, confirme o seguinte: • Um agente BMC AMI Cloud está sendo executado na LPAR do mainframe e foi totalment e inicializado. Identifique o agente procurando a mensagem de `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` inicializ ação no spool. • Um contêiner Docker para o servidor de gerenciamento está totalmente inicializado e em execução. Você deve criar um agente no servidor de gerenciam ento antes de definir qualquer política de backup e arquivamento. Para criar o agente, faça o seguinte:	Administrador ou desenvolv edor de armazenamento de mainframe

Tarefa	Descrição	Habilidades necessárias
	1. Use um navegador da web para acessar o servidor de gerenciamento que está implantado em sua EC2 máquina Amazon e, em seguida, faça login com suas credenciais de mainframe. 2. Escolha a guia AGENTES E escolha ADD NEW AGENT. 3. Em Nome, insira o nome do agente. 4. Em Nome do host/endereço IP, insira o nome do host ou o endereço IP do seu mainframe. 5. Em Porta, digite o número da porta. 6. Escolha TESTAR CONEXÃO. Você pode ver uma mensagem de sucesso se a conectividade for estabelecida com sucesso. 7. Escolha CREATE (CRIAR). Depois que o agente for criado, você verá o status conectado em relação ao agente de armazenamento de objetos e mainframe em uma	

Tarefa	Descrição	Habilidades necessárias
	nova janela que aparece na tabela.	
Crie uma política de backup ou arquivamento.	1. Escolha POLÍTICAS. 2. Escolha CRIAR POLÍTICA. 3. Na página CRIAR UMA NOVA POLÍTICA, insira suas especificações de política. **Note** Para obter mais informações sobre as especific ações disponíveis, consulte Criação de uma nova política na documentação da BMC. 4. Escolha Terminar. 5. A nova política agora está listada como uma tabela. Para ver essa tabela, escolha a guia POLÍTICAS.	Administrador ou desenvolv edor de armazenamento de mainframe

Execute a política de backup ou arquivamento a partir do servidor de gerenciamento

Tarefa	Descrição	Habilidades necessárias
Execute a política de backup ou arquivamento.	Execute a política de backup ou arquivamento de dados que você criou anteriormente	Administrador ou desenvolv edor de armazenamento de mainframe

Tarefa	Descrição	Habilidades necessárias
	no servidor de gerenciamento, manual ou automaticamente (com base em uma programação). Para executar a política manualmente: 1. No menu de navegação, escolha a guia POLÍTICAS. 2. No lado direito da tabela da política que você deseja executar, escolha o menu de três pontos. 3. Escolha Executar agora. 4. Na janela pop-up de confirmação, escolha SIM, EXECUTAR POLÍTICA AGORA. 5. Depois que a política for executada, verifique o status de execução na seção de atividade da política. 6. Para a política executada, escolha o menu de três pontos e, em seguida, escolha Exibir registro de execução para ver os registros. 7. Para verificar se o backup foi criado, verifique o bucket do S3.	

Tarefa	Descrição	Habilidades necessárias
Restaure a política de backup ou arquivamento.	1. No menu de navegação, escolha a guia POLÍTICAS. 2. Escolha a política na qual executar o processo de restauração. Isso listará todas as atividades de backup ou arquivamento executadas no passado para essa política específica. 3. Para selecionar os backups que você deseja restaurar, escolha a coluna Data-hora. O nome do grupo `file/Volume/Storage` mostra os detalhes de execução da política. 4. No lado direito da tabela, escolha o menu de três pontos e, em seguida, escolha RESTAURAR. 5. Na janela pop-up, insira o nome, o volume e o grupo de armazenamento do destino e escolha RESTAURAR. 6. Insira suas credenciais de mainframe e escolha RESTAURAR novamente. 7. Para verificar se a restauração foi bem-sucedida, verifique os registros ou o mainframe.	Administrador ou desenvolvedor de armazenamento de mainframe

Execute a política de backup ou arquivamento a partir do mainframe

Tarefa	Descrição	Habilidades necessárias
Execute a política de backup ou arquivamento usando o M9CLI.	Use o M9CLI para realizar processos de backup e restauração a partir do TSO/E, REXX ou até mesmo JCLs sem configurar regras no servidor de gerenciamento do BMC AMI Cloud. Usando o TSO/E: Se você usar TSO/E, certifique-se de que `M9CLI REXX` esteja concatenado com. `TSO` Para fazer backup de um conjunto de dados por meio do TSO/E, use o comando. `TSO M9CLI BACKDSN <DSNAME>` **Note** Para obter mais informações sobre os comandos da M9CLI, consulte a referência da CLI na documentação da BMC. Usando JCLs: Para executar a política de backup e arquivamento	Administrador ou desenvolvedor de armazenamento de mainframe

Tarefa	Descrição	Habilidades necessárias

	usando JCLs, execute o `M9CLI` comando.
	
	Usando operações em lote:
	
	O exemplo a seguir mostra como arquivar um conjunto de dados executando o `M9CLI` comando em lote:
	
	`//JOBNAME JOB …`
	`//M9CLI EXEC PGM=IKJEF`
	`T01`
	`//STEPLIB DD DISP=SHR,`
	`DSN=<MODEL9 LOADLIB>`
	`//SYSEXEC DD DISP=SHR,`
	`DSN=<MODEL9 EXEC LIB>`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSIN DD TSO M9CLI`
	` ARCHIVE`
	` M9CLI ARCHIVE <DSNNAME`
	` OR DSN PATTERN>`
	`/`	

Tarefa	Descrição	Habilidades necessárias
Execute a política de backup ou arquivamento no lote JCL.	O BMC AMI Cloud fornece um exemplo de rotina de JCL chamado M9SAPIJ. Você pode personalizar o M9SAPIJ para executar uma política específica criada no servidor de gerenciamento com uma JCL. Esse trabalho também pode fazer parte de um programador de lotes para executar processos de backup e restauração automatic amente. O trabalho em lotes espera os seguintes valores obrigatórios: • Endereço IP/nome do host do servidor de gerenciam ento • Número da porta • ID da política ou nome da política (que é criado no servidor de gerenciamento) **Note** Você também pode alterar outros valores seguindo as instruções na tarefa de amostra.	Administrador ou desenvolv edor de armazenamento de mainframe

Recursos relacionados

- Modernização do mainframe com a AWS (documentação da AWS)
- Como o backup na nuvem para mainframes reduz custos com o Model9 e a AWS (blog da rede de parceiro da AWS)
- Como habilitar a análise de dados de mainframe na AWS usando o Model9 (blog da rede de parceiro da AWS)
- Recomendações de resiliência do AWS Direct Connect (documentação da AWS)
- Documentação da BMC AMI Cloud (site da BMC)

Crie programas COBOL Db2 usando e AWS Mainframe ModernizationAWS CodeBuild

Criado por Luis Gustavo Dantas (AWS) e Eduardo Zimelewicz (AWS)

Resumo

Esse padrão explica como criar um AWS CodeBuild projeto simples para pré-compilar e vincular programas COBOL Db2 usando as ferramentas Replatform. AWS Mainframe Modernization Isso permite a implantação e a execução desses programas no ambiente de execução do AWS Mainframe Modernization Replatform.

O COBOL, uma linguagem de programação voltada para negócios, alimenta muitos aplicativos críticos devido à sua confiabilidade e legibilidade. O IBM Db2, um sistema de gerenciamento de banco de dados relacional, gerencia grandes volumes de dados com eficiência e se integra aos programas COBOL por meio de SQL. Juntos, o COBOL e o Db2 formam a espinha dorsal das operações de missão crítica em setores como finanças e governo, apesar do surgimento de novas tecnologias.

A migração de componentes COBOL e Db2 do ambiente de mainframe para outras plataformas leva a desafios como compatibilidade de plataformas, complexidade de integração, migração de dados e otimização de desempenho. A movimentação desses componentes essenciais requer planejamento cuidadoso, conhecimento técnico e recursos para garantir uma migração tranquila e, ao mesmo tempo, manter a confiabilidade e a funcionalidade.

O AWS Mainframe Modernization serviço fornece ferramentas e recursos para reformular aplicativos e bancos de dados de mainframe para execução em AWS infraestrutura, como instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Isso envolve mover as cargas de trabalho do mainframe para a nuvem sem grandes alterações no código.

O processo de pré-compilação e vinculação do Db2 é essencial para otimizar o desempenho e a confiabilidade dos aplicativos de banco de dados. A pré-compilação transforma instruções SQL incorporadas em código executável, o que reduz a sobrecarga de tempo de execução e aumenta a eficiência. O processo de vinculação vincula o código pré-compilado às estruturas do banco de dados, facilitando os caminhos de acesso e a otimização de consultas. Esse processo garante a integridade dos dados, melhora a capacidade de resposta do aplicativo e protege contra vulnerabilidades de segurança. Aplicativos devidamente pré-compilados e vinculados minimizam o consumo de recursos, aprimoram a escalabilidade e reduzem os riscos de ataques de injeção de SQL.

Pré-requisitos e limitações

Pré-requisitos

- Um acesso Conta da AWS ao console em nível administrativo.
- Um sistema de banco de dados IBM Db2, como IBM Db2 for z/OS ou Db2 for Linux, Unix e Windows (LUW).
- O software IBM Data Server Client, disponível para download no site da IBM. Para obter mais informações, consulte os tipos IBM Data Server Client e Data Server Driver.
- Um programa COBOL Db2 a ser compilado e vinculado. Como alternativa, esse padrão fornece um exemplo básico de programa que você pode usar.
- Uma nuvem privada virtual (VPC) AWS com uma rede privada. Para obter informações sobre a criação de uma VPC, consulte a documentação da Amazon Virtual Private Cloud (Amazon VPC).
- Um repositório de controle de origem, como GitHub ou GitLab.

Limitações

- Para AWS CodeBuild cotas, consulte Cotas para. AWS CodeBuild
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Pilha de tecnologia de origem

A pilha de origem inclui:

- Programas COBOL que usam um banco de dados Db2 para armazenar dados
- Compilador IBM COBOL e pré-compilador Db2 for z/OS
- Outras partes da configuração do mainframe, como o sistema de arquivos, o gerenciador de transações e o spool

Pilha de tecnologias de destino

A abordagem desse padrão funciona com duas opções: mover dados do Db2 for z/OS para o Db2 for LUW ou permanecer no Db2 for z/OS. A arquitetura de destino inclui:

- Programas COBOL que usam um banco de dados Db2 para armazenar dados
- AWS Mainframe Modernization Ferramentas de compilação de replataformas
- AWS CodeBuild como a infraestrutura para criar o aplicativo
- Outros Nuvem AWS recursos, como Amazon Linux

Arquitetura de destino

O diagrama ilustra o seguinte:

1. O usuário carrega seu código em um repositório de controle de origem, como GitHub ou. GitLab
2. AWS CodePipeline percebe a alteração e obtém o código do repositório.
3. CodePipeline inicia AWS CodeBuild e envia o código.
4. CodeBuild segue as instruções no `buildspec.yml` modelo (fornecidas na seção Informações adicionais) para:
   a. Obtenha o IBM Data Server Client de um bucket do Amazon Simple Storage Service (Amazon S3).
   b. Instale e configure o IBM Data Server Client.
   c. Recupere as credenciais do Db2 de. AWS Secrets Manager
   d. Conecte-se ao servidor do Db2.
   e. Pré-compile, compile e vincule o programa COBOL.
   f. Guarde os produtos acabados em um balde S3 AWS CodeDeploy para uso.
5. CodePipeline começa CodeDeploy.
6. CodeDeploy coordena seus agentes, que já estão instalados nos ambientes de execução. Os agentes buscam o aplicativo no Amazon S3 e o instalam com base nas instruções em. `appspec.yml`

Para manter as coisas simples e focadas na construção, as instruções nesse padrão abrangem as etapas de 1 a 4, mas não incluem a implantação do programa COBOL Db2.

Automação e escala

Para simplificar, esse padrão descreve como provisionar recursos manualmente. No entanto, existem várias opções de automação disponíveis, como AWS CloudFormation AWS Cloud Development Kit (AWS CDK), e HashiCorp Terraform, que automatizam essas tarefas. Para obter mais informações, consulte AWS CloudFormationa AWS CDKdocumentação e.

Ferramentas

Serviços da AWS

- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeDeployautomatiza implantações na Amazon EC2 ou em instâncias, AWS Lambda funções ou serviços do Amazon Elastic Container Service (Amazon ECS).
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- AWS Mainframe Modernizationfornece ferramentas e recursos para ajudá-lo a planejar e implementar a migração e a modernização de mainframes para ambientes de tempo de execução AWS gerenciados.

Outras ferramentas

- Imagem do Amazon ECR para ferramentas de AWS Mainframe Modernization replataforma. Para compilar um aplicativo COBOL, você precisará começar CodeBuild usando uma imagem do Amazon Elastic Container Registry (Amazon ECR) que contém as ferramentas Replatform: AWS Mainframe Modernization

  ```
  673918848628.dkr.ecr.<your-region>.amazonaws.com/m2-enterprise-build-tools:9.0.7.R1
  ```

  Para obter mais informações sobre a imagem ECR disponível, consulte o tutorial no Guia do AWS Mainframe Modernization usuário.
- O software IBM Data Server Client é essencial para pré-compilar e vincular programas COBOL Db2. CodeBuild Ele atua como uma ponte entre o compilador COBOL e o Db2.

Práticas recomendadas

- Nem todo programa COBOL depende do Db2 como sua camada de persistência de dados. Certifique-se de que as diretivas de compilação para acessar o Db2 sejam aplicadas somente aos programas COBOL projetados especificamente para interagir com o Db2. Implemente uma lógica para distinguir entre programas COBOL Db2 e programas COBOL que não usam Db2.
- Recomendamos que você evite compilar programas que não tenham sido modificados. Implemente um processo para identificar quais programas precisam ser compilados.

Épicos

Crie a infraestrutura de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um bucket S3 para hospedar o IBM Data Server Client e os artefatos do pipeline.	Você precisa configurar um bucket S3 para (a) carregar o IBM Data Server Client, (b) armazenar seu código do repositório e (c) armazenar os resultados do processo de criação. 1. Faça login no AWS Management Console e abra o console do Amazon S3. 2. Escolha um bucket S3 existente ou crie um novo bucket. Anote o Amazon Resource Name (ARN) do bucket para uso futuro. Para saber como criar um bucket do S3, consulte a documentação do Amazon S3.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Faça o upload do IBM Data Server Client para o bucket S3.	1. No console do Amazon S3, escolha o bucket para abri-lo. 2. Escolha Criar pasta, especifique seu nome como cliente e escolha Criar pasta. 3. Abra a pasta do cliente, escolha Carregar, Adicionar arquivos. 4. Escolha o arquivo IBM Data Server Client que você baixou anteriormente do site da IBM para seu sistema de arquivos local. O nome do arquivo deve ser semelhant e a `v11.5.8_linuxx64_client.tar.gz` ou `v11.5.9_linuxx64_client.tar.gz`. 5. Escolha Abrir, Carregar e aguarde a conclusão do upload. 6. Na guia Arquivos e pastas, escolha o Data Server Client e anote seu URI do S3.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie um AWS Secrets Manager segredo para suas credenciais do Db2.	Para criar um segredo para armazenar suas DB2 credenciais com segurança: 1. No console do Secrets Manager, escolha Armazenar um novo segredo. 2. No painel Escolher tipo de segredo, escolha Outro tipo de segredo e Texto sem formatação. 3. Na caixa Texto simples, digite suas credenciais do Db2 usando a seguinte estrutura JSON. `{ "username": "<your-db2-user-name>", "password": "<your-db2-password>", "db2node": "db2dev", "db2host": "<your-db2-hostname-or-IP>", "db2port": <your-db2-port>, "db2name": "<your-db2-location>", "qualifier": "<your-db2-qualifier>"`	AWS geral

Tarefa	Descrição	Habilidades necessárias
	<pre>}</pre> 4. Escolha Avançar e dê ao segredo um nome como `dev-db2-cred` . 5. Escolha Avançar, Avançar e Armazenar. Para obter mais informações sobre a criação de segredos, consulte a documentação do Secrets Manager.	

Tarefa	Descrição	Habilidades necessárias
Verifique se o Db2 está acessível a partir da sub-rede VPC.	AWS CodeBuild precisa de uma conexão com o servidor Db2 para que o Data Server Client possa realizar operações de pré-compilação e vinculação. Certifique-se de que CodeBuild possa acessar o servidor Db2 por meio de uma conexão segura. 1. Abra o console da Amazon VPC. 2. No painel de navegação, escolha Sub-redes e anote o IDs final IPv4 CIDRsdas sub-redes privadas onde funcionará. CodeBuild 3. Atualize as configurações atuais de controle de acesso à rede para seu sistema Db2 introduzindo uma regra de entrada. Essa regra deve permitir o acesso TCP personali zado à porta Db2 exclusiva mente da sub-rede CIDRs associada ao seu projeto. CodeBuild	Administrador de rede, General AWS

Crie os artefatos do aplicativo

Tarefa	Descrição	Habilidades necessárias
Crie o ativo COBOL Db2.	1. Se você quiser usar um exemplo simples de COBOL Db2, salve o código-fonte a seguir como. `CDB2SMP.cbl` Ou você pode substituir esse exemplo por um programa que você já possui. `IDENTIFICATION DIVISION. PROGRAM-ID. CDB2SMP. DATA DIVISION. WORKING-STORAGE SECTION. 01 WS-NAME PIC X(100). PROCEDURE DIVISION. EXEC SQL SELECT NAME INTO :WS-NAME FROM SYSIBM.SYSTABLES END-EXEC GOBACK.` 2. Confirme as alterações e envie o arquivo para o seu repositório.	Desenvolvedor de aplicativos
Crie o arquivo `buildspec.yml` .	1. Gere o `buildspec.yml` arquivo com base no	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	exemplo fornecido na seção Informações adicionais. 2. Confirme as alterações e envie o arquivo para o seu repositório.	
Conecte seu repositório a. CodePipeline	1. Abra o AWS console de Ferramentas do desenvolvedor. 2. No painel de navegação , escolha Configurações, Conexões. 3. Siga as instruções na documentação do console Developer Tools para o provedor de origem de sua escolha. Você precisará do Amazon Resource Name (ARN) para a conexão ao criar a política AWS Identity and Access Management (IAM) para uma CodePipeline etapa posterior.	AWS DevOps

Configurar permissões do

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM para CodeBuild.	O CodeBuild projeto requer acesso a alguns recursos, incluindo Secrets Manager e Amazon S3.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	Para configurar as permissões necessárias: 1. Abra o console do IAM. 2. No painel de navegação , escolha Políticas, Criar política e selecione o CodeBuild serviço. 3. Alterne a formatação de Visual para JSON e copie a CodeBuild política fornecida na seção Informações adicionais para o campo Editor de políticas. 4. Nomeie e salve essa política para futura referênci a na próxima etapa. Para obter mais informações sobre a criação de políticas do IAM, consulte a documenta ção do IAM.	

Tarefa	Descrição	Habilidades necessárias
Crie uma função do IAM para CodeBuild.	Para disponibilizar as políticas de segurança CodeBuild, você precisa configurar uma função do IAM. Para criar essa função: 1. No console do IAM, no painel de navegação, escolha Roles, Create Role. 3. Para o tipo de entidade confiável, mantenha a AWS service (Serviço da AWS)configuração padrão. 4. Em Caso de uso, selecione o CodeBuild serviço e escolha Avançar. 4. Na lista de políticas do IAM disponíveis, localize a política para CodeBuild a qual você criou e escolha Avançar para anexá-la à função. 5. Especifique um nome para a função e escolha Create role para salvá-la para futura referência CodeBuild. Para obter mais informações sobre como criar uma função do IAM para um AWS service (Serviço da AWS), consulte a documentação do IAM.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM para CodePipeline.	O AWS CodePipeline pipeline requer acesso a alguns recursos, incluindo seu repositório de código e o Amazon S3. Repita as etapas fornecida s anteriormente CodeBuild para criar uma política do IAM para CodePipeline (na etapa 2, escolha CodePipelineem vez de CodeBuild).	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Crie uma função do IAM para CodePipeline.	Para disponibilizar as políticas de segurança CodePipeline, você precisa configurar uma função do IAM.
	
	Para criar essa função:
	
	1. No console do IAM, escolha Roles, Create Role.
	2. Em Trusted entity type (Tipo de entidade confiável), escolha Custom trust policy (Política de confiança personalizada).
	
	Uma política com um `Principal` elemento vazio será exibida.
	3. Na `Principal` linha, entre as chaves, adicione:
	
	`"Service": "codepipeline.amazonaws.com"`
	
	A política de confiança terá a seguinte aparência:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Sid": "Statement1", "Effect": "Allow", "Principal": {`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	<pre>"Service": "codepipeline.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre> 4. Escolha Próximo. 5. Na lista de políticas do IAM disponíveis, localize a política para CodePipeline a qual você criou e escolha Avançar para anexá-la à função. 6. Especifique um nome para a função e escolha Create role para salvá-la para futura referência CodePipeline.	

Compilar e vincular o programa COBOL Db2

Tarefa	Descrição	Habilidades necessárias
Crie um CodePipeline pipeline e um CodeBuild projeto.	Para criar um CodePipeline pipeline e o CodeBuild projeto que compila e vincula o programa COBOL Db2: 1. Abra o CodePipeline console e escolha Create Pipeline, Build custom pipeline.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	2. Especifique um nome para o pipeline. 3. Em Função de serviço, escolha Função de serviço existente e escolha especificar o ARN da função do IAM para a qual você criou. CodePipeline 4. Expanda Configurações avançadas, escolha Local personalizado, escolha o bucket do S3 que você criou anteriormente e escolha Avançar. 5. Para provedor de origem, selecione seu provedor de origem terceirizado, e forneça as informações relevantes para o provedor:. a. Em Conexão, selecione a conexão que foi criada para o provedor de origem. b. Em Nome do repositório, selecione seu repositór io. c. Em Ramificação padrão, selecione a ramificaç ão que armazena seu programa COBOL e. `buildspec.yml` d. Escolha Próximo.	

Tarefa	Descrição	Habilidades necessárias
	6. Em Provedor de compilação, escolha Outros provedores de compilação, AWS CodeBuild. 7. Em Nome do projeto, escolha Criar projeto. O console exibe uma CodeBuild janela na qual você pode criar um projeto de construção. Nesta janela: a. Insira um nome para o projeto. b. Em Environment image (Imagem de ambiente), escolha Custom image (Imagem personalizada). c. Em Tipo de ambiente, escolha Linux Container. d. Em Conta ECR, escolha Outra conta ECR. e. Para URI do repositório Amazon ECR, insira:. `673918848628.dkr.ecr.<your-region>.amazonaws.com/m2-enterprise-build-tools:8.0.9.R1` f. Em Função de serviço, escolha Função de	

Tarefa	Descrição	Habilidades necessárias
	serviço existente e selecione a função para a qual você criou CodeBuild. g. Expanda a seção Configuração adicional e escolha a VPC, as sub-redes privadas e o grupo de segurança para esse projeto. h. Na seção Buildspec, escolha Usar um arquivo buildspec. i. No final da janela, escolha Continuar paraCodePipeline. A CodeBuild janela será fechada para que você possa voltar ao CodePipeline console. 8. De volta ao CodePipeline console, escolha Avançar. 9. No painel Adicionar estágio de implantação, escolha Ignorar estágio de implantação e confirme. 10. Revise os parâmetros do pipeline e escolha Create pipeline.	
Revise a saída.	Verifique o sucesso da compilação revisando os registros da CodePipeline compilação.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Verifique os resultados no Db2.	Verifique a versão do pacote na tabela SYSPLAN.
	
	`select CAST(NAME AS VARCHAR(10)) as name, VALIDATE, LAST_BIND_TIME, LASTUSED, CAST(PKGVERSION AS VARCHAR(10)) as PKGVERSION from SYSIBM.SYSPLAN where NAME = 'CDB2SMP' order by LAST_BIND_TIME desc`
	
	A versão deve corresponder ao ID da CodeBuild compilaçã o, que está CDB2SMP em nosso exemplo:
	
	`NAME VALIDATE LAST_BIND_TIME LASTUSED PKGVERSION ---------- -------- ---------- -------- CDB2SMP B 2024-05-18-11.53.1 1.503738 01/01/0001 19`	

Solução de problemas

Problema	Solução
Ocasionalmente, o AWS console muda de região quando você se move entre os serviços.	Certifique-se de verificar o selecionado Região da AWS sempre que alternar entre os serviços.

Problema	Solução
	O Região da AWS seletor está no canto superior direito da janela do console.
Pode ser difícil identificar problemas de conectividade do Db2 a partir do CodeBuild.	Para solucionar problemas de conectividade, adicione o seguinte comando DB2 connect ao `buildspec.yml` arquivo. Essa adição ajuda você a depurar e resolver problemas de conectividade. `db2 connect to $DB_NAME user $DB2USER using $DB2PASS`
Ocasionalmente, o painel de funções no console do IAM não mostra imediatamente a política do IAM que você criou.	Se você encontrar um atraso, atualize a tela para exibir as informações mais recentes.

Recursos relacionados

Documentação da IBM

- Tipos de cliente e driver do IBM Data Server
- Baixe o IBM Data Server Client e os tipos de driver

AWS documentação

- Guia do usuário do Amazon S3
- AWS CodeBuild Guia do usuário
- AWS Mainframe Modernization Guia do usuário
- AWS Secrets Manager Guia do usuário
- AWS CodePipeline Guia do usuário
- AWS CodeDeploy Guia do usuário

Mais informações

CodeBuild política

Substitua os espaços reservados <RegionID><AccountID>,<SubnetARN>,<BucketARN>, e <DB2CredSecretARN> por seus valores.

```
{"Version": "2012-10-17",
    "Statement": [
        {"Action": "ecr:GetAuthorizationToken", "Effect": "Allow", "Resource": "*" },
        {"Action": ["ecr:GetDownloadUrlForLayer", "ecr:BatchGetImage",
                    "ecr:BatchCheckLayerAvailability"],
         "Effect": "Allow",
         "Resource": "arn:aws:ecr:*:673918848628:repository/m2-enterprise-build-
tools"},
        {"Action": "s3:PutObject", "Effect": "Allow", "Resource": "arn:aws:s3:::aws-m2-
repo-*/*"},
        {"Action": ["logs:PutLogEvents", "logs:CreateLogStream",
 "logs:CreateLogGroup"],
         "Effect": "Allow", "Resource": "arn:aws:logs:<RegionId>:<AccountId>:*"},
        {"Action": ["ec2:DescribeVpcs", "ec2:DescribeSubnets",
                    "ec2:DescribeSecurityGroups", "ec2:DescribeNetworkInterfaces",
                    "ec2:DescribeDhcpOptions", "ec2:DeleteNetworkInterface",
                    "ec2:CreateNetworkInterface"],
         "Effect": "Allow", "Resource": "*"},
        {"Action": "ec2:CreateNetworkInterfacePermission",
         "Effect": "Allow", "Resource": ["<SubnetARN>"]},
        {"Action": "s3:*", "Effect": "Allow", "Resource": ["<BucketARN>/
*","<BucketARN>"]},
        {"Action": "secretsmanager:GetSecretValue",
         "Effect": "Allow", "Resource": "<DB2CredSecretARN>"}
    ]
}
```

CodePipeline política

Substitua os espaços reservados <BucketARN> <ConnectionARN> por seus valores.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {"Action": ["s3:List*", "s3:GetObjectVersion", "s3:GetObject",
 "s3:GetBucketVersioning" ],
```

```
        "Effect": "Allow",
        "Resource": ["<BucketARN>/*", "<BucketARN>"]},
        {"Action": ["codebuild:StartBuild", "codebuild:BatchGetBuilds"],
         "Effect": "Allow", "Resource": "*"},
        {"Action": ["codestar-connections:UseConnection"],
         "Effect": "Allow", "Resource": "<ConnectionARN>"}
        ]
}
```

buildspec.yml

Substitua o <your-bucket-name> espaço reservado pelo nome real do bucket do S3.

```
version: 0.2
phases:
  pre_build:
    commands:
      - /var/microfocuslicensing/bin/mfcesd -no > /var/microfocuslicensing/logs/
mfcesd_startup.log 2>&1 &
      - |
        mkdir $CODEBUILD_SRC_DIR/db2client
        aws s3 cp s3://<your-bucket-name>/v11.5.8_linuxx64_client.tar.gz
 $CODEBUILD_SRC_DIR/db2client/ >> /dev/null 2>&1
        tar -xf $CODEBUILD_SRC_DIR/db2client/v11.5.8_linuxx64_client.tar.gz -C
 $CODEBUILD_SRC_DIR/db2client/
        cd $CODEBUILD_SRC_DIR/db2client/
        ./client/db2_install -f sysreq -y -b /opt/ibm/db2/V11.5 >> /dev/null 2>&1

        useradd db2cli
        /opt/ibm/db2/V11.5/instance/db2icrt -s client -u db2cli db2cli
        DB2CRED=$(aws secretsmanager get-secret-value --secret-id dev-db2-cred | jq -r
 '.SecretString | fromjson')
        read -r DB2USER DB2PASS DB_NODE DB_HOST DB_PORT DB_NAME DB_QUAL <<<$(echo
 $DB2CRED | jq -r
 '.username, .password, .db2node, .db2host, .db2port, .db2name, .qualifier')
        . /home/db2cli/sqllib/db2profile
        db2 catalog tcpip node $DB_NODE remote $DB_HOST server $DB_PORT
        db2 catalog db $DB_NAME as $DB_NAME at node $DB_NODE authentication server
  build:
    commands:
      - |
        revision=$CODEBUILD_SRC_DIR/loadlib
        mkdir -p $revision; cd $revision
        . /opt/microfocus/EnterpriseDeveloper/bin/cobsetenv
```

```
        cob -zU $CODEBUILD_SRC_DIR/CDB2SMP.cbl -C "DB2(DB==${DB_NAME} PASS==${DB2USER}.
${DB2PASS} VERSION==${CODEBUILD_BUILD_NUMBER} COLLECTION==DB2AWSDB"
artifacts:
  files:
    - "**/*"
  base-directory: $revision
```

Crie um PAC de servidor corporativo da Micro Focus com o Amazon EC2 Auto Scaling e o Systems Manager

Criado por Kevin Yung (AWS), Peter Woods, Abraham Rondon (Micro Focus) e Krithika Palani Selvam (AWS)

Resumo

Esse padrão introduz uma arquitetura escalável para aplicativos de mainframe usando o Micro Focus Enterprise Server no Scale-Out Performance and Availability Cluster (PAC) e um grupo Amazon Elastic Compute Cloud (Amazon) EC2 Auto Scaling no Amazon Web Services ().AWS A solução é totalmente automatizada com ganchos de AWS Systems Manager ciclo de vida do Amazon EC2 Auto Scaling. Ao usar esse padrão, você pode configurar seus aplicativos de mainframe on-line e em lote para obter alta resiliência, aumentando e reduzindo automaticamente a escala com base em suas demandas de capacidade.

> **Note**
>
> Esse padrão foi testado com o Micro Focus Enterprise Server versão 6.0. Para a versão 8, consulte Configurar o Micro Focus Runtime (na Amazon EC2).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Software e licença do Micro Focus Enterprise Server. Para obter detalhes, entre em contato com a equipe de vendas da Micro Focus.
- Uma compreensão do conceito de reconstrução e entrega de um aplicativo de mainframe para ser executado no Micro Focus Enterprise Server. Para obter uma visão geral de alto nível, consulte a planilha de dados do Micro Focus Enterprise Server.
- Uma compreensão dos conceitos do Cluster Escalável de Desempenho e Disponibilidade do Micro Focus Enterprise Server. Para ter mais informações, consulte a documentação do Micro Focus Enterprise Server.

- Uma compreensão do conceito geral de aplicativo de mainframe DevOps com integração contínua (CI). Para um padrão de orientação AWS prescritiva desenvolvido pela AWS Micro Focus, consulte Modernização do mainframe: DevOps on AWS with Micro Focus.

> **Note**
>
> Esse padrão foi testado com o Micro Focus Enterprise Server versão 6. Para a versão 8, consulte Configurar o Micro Focus Runtime (na Amazon EC2).

Limitações

- Para obter uma lista das plataformas suportadas pelo Micro Focus Enterprise Server, consulte a ficha técnica do Micro Focus Enterprise Server.
- Os scripts e testes usados nesse padrão são baseados no Amazon EC2 Windows Server 2019; outras versões e sistemas operacionais do Windows Server não foram testados para esse padrão.
- O padrão é baseado no Micro Focus Enterprise Server 6.0 para Windows; versões anteriores ou superiores não foram testadas no desenvolvimento desse padrão.

Versões do produto

- Micro Focus Enterprise Server 6.0
- Windows Server 2019

Arquitetura

No ambiente convencional de mainframe, você deve provisionar hardware para hospedar seus aplicativos e dados corporativos. Para atender e atender aos picos de demandas sazonais, mensais, trimestrais ou até mesmo sem precedentes ou inesperadas, os usuários de mainframe devem aumentar a escala horizontalmente comprando capacidade adicional de armazenamento e computação. Aumentar o número de recursos de armazenamento e capacidade computacional melhora o desempenho geral, mas o dimensionamento não é linear.

Esse não é o caso quando você começa a adotar um modelo de consumo sob demanda na AWS usando Amazon Auto EC2 Scaling e Micro Focus Enterprise Servers. As seções a seguir explicam detalhadamente como criar uma arquitetura de aplicativo de mainframe totalmente automatizada

e escalável usando o cluster de desempenho e disponibilidade (PAC) do Micro Focus Enterprise Server Scale-Out com um grupo Amazon Auto Scaling. EC2

Arquitetura de escalabilidade automática do Micro Focus Enterprise Server

Primeiro, é importante entender os conceitos básicos do Micro Focus Enterprise Server. Esse ambiente fornece um ambiente de implantação x86 compatível com mainframe para aplicativos que tradicionalmente são executados no mainframe IBM. Ele oferece execuções on-line e em lote e um ambiente de transações que oferece suporte ao seguinte:

- IBM COBOL
- IBM PL/I
- Trabalhos em lote do IBM JCL
- Transações IBM CICS e IMS TM
- Serviços da web
- Utilitários de lote comuns, incluindo SORT

O Micro Focus Enterprise Server permite que os aplicativos de mainframe sejam executados com o mínimo de alterações. Os workloads de mainframe existentes podem ser transferidos para plataformas x86 e modernizadas para aproveitar as extensões nativas de nuvem da AWS Cloud para uma rápida expansão para novos mercados ou regiões.

O padrão de orientação prescritiva da AWS Modernização do mainframe: na DevOps AWS com a Micro Focus introduziu a arquitetura para acelerar o desenvolvimento e o teste de aplicativos de mainframe na AWS usando o Micro Focus Enterprise Developer e o Enterprise Test Server com AWS e AWS. CodePipeline CodeBuild Esse padrão se concentra na implantação de aplicativos de mainframe no ambiente de produção da AWS para alcançar alta disponibilidade e resiliência.

Em um ambiente de produção de mainframe, você pode ter configurado o IBM Parallel Sysplex no mainframe para obter alto desempenho e alta disponibilidade. Para criar uma arquitetura escalável semelhante à Sysplex, a Micro Focus introduziu o Cluster de Desempenho e Disponibilidade (PAC) no Enterprise Server. PACs oferecem suporte à implantação de aplicativos de mainframe em várias regiões do Enterprise Server gerenciadas como uma única imagem e escaladas em instâncias da Amazon EC2 . PACs também oferecem suporte ao desempenho previsível do aplicativo e à taxa de transferência do sistema sob demanda.

Em um PAC, várias instâncias do Enterprise Server trabalham juntas como uma única entidade lógica. A falha de uma instância do Enterprise Server, portanto, não interromperá a continuidade

dos negócios porque a capacidade é compartilhada com outras regiões, enquanto novas instâncias são iniciadas automaticamente usando a funcionalidade padrão do setor, como um grupo Amazon Auto EC2 Scaling. Isso remove pontos únicos de falha, melhorando a resiliência a problemas de hardware, rede e aplicativos. Instâncias escaláveis do Enterprise Server podem ser operadas e gerenciadas usando a Enterprise Server Common Web Administration (ESCWA) APIs, simplificando a manutenção operacional e a capacidade de manutenção dos servidores corporativos.

> **Note**
>
> A Micro Focus recomenda que o Cluster de Desempenho e Disponibilidade (PAC) consista em pelo menos três regiões do Enterprise Server para que a disponibilidade não seja comprometida caso uma região do Enterprise Server falhe ou exija manutenção.

A configuração do PAC requer um serviço de gerenciamento de banco de dados relacional (RDBMS - relational database management service) compatível para gerenciar o banco de dados regional, um banco de dados entre regiões e bancos de dados opcionais de armazenamento de dados. Um banco de dados de armazenamento de dados deve ser usado para gerenciar arquivos do Método de Acesso ao Armazenamento Virtual (VSAM - Virtual Storage Access Method) usando o suporte do Micro Focus Database File Handler para melhorar a disponibilidade e a escalabilidade. RDBMSs Os compatíveis incluem o seguinte:

- Microsoft SQL Server 2009 R2 ou superior
- PostgreSQL 10.x, incluindo o Amazon Aurora Edição Compatível com PostgreSQL
- DB2 10.4 e versões posteriores

Para obter detalhes sobre os requisitos de RDBMS e PAC suportados, consulte Micro Focus Enterprise Server – Pré-requisitos e Micro Focus Enterprise Server – Configuração de PAC recomendada.

O diagrama a seguir mostra uma configuração típica da arquitetura da AWS para uma PAC do Micro Focus.

Componente	Descrição

1	Grupo de escalabilidade automática de instâncias do Enterprise Server	Configure um grupo de escalabilidade automática implantado com instâncias do Enterprise Server em um PAC. O número de instâncias pode ser ampliado ou iniciado pelos CloudWatch alarmes da Amazon usando CloudWatch métricas.
2	Grupo de escalabilidade automática de instâncias ESCWA do Enterprise Server	Configure um grupo de escalabilidade automática implantado com o Enterpris e Server Common Web Administration (ESCWA). A ESCWA fornece gerenciam ento APIs de clusters. Os servidores ESCWA atuam como um ambiente de gerenciamento para adicionar ou remover servidores corporativos e iniciar ou interromper regiões do servidor corporativo no PAC durante os eventos de escalabilidade automática da instância do servidor corporati vo. Como a instância ESCWA é usada somente para o gerenciamento do PAC, seu padrão de tráfego é previsível e o requisito de capacidade desejado de escalabilidade automática pode ser definido como 1.

3	Instância do Amazon Aurora em uma configuração multi-AZ	Configure um sistema de gerenciamento de banco de dados relacional (RDBMS) para hospedar arquivos de dados do usuário e do sistema a serem compartilhados entre as instâncias do Enterprise Server.
4	Instância e réplica da Amazon ElastiCache (Redis OSS)	Configure uma instância primária ElastiCache (Redis OSS) e pelo menos uma réplica para hospedar dados do usuário e atuar como um repositório de expansão (SOR) para as instâncias do Enterprise Server. Você pode configurar um ou mais repositórios de expansão horizontal para armazenar tipos específicos de dados do usuário. O Enterprise Server usa um banco de dados Redis NoSQL como SOR, um requisito para manter a integridade do PAC.
5	Network Load Balancer	Configure um balanceador de carga, fornecendo um nome de host para que os aplicativos se conectem aos serviços fornecidos pelas instâncias do Enterprise Server (por exemplo, acessando o aplicativo por meio de um emulador 3270).

Esses componentes formam o requisito mínimo para um cluster PAC do Micro Focus Enterprise Server. A próxima seção aborda a automação do gerenciamento de clusters.

Usando o AWS Systems Manager Automation para escalabilidade

Depois que o cluster PAC é implantado na AWS, o PAC é gerenciado por meio da Enterprise Server Common Web Administration (ESCWA). APIs

Para automatizar as tarefas de gerenciamento de clusters durante eventos de escalabilidade automática, você pode usar os runbooks do Systems Manager Automation e o Amazon Auto EC2 Scaling com a Amazon. EventBridge A arquitetura dessas automações é mostrada no diagrama a seguir.

	Componente	Descrição
1	Gancho do ciclo de vida de escalabilidade automática	Configure ganchos de ciclo de vida de escalabilidade automática e envie notificaç ões para a Amazon EventBrid ge quando novas instâncias forem lançadas e instâncias existentes forem encerrada s no grupo de escalabilidade automática.
2	Amazon EventBridge	Configure uma EventBridge regra da Amazon para rotear eventos de escalabilidade automática para destinos do runbook do Systems Manager Automation.
3	Runbooks do Automation	Configure os runbooks do Systems Manager Automatio n para executar PowerShell scripts do Windows e invocar o ESCWA APIs para gerenciar

		o PAC. Para obter exemplos, consulte a seção Informações adicionais.
4	Instância ESCWA do Enterpris e Server em um grupo de escalabilidade automática	Configure uma instância ESCWA do Enterprise Server em um grupo de escalabil idade automática. A instância ESCWA fornece APIs o gerenciamento do PAC.

Ferramentas

- Micro Focus Enterprise Server: o Micro Focus Enterprise Server fornece o ambiente de execução para aplicativos criados com qualquer variante de ambiente de desenvolvimento integrado (IDE) do Enterprise Developer.
- Amazon EC2 Auto Scaling — O Amazon EC2 Auto Scaling ajuda você a garantir que você tenha o número correto de instâncias da EC2 Amazon disponíveis para lidar com a carga do seu aplicativo. Você cria coleções de EC2 instâncias, chamadas grupos de Auto Scaling, e especifica os números mínimo e máximo de instâncias.
- Amazon ElastiCache (Redis OSS) — A Amazon ElastiCache é um serviço web para configurar, gerenciar e escalar um armazenamento de dados distribuído na memória ou ambiente de cache na nuvem. Ele fornece uma solução de armazenamento em cache econômica, de alta performance e escalável.
- Amazon RDS: o Amazon Relational Database Service (Amazon RDS) é um serviço Web que facilita a configuração, a operação e escalabilidade de um banco de dados relacional na Nuvem AWS. Ele fornece capacidade econômica e redimensionável para um banco de dados relacional e gerencia tarefas comuns de administração de banco de dados.
- AWS Systems Manager: o AWS Systems Manager é um serviço da AWS que você pode usar para visualizar e controlar sua infraestrutura na AWS. Usando o console do Systems Manager, você pode visualizar dados operacionais de vários serviços da AWS e automatizar tarefas operacionais nos recursos da AWS. O Systems Manager ajuda você a manter a segurança e a conformidade verificando suas instâncias gerenciadas e gerando relatórios (ou tomando medidas corretivas) sobre quaisquer violações de políticas detectadas.

Épicos

Criar uma instância do Amazon Aurora

Tarefa	Descrição	Habilidades necessárias
Crie um CloudFormation modelo da AWS para uma instância do Amazon Aurora.	Use o trecho de código de exemplo da AWS para criar um CloudFormation modelo que criará uma instância de edição compatível com o Amazon Aurora PostgreSQL.	Arquiteto de nuvem
Implante uma CloudFormation pilha para criar a instância do Amazon Aurora.	Use o CloudFormation modelo para criar uma instância compatível com o Aurora PostgreSQL que tenha a replicação Multi-AZ habilitad a para cargas de trabalho de produção.	Arquiteto de nuvem
Defina as configurações de conexão do banco de dados para o Enterprise Server.	Siga as instruções na documentação da Micro Focus para preparar as strings de conexão e a configuração do banco de dados para o Micro Focus Enterprise Server.	Engenheiro de dados, DevOps engenheiro

Crie um ElastiCache cluster da Amazon para a instância do Redis

Tarefa	Descrição	Habilidades necessárias
Crie um CloudFormation modelo para o ElastiCache cluster da Amazon para a instância do Redis.	Use o trecho de código de exemplo da AWS para criar um CloudFormation modelo que criará um ElastiCache	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	cluster da Amazon para a instância do Redis.	
Implante a CloudFormation pilha para criar um ElastiCac he cluster da Amazon para a instância do Redis.	Crie o ElastiCache cluster da Amazon para a instância do Redis que tenha a replicaçã o Multi-AZ habilitada para cargas de trabalho de produção.	Arquiteto de nuvem
Defina as configurações de conexão PSOR do Enterprise Server.	Siga as instruções na documentação da Micro Focus para preparar a configuração de conexão do Repositório escalável do PAC (PSOR - PAC Scale-Out Repository) para o Micro Focus Enterprise Server PAC.	DevOps engenheiro

Crie um grupo de escalabilidade automática ESCWA do Micro Focus Enterprise Server

Tarefa	Descrição	Habilidades necessárias
Crie uma AMI do Micro Focus Enterprise Server.	Crie uma instância EC2 do Amazon Windows Server e instale o binário do Micro Focus Enterprise Server na EC2 instância. Crie uma Amazon Machine Image (AMI) da EC2 instância. Para ter mais informações, consulte a documentação do Micro Focus Enterprise Server.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um CloudFormation modelo para o Enterprise Server ESCWA.	Use o trecho de código de exemplo da AWS para criar um modelo para criar uma pilha personalizada do Enterprise Server ESCWA em um grupo de escalabilidade automática.	Arquiteto de nuvem
Implante a CloudFormation pilha para criar um grupo de EC2 escalabilidade da Amazon para o Enterprise Server ESCWA.	Use o CloudFormation modelo para implantar o grupo de escalabilidade automática com a AMI ESCWA do Micro Focus Enterprise Server criada na história anterior.	Arquiteto de nuvem

Crie um runbook do AWS Systems Manager Automation.

Tarefa	Descrição	Habilidades necessárias
Crie um CloudFormation modelo para um runbook do Systems Manager Automation.	Use os trechos de código de exemplo na seção Informaçõ es adicionais para criar um CloudFormation modelo que criará um runbook do Systems Manager Automation para automatizar a criação de PAC, a expansão do Enterprise Server e a expansão horizonta l do Enterprise Server.	Arquiteto de nuvem
Implante a CloudForm ation pilha que contém o runbook do Systems Manager Automation.	Use o CloudFormation modelo para implantar uma pilha que contém o runbook de automação para criação de PAC, expansão do Enterprise	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Server e expansão horizontal do Enterprise Server.	

Crie um grupo de escalabilidade automática para o Micro Focus Enterprise Server

Tarefa	Descrição	Habilidades necessárias
Crie um CloudFormation modelo para configurar um grupo de escalabilidade automática para o Micro Focus Enterprise Server.	Use o trecho de código de exemplo da AWS para criar um CloudFormation modelo que criará um grupo de escalabilidade automática. Esse modelo reutilizará a mesma AMI que foi criada para a instância ESCWA do Micro Focus Enterprise Server. Em seguida, use um trecho de código de exemplo da AWS para criar o evento de ciclo de vida de escalabil idade automática e configura r EventBridge a Amazon para filtrar eventos de expansão e expansão no mesmo modelo. CloudFormation	Arquiteto de nuvem
Implante a CloudFormation pilha para o grupo de escalabil idade automática para servidores corporativos da Micro Focus.	Implante a CloudFormation pilha que contém o grupo de escalabilidade automática para servidores corporativos da Micro Focus.	Arquiteto de nuvem

Recursos relacionados

- Cluster de desempenho e disponibilidade (PAC) de Micro Focus Enterprise Server
- Ganchos do ciclo de vida do Amazon EC2 Auto Scaling
- Executando automações com gatilhos usando EventBridge

Mais informações

Os cenários a seguir devem ser automatizados para aumentar ou reduzir a escala dos clusters PAC.

Automação para iniciar ou recriar um PAC

No início de um cluster de PAC, o Enterprise Server exige que o ESCWA seja invocado APIs para criar uma configuração de PAC. Isso inicia e adiciona regiões do Enterprise Server ao PAC. Para criar ou recriar um PAC, siga as etapas a seguir:

1. Configure um PAC Scale-Out Repository (PSOR) no ESCWA com um determinado nome.

```
POST /server/v1/config/groups/sors
```

2. Crie um PAC com um determinado nome e anexe o PSOR a ele.

```
POST /server/v1/config/groups/pacs
```

3. Configure o banco de dados da região e o banco de dados entre regiões se for a primeira vez que você estiver configurando uma PAC.

> **Note**
>
> Essa etapa usa consultas SQL e a ferramenta dbhfhadmin de linha de comando do Micro Focus Enterprise Suite para criar o banco de dados e importar os dados iniciais.

4. Instale a definição do PAC nas regiões do Enterprise Server.

```
POST /server/v1/config/mfds
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

5. Inicie as regiões do Enterprise Server no PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

As etapas anteriores podem ser implementadas usando um PowerShell script do Windows.

As etapas a seguir explicam como criar uma automação para criar uma PAC reutilizando o script do Windows PowerShell .

1. Crie um modelo de EC2 lançamento da Amazon que baixe ou crie o PowerShell script do Windows como parte do processo de bootstrap. Por exemplo, você pode usar dados EC2 do usuário para baixar o script de um bucket do Amazon Simple Storage Service (Amazon S3).
2. Crie um runbook do AWS Systems Manager Automation para invocar o script do Windows PowerShell .
3. Associe o runbook à instância ESCWA usando a tag de instância.
4. Criar um grupo de escalabilidade automática ESCWA usando um modelo de execução.

Você pode usar o seguinte exemplo de CloudFormation trecho da AWS para criar o runbook de automação.

Exemplo de CloudFormation trecho de um runbook do Systems Manager Automation usado para criação de PAC

```
PACInitDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to create Enterprise Server PAC
       mainSteps:
       - action: aws:runPowerShellScript
         name: CreatePAC
         inputs:
           onFailure: Abort
           timeoutSeconds: "1200"
           runCommand:
           - |
             C:\Scripts\PAC-Init.ps1
PacInitAutomation:
```

```
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        description: Prepare Micro Focus PAC Cluster via ESCWA Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunPACInitDocument
            action: aws:runCommand
            timeoutSeconds: 300
            onFailure: Abort
            inputs:
              DocumentName: !Ref PACInitDocument
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
  PacInitDocumentAssociation:
    Type: AWS::SSM::Association
    Properties:
      DocumentVersion: "$LATEST"
      Name: !Ref PACInitDocument
      Targets:
        - Key: tag:Enterprise Server - ESCWA
          Values:
            - "true"
```

Para obter mais informações, consulte Micro Focus Enterprise Server – Configurando um PAC.

Automação para expansão horizontal com uma nova instância do Enterprise Server

Quando uma instância do Enterprise Server é expandida, sua região do Enterprise Server deve ser adicionada ao PAC. As etapas a seguir explicam como invocar a ESCWA APIs e adicionar a região do Enterprise Server à PAC.

1. Instale a definição do PAC nas regiões do Enterprise Server.

```
POST '/server/v1/config/mfds'
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

2. Inicie a região em modo de inicialização rápida no PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

3. Adicione a instância do Enterprise Server ao balanceador de carga associando o grupo de escalabilidade automática ao balanceador de carga.

As etapas anteriores podem ser implementadas usando um PowerShell script do Windows. Para obter mais informações, consulte Micro Focus Enterprise Server – Configurando um PAC.

As etapas a seguir podem ser usadas para criar uma automação orientada por eventos para adicionar uma instância recém-lançada do Enterprise Server a uma PAC reutilizando o script do Windows PowerShell .

1. Crie um modelo de EC2 lançamento da Amazon para a instância do Enterprise Server que provisione uma região do servidor corporativo durante sua inicialização. Por exemplo, você pode usar o comando mfds do Micro Focus Enterprise Server para importar uma configuração de região. Para obter mais detalhes e opções disponíveis para esse comando, consulte a Referência do Enterprise Server.
2. Crie um grupo de escalabilidade automática do Enterprise Server que use o modelo de execução criado na etapa anterior.
3. Crie um runbook do Systems Manager Automation para invocar o script do Windows PowerShell .
4. Associe o runbook à instância ESCWA usando a tag de instância.
5. Crie uma EventBridge regra da Amazon para filtrar o evento EC2 Instance Launch Successful para o grupo de escalabilidade automática do Enterprise Server e crie o destino para usar o runbook de automação.

Você pode usar o seguinte exemplo de CloudFormation trecho para criar o runbook de automação e a regra. EventBridge

Exemplo de CloudFormation trecho do Systems Manager usado para escalar instâncias do Enterprise Server

```
ScaleOutDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
```

```
        description: Operation Runbook to Adding MFDS Server into an existing PAC
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        mainSteps:
        - action: aws:runPowerShellScript
          name: Add_MFDS
          inputs:
            onFailure: Abort
            timeoutSeconds: "300"
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-Out.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleOutAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale Out 1 New Server in Micro Focus PAC Cluster via ESCWA
Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
```

```
      - name: RunScaleOutCommand
        action: aws:runCommand
        timeoutSeconds: 300
        onFailure: Abort
        inputs:
          DocumentName: !Ref ScaleOutDocument
          Parameters:
            InstanceIpAddress: "{{InstanceIpAddress}}"
            InstanceId: "{{InstanceId}}"
            MfdsPort: "{{MfdsPort}}"
          Targets:
            - Key: tag:Enterprise Server - ESCWA
              Values:
                - "true"
```

Automação para reduzir a escala horizontalmente em uma instância do Enterprise Server

Semelhante à escalabilidade horizontal, quando uma instância do Enterprise Server é ampliada, o evento EC2 Instance-terminate Lifecycle Action é iniciado e os seguintes processos e chamadas de API são necessários para remover uma instância do Micro Focus Enterprise Server da PAC.

1. Pare a região na instância de encerramento do Enterprise Server.

```
POST "/native/v1/regions/${host_ip}/${port}/${region_name}/stop"
```

2. Remova a instância do servidor corporativo do PAC.

```
DELETE "/server/v1/config/mfds/${uid}"
```

3. Envie um sinal para continuar encerrando a instância do Enterprise Server.

As etapas anteriores podem ser implementadas em um PowerShell script do Windows. Para obter detalhes adicionais sobre esse processo, consulte o documento do Micro Focus Enterprise Server – Administrando uma PAC.

As etapas a seguir explicam como criar uma automação orientada por eventos para encerrar uma instância do Enterprise Server a partir de uma PAC reutilizando o script do Windows. PowerShell

1. Crie um runbook do Systems Manager Automation para invocar o script do Windows PowerShell .
2. Associe o runbook à instância ESCWA usando a tag de instância.

3. Crie um gancho automático do ciclo de vida do grupo de escalabilidade, por EC2 exemplo, encerramento.
4. Crie uma EventBridge regra da Amazon para filtrar o evento EC2 Instance-terminate Lifecycle Action para o grupo de escalabilidade automática do Enterprise Server e crie o destino para usar o runbook de automação.

Você pode usar o CloudFormation modelo de exemplo a seguir para criar um runbook, um gancho de ciclo de vida e uma regra do Systems Manager Automation. EventBridge

Exemplo de CloudFormation trecho de um runbook do Systems Manager Automation usado para escalar em uma instância do Enterprise Server

```
 ScaleInDocument:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Command
      Content:
        schemaVersion: '2.2'
        description: Operation Runbook to Remove MFDS Server from PAC
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        mainSteps:
        - action: aws:runPowerShellScript
          name: Remove_MFDS
          inputs:
            onFailure: Abort
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-In.ps1 -host_ip ${ip} -port {{MfdsPort}}
```

```
  PacScaleInAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale In 1 New Server in Micro Focus PAC Cluster via ESCWA Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleInCommand
            action: aws:runCommand
            timeoutSeconds: "600"
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleInDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                MfdsPort: "{{MfdsPort}}"
                InstanceId: "{{InstanceId}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
          - name: TerminateTheInstance
            action: aws:executeAwsApi
            inputs:
              Service: autoscaling
              Api: CompleteLifecycleAction
              AutoScalingGroupName: !Ref AutoScalingGroup
              InstanceId: "{{ InstanceId }}"
              LifecycleActionResult: CONTINUE
              LifecycleHookName: !Ref ScaleInLifeCycleHook
```

Automação para um gatilho de escalabilidade EC2 automática da Amazon

O processo de configuração de uma política de escalabilidade para instâncias do Enterprise Server requer uma compreensão do comportamento do aplicativo. Na maioria dos casos, você pode configurar políticas de escalabilidade de rastreamento de destino. Por exemplo, você pode usar a média de utilização da CPU como CloudWatch métrica da Amazon para definir a política de escalabilidade automática. Para obter mais informações, consulte Políticas de escalabilidade de rastreamento de metas para o Amazon EC2 Auto Scaling. Para aplicativos que têm padrões de tráfego regulares, considere usar uma política de escalabilidade preditiva. Para obter mais informações, consulte Escalabilidade preditiva para Amazon Auto EC2 Scaling.

Crie um visualizador avançado de arquivos de mainframe na Nuvem AWS

Criado por Boopatia GOPALSAMY (AWS) e Jeremiah O'Connor (AWS)

Resumo

Esse padrão fornece exemplos de código e etapas para ajudá-lo a criar uma ferramenta avançada para navegar e revisar seus arquivos de formato fixo de mainframe usando os serviços de tecnologia sem servidor da AWS. O padrão fornece um exemplo de como converter um arquivo de entrada de mainframe em um documento do Amazon OpenSearch Service para navegação e pesquisa. A ferramenta de visualização de arquivos pode ajudá-lo a conseguir o seguinte:

- Reter a mesma estrutura e layout de arquivos de mainframe para obter consistência em seu ambiente de migração de destino da AWS (por exemplo, você pode manter o mesmo layout para arquivos em um aplicativo em lote que transmite arquivos para terceiros)
- Acelerar o desenvolvimento e os testes durante a migração do mainframe
- Apoiar as atividades de manutenção após a migração

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) com uma sub-rede acessível por sua plataforma legada
-
> **Note**
>
> Um arquivo de entrada e seu caderno correspondente de linguagem orientada a negócios (COBOL) (: Para obter exemplos de arquivos de entrada e cadernos COBOL, consulte no repositório. gfs-mainframe-solutions GitHub Para obter mais informações sobre os copybooks do COBOL, consulte o Guia de Programação do Enterprise COBOL for z/OS 6.3 no site da IBM.)

Limitações

- A análise do copybook é limitada a não mais do que dois níveis aninhados (OCCURS)

Arquitetura

Pilha de tecnologia de origem

- Arquivos de entrada no formato FB (Fixed Blocked)
- Layout de cadernos em COBOL

Pilha de tecnologias de destino

- Amazon Athena
- OpenSearch Serviço Amazon
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS Step Functions

Arquitetura de destino

O diagrama a seguir mostra o processo de análise e conversão de um arquivo de entrada de mainframe em um documento de OpenSearch serviço para navegação e pesquisa.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário administrador ou aplicativo envia os arquivos de entrada para um bucket do S3 e os copybooks do COBOL para outro bucket do S3.
2.
> **Note**
>
> O bucket do S3 com os arquivos de entrada invoca uma função do Lambda que inicia um fluxo de trabalho de Step Functions de tecnologia sem servidor. : o uso de um acionador de eventos do S3 e da função Lambda para impulsionar o fluxo de trabalho do Step Functions nesse padrão é opcional. Os exemplos de GitHub código nesse padrão não incluem o uso desses serviços, mas você pode usá-los com base em seus requisitos.

3. O fluxo de trabalho do Step Functions coordena todos os processos em lote das seguintes funções do Lambda:
   - A função `s3copybookparser.py` analisa o layout do caderno e extrai atributos de campo, tipos de dados e deslocamentos (necessários para o processamento de dados de entrada).

- A função `s3toathena.py` cria um layout de tabela do Athena. O Athena analisa os dados de entrada que são processados pela função `s3toathena.py` e os converte em um arquivo CSV.
- A `s3toelasticsearch.py` função ingere o arquivo de resultados do bucket do S3 e envia o arquivo para o Service. OpenSearch

4. Os usuários acessam os OpenSearch painéis com o OpenSearch Service para recuperar os dados em vários formatos de tabela e coluna e, em seguida, executar consultas nos dados indexados.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que ajuda na análise de dados diretamente no Amazon Simple Storage Service (Amazon S3) usando SQL padrão.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado. Nesse padrão, você usa o Lambda para implementar a lógica central, como analisar arquivos, converter dados e carregar dados no OpenSearch Service para acesso interativo a arquivos.
- O Amazon OpenSearch Service é um serviço gerenciado que ajuda você a implantar, operar e escalar clusters de OpenSearch serviços na nuvem da AWS. Nesse padrão, você usa o OpenSearch Service para indexar os arquivos convertidos e fornecer recursos de pesquisa interativa para os usuários.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Step Functions é um serviço de orquestração de tecnologia sem servidor que permite combinar funções do Lambda e outros serviços da AWS para criar aplicações essenciais aos negócios. Nesse padrão, você usa o Step Functions para orquestrar funções do Lambda.

Outras ferramentas

- GitHubé um serviço de hospedagem de código que fornece ferramentas de colaboração e controle de versão.
- O Python é uma linguagem de programação de alto nível.

Código

O código desse padrão está disponível no GitHub gfs-mainframe-patternsrepositório.

Épicos

Preparar o ambiente de destino

Tarefa	Descrição	Habilidades necessárias
Crie o bucket do S3.	Crie um bucket S3 para armazenar os cadernos, arquivos de entrada e arquivos de saída. Recomendamos a seguinte estrutura de pastas para seu bucket do S3: • `copybook/` • `input/` • `output/` • `query/` • `results/`	AWS geral
Crie a função s3copyboo kparser.	1. Crie uma função Lambda chamada `s3copyboo kparser` e faça o upload do código-fonte (`s3copybookparser.p y` `ecopybook.py`) do GitHubrepositório.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	2. Anexe a política do IAM `S3ReadOnly` à função do Lambda.	
Crie a função s3toathena.	1. Crie uma função Lambda chamada `s3toathena` e faça o upload do código-fonte (`s3toathena.py`) do GitHubrepositório. Configure o tempo limite do Lambda para > 60 segundos. 2. Para fornecer acesso aos recursos necessários, vincule `AmazonAthenaFullAccess` às políticas do IAM e `S3FullAccess` à função do Lambda.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie a função s3toelasticsearch.	1. **Important** Adicione uma dependência do Python ao seu ambiente Lambda. : Para usar a `s3toelasticsearch` função, você deve adicionar a dependência do Python porque a função Lambda usa dependências do cliente do Python Elasticsearch (e). `Elasticsearch==7.9.0 requests_aws4auth` 2. Crie uma função Lambda chamada `s3toelasticsearch` e faça o upload do código-fonte (`s3toelasticsearch.py`) do GitHubrepositório. 3. Importe a dependência do Python como uma camada do Lambda. 4. Vincule `S3ReadOnly` às políticas do IAM e `AmazonOpenSearchSe`	AWS geral

Tarefa	Descrição	Habilidades necessárias
	`rviceReadOnlyAcces s` à função do Lambda.	

Tarefa	Descrição	Habilidades necessárias
Crie o cluster OpenSearch de serviços.	Criar um cluster 1. Crie um cluster OpenSearch de serviços. Ao criar o cluster, faça o seguinte: • **Note** Crie um usuário mestre e uma senha para o cluster que você pode usar para entrar nos OpenSearch painéis. : Essa etapa não é necessária se você usa a autenticação por meio do Amazon Cognito. • Escolha o controle de acesso detalhado. Isso oferece formas adicionais de controlar o acesso aos seus dados no OpenSearch Serviço. 2. Copie o URL do domínio e passe-o como a variável de ambiente 'HOST' para a função do Lambda `s3toelasticsearch` .	AWS geral

Tarefa	Descrição	Habilidades necessárias
	Conceder acesso ao perfil do IAM Para fornecer acesso refinado ao perfil do IAM (`arn:aws:iam::**:role/service-role/s3toelasticsearch-role-**`) da função Lambda, faça o seguinte: 1. Faça login no OpenSearch Dashboards como usuário principal. 2. Escolha a guia Segurança e, em seguida, escolha Perfis, all_access, Mapear usuário, perfis de backend. 3. Adicione o nome do recurso da Amazon (ARN) do perfil do IAM da função do Lambda e escolha Salvar. Para obter mais informações, consulte Mapeamento de funções para usuários na documentação do OpenSearch Serviço.	

Tarefa	Descrição	Habilidades necessárias
Crie Step Functions para orquestração.	1. Crie uma máquina de estado do Step Functions com o fluxo padrão. A definição está incluída no GitHub repositório. 2. No script JSON, substitua as funções Lambda pelas ARNs da função ARNs Lambda em seu ambiente.	AWS geral

Implemente e execute

Tarefa	Descrição	Habilidades necessárias
Carregue os arquivos de entrada e os cadernos para seu bucket do S3.	Faça o download dos arquivos de amostra da pasta de amostra do GitHub repositório e faça o upload dos arquivos para o bucket do S3 que você criou anteriormente. 1. Carregue `Mockedcopy.cpy` e `acctix.cpy` na pasta `<S3_Bucket>/copybook` . 2. Faça upload dos arquivos de entrada `Modedupdate.txt` e `acctindex.cpy` da amostra para a pasta `<S3_Bucket>/input`.	AWS geral
chame o Step Functions.	1. Faça login no Console de Gerenciamento da AWS	AWS geral

Tarefa	Descrição	Habilidades necessárias

	e abra o console do Step Functions.
	2. No painel de navegação, escolha Máquinas de estado.
	3. Escolha sua máquina de estado e, em seguida, escolha Iniciar execução.
	4. Na caixa Entrada, insira o seguinte caminho de caderno/arquivo como uma variável JSON para o bucket do S3 e escolha Iniciar execução.
	
	`{ "s3_copybook_bucket_name": "<BUCKET NAME>", "s3_copybook_bucket_key": "<COPYBOOK PATH>", "s3_source_bucket_name": "<BUCKET NAME", "s3_source_bucket_key": "INPUT FILE PATH" }`
	
	Por exemplo:
	
	`{ "s3_copybook_bucket_name": "fileaidtest",`	

Tarefa	Descrição	Habilidades necessárias

	<pre>"s3_copybook_bucke
	t_key": "copybook/
	acctix.cpy",
	"s3_source_bucket_
	name": "fileaidtest",
	"s3_source_bucket_
	key": "input/ac
	ctindex"
	}</pre>	

Valide a execução do fluxo de trabalho em Step Functions.	No console Step Functions, revise a execução do fluxo de trabalho no inspetor gráfico. Os estados de execução são codificados por cores para representar o status da execução. Por exemplo, azul indica Em andamento , verde indica Sucesso e vermelho indica Falha. Você também pode revisar a tabela na seção Histórico de eventos de execução para obter informações mais detalhadas sobre os eventos de execução. Para obter um exemplo de execução gráfica do fluxo de trabalho, consulte o gráfico Step Functions na seção Informações adicionais desse padrão.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Valide os registros de entrega na Amazon CloudWatch.	1. Faça login no Console de Gerenciamento da AWS e abra o console do CloudWatch . 2. No painel de navegação , expanda Logs e, em seguida, escolha Grupos de log. 3. Na caixa de pesquisa, pesquise o grupo de logs do perfil `s3toelasticsearch` . Para ver um exemplo de registros de entrega bem-sucedidos, consulte os registros de CloudWatch entrega na seção Informações adicionais desse padrão.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Valide o arquivo formatado nos OpenSearch painéis e execute operações de arquivo.	1. Faça login no Console de Gerenciamento da AWS. Em Analytics, escolha Amazon OpenSearch Service. 2. No painel de navegação à esquerda, escolha Domínios. 3. Na caixa de pesquisa, insira o URL do seu domínio em OpenSearch Painéis. 4. Escolha seu painel e, em seguida, faça login como usuário principal. 5. Procure os dados indexados em formato de tabela. 6. Compare o arquivo de entrada com o arquivo de saída formatado (documento indexado) nos OpenSearch painéis. A visualização do painel mostra os cabeçalhos de coluna adicionados aos seus arquivos formatados. Confirme se os dados de origem dos seus arquivos de entrada não formatados correspondem aos dados de destino na visualização do painel. 7. Execute ações como pesquisa (por exemplo,	AWS geral

Tarefa	Descrição	Habilidades necessárias
	usando nomes de campo, valores ou expressões), filtro e operações de DQL (Dashboard Query Language) em relação ao arquivo indexado.	

Recursos relacionados

Referências

- Exemplo de copybook COBOL (documentação da IBM)
- BMC Compuware File-AID (documentação da BMC)

Tutoriais

- Tutorial: Uso de um acionador do Amazon S3 para invocar uma função do Lambda (documentação do AWS Lambda)
- Como faço para criar um fluxo de trabalho de tecnologia sem servidor com o AWS Step Functions e o AWS Lambda (documentação da AWS)
- Usando OpenSearch painéis com o Amazon OpenSearch Service (documentação da AWS)

Mais informações

Gráfico de Step Functions

O exemplo a seguir mostra um gráfico do Step Functions. O gráfico mostra o status da execução das funções do Lambda usadas nesse padrão.

CloudWatch registros de entrega

O exemplo a seguir mostra registros de entrega bem-sucedidos para a execução da execução `s3toelasticsearch`.

2022-08-10T15:53:33.033-05:00	Número de documentos de processamento: 100	
	2022-08-10T15:53:33.171-05:00	[INFO] 2022-08-10T 20:53:33, 171 Z a1b2c3d4-5678-90ab-cdef- POST:443/_bulk [status: 200 solicitação: 0,100s] EXAMPLE11111 https://search-essearch-3h4uqclifeqaj2vg4mphe7ffle.us-east-2.es.amazonaws.com
	2022-08-10T15:53:33.172-05:00	Gravação em massa bem-sucedida: 100 documentos

Containerize workloads de mainframe que foram modernizadas pela Blu Age

Criado por Richard Milner-Watts (AWS)

Resumo

Esse padrão fornece um ambiente de contêiner de exemplo para executar workloads de mainframe que foram modernizadas com o uso da ferramenta Blu Age. O Blu Age converte workloads antigas de mainframe em código Java moderno. Esse padrão fornece um encapsulamento ao redor da aplicação Java para que você possa executá-la usando os serviços de orquestração de contêiner, como Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS).

Para obter mais informações sobre a modernização de suas workloads usando o Blu Age e os serviços da AWS, consulte estas publicações de Recomendações da AWS:

- Executar workloads modernizadas de mainframe Blu Age em uma infraestrutura AWS de tecnologia sem servidor
- Implemente um ambiente para aplicativos Blu Age em contêineres usando o Terraform

Para obter ajuda com o uso do Blu Age para modernizar suas workloads de mainframe, entre em contato com a equipe da Blu Age selecionando Entrar em contato com nossos especialistas no site da Blu Age. Para obter ajuda para migrar suas workloads modernizadas para a AWS, integrá-las aos serviços da AWS e colocá-las em produção, entre em contato com seu gerente de contas da AWS ou preencha o formulário AWS Professional Services.

Pré-requisitos e limitações

Pré-requisitos

- Um aplicativo Java modernizado que foi criado pela Blu Age. Para fins de teste, esse padrão fornece um exemplo de aplicativo Java que você poderá usar como prova de conceito.
- Um ambiente Docker que você poderá usar para criar o contêiner.

Limitações

Dependendo da plataforma de orquestração de contêineres que você usa, os recursos que podem ser disponibilizados para o contêiner (como CPU, RAM e armazenamento) podem ser limitados. Por exemplo, se você estiver usando o Amazon ECS com o AWS Fargate, consulte a documentação do Amazon ECS para ver os limites e considerações.

Arquitetura

Pilha de tecnologia de origem

- Blu Age
- Java

Pilha de tecnologias de destino

- Docker

Arquitetura de destino

O diagrama a seguir mostra a arquitetura de uma aplicação em Blu Age dentro de um contêiner do Docker.

1. O ponto de entrada para o contêiner é o script do encapsulamento. Esse script bash é responsável por preparar o ambiente de runtime para o aplicativo Blu Age e processar as saídas.
2. As variáveis de ambiente no contêiner são usadas para configurar variáveis no script do encapsulamento, como os nomes de bucket do Amazon Simple Storage Service (Amazon S3) e as credenciais do banco de dados. As variáveis de ambiente são fornecidas pelo AWS Secrets Manager ou pelo Parameter Store, um recurso do AWS Systems Manager. Se você estiver usando o Amazon ECS como seu serviço de orquestração de contêineres, você também poderá codificar as variáveis de ambiente na definição de tarefas do Amazon ECS.
3. O script wrapper é responsável por puxar todos os arquivos de entrada do bucket do S3 para o contêiner antes de você executar o aplicativo Blu Age. A AWS Command Line Interface (AWS CLI) foi instalada no contêiner. Isso fornece um mecanismo para acessar objetos que são armazenados no Amazon S3 por meio do endpoint de nuvem privada virtual (VPC) do gateway.
4. O arquivo Java Archive (JAR) do aplicativo Blu Age poderá precisar se comunicar com outras fontes de dados, como o Amazon Aurora.

5. Após a conclusão, o script do wrapper entrega os arquivos de saída resultantes em um bucket do S3 para processamento adicional (por exemplo, pelos serviços de CloudWatch registro da Amazon). O padrão também suporta a entrega de arquivos de log compactados para o Amazon S3, se você estiver usando uma alternativa ao CloudWatch registro padrão.

Ferramentas

Serviços da AWS

- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.

Ferramentas

- O Docker é uma plataforma de software para criar, testar e implantar aplicativos. O Docker empacota o software em unidades padronizadas chamadas contêineres, que têm tudo o que o software precisa para ser executado, incluindo bibliotecas, ferramentas do sistema, código e runtime. Você poderá usar o Docker para implantar e dimensionar aplicações em qualquer ambiente.
- O Bash é uma interface de linguagem de comando (shell) para o sistema operacional GNU.
- Java é a linguagem de programação e o ambiente de desenvolvimento usados nesse padrão.
- O Blu Age é uma ferramenta de AWS Mainframe Modernization que converte workloads antigas de mainframe, incluindo código de aplicativo, dependências e infraestrutura, em workloads modernas para a nuvem.

Repositório de código

O código desse padrão está disponível no repositório de contêineres de amostras do GitHub Blu Age.

Práticas recomendadas

- Externalize as variáveis para alterar o comportamento do seu aplicativo usando variáveis de ambiente. Essas variáveis permitem que a solução de orquestração de contêineres altere o

ambiente de runtime sem reconstruir o contêiner. Esse padrão inclui exemplos de variáveis de ambiente que podem ser úteis para aplicativos Blu Age.

- Valide todas as dependências do aplicativo antes de executar seu aplicativo Blu Age. Por exemplo, verifique se o banco de dados está disponível e se as credenciais são válidas. Escreva testes no script de encapsulamento para verificar as dependências e que apresente falhas com antecedência, caso não sejam atendidas.
- Use o login detalhado no script do encapsulamento. Interagir diretamente com um contêiner em execução poderá ser um desafio, dependendo da plataforma de orquestração e da duração do trabalho. Certifique-se de que uma saída útil seja gravada em `STDOUT` para ajudar a diagnosticar quaisquer problemas. Por exemplo, a saída poderá incluir o conteúdo do diretório de trabalho do aplicativo antes e depois da execução do aplicativo.

Épicos

Obtenha um arquivo JAR do aplicativo Blu Age

Tarefa	Descrição	Habilidades necessárias
Opção 1: trabalhe com o Blu Age para obter o arquivo JAR de seu aplicativo.	O contêiner nesse padrão requer um aplicativo Blu Age. Como alternativa, você poderá usar o aplicativo Java de exemplo fornecido com esse padrão para um protótipo. Trabalhe com a equipe do Blu Age para obter um arquivo JAR para seu aplicativo que possa ser incorporado ao contêiner. Se o arquivo JAR não estiver disponível, consulte a próxima tarefa para usar o aplicativo de exemplo em vez disso.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Opção 2: crie ou use o arquivo JAR do aplicativo de exemplo fornecido.	Esse padrão fornece um arquivo JAR de exemplo pré-construído. Esse arquivo envia as variáveis de ambiente do aplicativo para STD0UT antes de entrar em repouso por 30 segundos e sair. Esse arquivo tem um nome `bluAgeSample.jar` e está localizado na pasta docker do GitHub repositório. Se você quiser alterar o código e criar sua própria versão do arquivo JAR, use o código-fonte localizado em. /java_ sample/src/sample _java_app.java no repositór io. GitHub Você poderá usar o script de construção em ./ java_sample/build.sh para compilar o código-fonte Java e criar um novo arquivo JAR.	Desenvolvedor de aplicativos

Construa o contêiner Blu Age

Tarefa	Descrição	Habilidades necessárias
Clone o GitHub repositório.	Clone o repositório de códigos de exemplo usando o comando: `git clone https://g ithub.com/aws-samp`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`les/aws-blu-age-sa mple-container`	
Use o Docker para criar o contêiner.	Use o Docker para criar o contêiner antes de enviá-lo para um registro do Docker, como o Amazon ECR: 1. No terminal escolhido, navegue até a `docker` pasta dentro do seu GitHub repositório local. 2. Use este comando para criar o contêiner: `docker build -t <tag> .` em que `<tag>` é o nome do contêiner que você deseja usar.	AWS DevOps
Teste o contêiner Blu Age.	(Opcional) Se necessário, teste o contêiner localmente usando o comando: `docker run -it <tag> / bin/bash`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Autentique-se no seu repositório Docker.	Se você planeja usar o Amazon ECR, siga as instruções na documentação do Amazon ECR para instalar e configurar a AWS CLI e autenticar o CLI do Docker em seu registro padrão. Recomendamos que você use o get-login-password comando para autenticação. **Note** O console do Amazon ECR fornece uma versão pré-preenchida desse comando se você usar o botão Exibir comandos push. Para obter mais informações, consulte a documentação do Amazon ECR. `aws ecr get-login-password --region <region> | docker login --username AWS --password-stdin <account>.dkr.ecr.<region>.amazonaws.com`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Se você não planeja usar o Amazon ECR, siga as instruções fornecidas para seu sistema de registro de contêineres.	
Crie um repositório de contêineres.	Crie um repositório do Amazon ECR. Para obter instruções, consulte o padrão Implemente um ambiente para aplicativos Blu Age em contêineres usando o Terraform. Se você estiver usando outro sistema de registro de contêiner, siga as instruções fornecidas para esse sistema.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Marque e envie seu contêiner para o repositório de destino.	Se você estiver usando o Amazon ECR:
	1. Marque a imagem do Docker local com o registro e o repositório do Amazon ECR, para que você possa enviá-la para seu repositór io remoto:
	`docker tag <tag>:lat est <account> .dkr.ecr.<region>. amazonaws.com/<rep ository>:<versionN umber>`
	2. Envie a imagem ao repositório remoto:
	`docker push <account> .dkr.ecr.<region>. amazonaws.com/<rep ository>:<versionN umber>`
	Para obter mais informaçõ es, consulte Envio de uma imagem do Docker no Guia do usuário do Amazon ECR.
		AWS DevOps

Recursos relacionados

Recursos da AWS

- Repositório de contêineres de exemplo do AWS Blu Age

- Executar workloads modernizadas de mainframe Blu Age em uma infraestrutura AWS de tecnologia sem servidor
- Implemente um ambiente para aplicativos Blu Age em contêineres usando o Terraform
- Usar o Amazon ECR com a AWS CLI (Guia do usuário do Amazon ECR)
- Autenticação de registro privado (Guia do usuário do Amazon ECR)
- Documentação do Amazon ECS
- Documentação do Amazon EKS

Recursos adicionais

- Site da Blu Age
- Site do Docker

Converta e descompacte dados EBCDIC em ASCII na AWS usando Python

Criado por Luis Gustavo Dantas (AWS)

Resumo

Como os mainframes normalmente hospedam dados comerciais críticos, a modernização dos dados é uma das tarefas mais importantes ao migrar dados para a nuvem da Amazon Web Services (AWS) ou outro ambiente do American Standard Code for Information Interchange (ASCII). Em mainframes, os dados geralmente são codificados no formato EBCDIC (código de intercâmbio decimal codificado por código binário estendido). A exportação de banco de dados, VSAM (Virtual Storage Access Method) ou arquivos simples geralmente produz arquivos EBCDIC binários compactados, que são mais complexos de migrar. A solução de migração de banco de dados mais usada é a captura de dados de alteração (CDC), que, na maioria dos casos, converte automaticamente a codificação de dados. No entanto, os mecanismos do CDC podem não estar disponíveis para esses bancos de dados, VSAM ou arquivos simples. Para esses arquivos, é necessária uma abordagem alternativa para modernizar os dados.

Esse padrão descreve como modernizar os dados EBCDIC convertendo-os para o formato ASCII. Após a conversão, você pode carregar os dados em bancos de dados distribuídos ou fazer com que aplicativos na nuvem processem os dados diretamente. O padrão usa o script de conversão e os arquivos de amostra no mainframe-data-utilities GitHub repositório.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um arquivo de entrada EBCDIC e seu copybook correspondente de linguagem comum orientada a negócios (COBOL). Um arquivo EBCDIC de amostra e um caderno COBOL estão incluídos no repositório. mainframe-data-utilities GitHub Para obter mais informações sobre os copybooks de COBOL, consulte o Guia de Programação do Enterprise COBOL for z/OS 6.4 no site da IBM.

Limitações

- Os layouts de arquivo definidos nos programas COBOL não são suportados. Eles devem ser disponibilizados separadamente.

Versões do produto

- Python, versão 3.8 ou superior

Arquitetura

Pilha de tecnologia de origem

- Dados EBCDIC em um mainframe
- Copybook de COBOL

Pilha de tecnologias de destino

- Instância do Amazon Elastic Compute Cloud (Amazon EC2) em uma nuvem privada virtual (VPC)
- Amazon Elastic Block Store (Amazon EBS)
- Python e seus pacotes necessários, JavaScript Object Notation (JSON), sys e datetime
- Arquivo plano ASCII pronto para ser lido por um aplicativo moderno ou carregado em uma tabela de banco de dados relacional

Arquitetura de destino

O diagrama de arquitetura mostra o processo de conversão de um arquivo EBCDIC em um arquivo ASCII em uma instância: EC2

1. Usando o script parse_copybook_to_json.py, você converte o copybook de COBOL em um arquivo JSON.
2. Usando o arquivo JSON e o script extract_ebcdic_to_ascii.py, você converte os dados EBCDIC em um arquivo ASCII.

Automação e escala

Depois que os recursos necessários para as primeiras conversões manuais de arquivos estiverem disponíveis, você poderá automatizar a conversão de arquivos. Esse padrão não inclui instruções para automação. Há várias maneiras de automatizar a conversão. Veja abaixo uma visão geral de uma possível abordagem:

1. Encapsular os comandos do AWS Command Line Interface (AWS CLI) e os comandos de script do Python em um script de shell.
2. Crie uma função do AWS Lambda que envie de forma assíncrona o trabalho de script de shell em uma instância. EC2 Para obter mais informações, consulte Agendamento de trabalhos de SSH usando o AWS Lambda.
3. Crie um acionador do Amazon Simple Storage Service (Amazon S3) que invoque a função do Lambda toda vez que um arquivo legado for carregado. Para obter mais informações, consulte Como usar um trigger do Amazon S3 para invocar uma função do Lambda.

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (Amazon). EC2
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

Outras ferramentas

- GitHubé um serviço de hospedagem de código que fornece ferramentas de colaboração e controle de versão.
- O Python é uma linguagem de programação de alto nível.

Repositório de código

O código desse padrão está disponível no mainframe-data-utilities GitHub repositório.

Épicos

Prepare a EC2 instância

Tarefa	Descrição	Habilidades necessárias
Execute uma EC2 instância.	A EC2 instância deve ter acesso de saída à Internet. Isso permite que a instância acesse o código-fonte do Python disponível em. GitHub Para criar a instância: 1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2. 2. Execute uma instância EC2 Linux. Use um endereço IP público e permita o acesso de entrada pela porta 22. Certifique-se de que o tamanho de armazenam ento da instância seja pelo menos o dobro do tamanho do arquivo de dados EBCDIC. Para obter instruções, consulte a EC2 documentação da Amazon.	AWS geral
Instale o Git.	1. Usando um cliente de shell seguro (SSH), conecte-se à EC2 instância que você acabou de iniciar. Para obter mais informações, consulte Conectar-se à instância do Linux.	AWS geral, Linux

Tarefa	Descrição	Habilidades necessárias

	2. No EC2 console da Amazon, execute o seguinte comando. Isso instala o Git na EC2 instância.
	`sudo yum install git`
	3. Execute o seguinte comando e confirme que o Git foi instalado com êxito.
	`git --version`	

Tarefa	Descrição	Habilidades necessárias

Instalar o Python.	1. No EC2 console da Amazon, execute o seguinte comando. Isso instala o Python na EC2 instância.
	`sudo yum install python3`
	2. No EC2 console da Amazon, execute o seguinte comando. Isso instala o Pip3 na instância. EC2
	`sudo yum install python3-pip`
	3. No EC2 console da Amazon, execute o seguinte comando. Isso instala o SDK da AWS para Python (Boto3) (Boto3) na instância. EC2
	`sudo pip3 install boto3`
	4. No EC2 console da Amazon, execute o comando a seguir, onde `<us-east-1>` está o código da sua região da AWS. Para obter uma lista completa dos códigos de região, consulte Regiões
		AWS geral, Linux

Tarefa	Descrição	Habilidades necessárias
	disponíveis na EC2 documentação da Amazon. `export AWS_DEFAU LT_REGION=<us-east -1>`	
Clone o GitHub repositório.	1. No EC2 console da Amazon, execute o seguinte comando. Isso clona o mainframe-data-utilitiesrepositório GitHub e abre o local de cópia padrão, a home pasta. `git clone https://g ithub.com/aws-samp les/mainframe-data- utilities.git` 2. Na pasta home, confirme se a pasta `mainframe-data-utilities` está presente.	AWS geral, GitHub

Crie o arquivo ASCII a partir dos dados EBCDIC

Tarefa	Descrição	Habilidades necessárias
Analise o copybook de COBOL no arquivo de layout JSON.	Dentro da pasta `mainframe -data-utilities` , execute o script parse_cop ybook_to_json.py. Esse módulo de automação lê o layout do arquivo de um copybook de COBOL e cria	AWS geral, Linux

Tarefa	Descrição	Habilidades necessárias

	um arquivo JSON. O arquivo JSON contém as informaçõ es necessárias para interpret ar e extrair os dados do arquivo de origem. Isso cria os metadados JSON do copybook de COBOL.
	
	O comando a seguir converte o copybook de COBOL em um arquivo JSON.
	
	`python3 parse_cop ybook_to_json.py \ -copybook LegacyRef erence/COBPACK2.cpy \ -output sample-data/ cobpack2-list.json \ -dict sample-data/ cobpack2-dict.json \ -ebcdic sample-data/ COBPACK.OUTFILE.txt \ -ascii sample-data/ COBPACK.ASCII.txt \ -print 10000`
	
	O script imprime os argumento s recebidos.
	
	`---------- ---------- ---------- ---------- Copybook file..... .....| LegacyRef erence/COBPACK2.cpy Parsed copybook (JSON List).| sample-data/ cobpack2-list.json`	

Tarefa	Descrição	Habilidades necessárias
	``` JSON Dict (document ation)...| sample-da ta/cobpack2-dict.json ASCII file..... .....| sample- data/COBPACK.ASCII.t xt EBCDIC file..... .....| sample- data/COBPACK.OUTFILE .txt Print each..... .....| 10000 ---------- ---------- ---------- ---------- ---------- ```	

Para obter mais informações sobre os argumentos, consulte o arquivo README no GitHub repositório.

Tarefa	Descrição	Habilidades necessárias
Inspecione o arquivo de layout JSON.	1. Navegue até o caminho de saída definido no script parse_copybook_to_json.py. 2. Verifique o horário de criação do arquivo sample-data/cobpack2-list.json para confirmar se você selecionou o arquivo de layout JSON apropriado. 3. Examine o arquivo JSON e confirme se o conteúdo é semelhante ao seguinte. `"input": "extract-ebcdic-to-ascii/COBPACK.OUTFILE.txt", "output": "extract-ebcdic-to-ascii/COBPACK.ASCII.txt", "max": 0, "skip": 0, "print": 10000, "lrecl": 150, "rem-low-values": true, "separator": "|", "transf": [ { "type": "ch", "bytes": 19, "name": "OUTFILE-TEXT" }`	AWS geral, JSON

Tarefa	Descrição	Habilidades necessárias
	Os atributos mais important es do arquivo de layout JSON são: • `input`: contém o caminho do arquivo EBCDIC a ser convertido • `output`: define o caminho em que o arquivo ASCII será gerado • `lrecl`: especifica o tamanho em bytes do tamanho do registro lógico • `transf`: lista todos os campos e seu tamanho em bytes Para obter mais informaçõ es sobre o arquivo de layout JSON, consulte o arquivo README no GitHub repositór io.	

Tarefa	Descrição	Habilidades necessárias

Criar o arquivo ASCII.	Execute o script extract_ebcdic_to_ascii.py, que está incluído no GitHub repositório clonado. Esse script lê o arquivo EBCDIC e grava um arquivo ASCII convertido e legível.
	`python3 extract_ebcdic_to_ascii.py -local-json sample-data/cobpack2-list.json`
	Conforme o script processa os dados do EBCDIC, ele imprime uma mensagem para cada lote de 10.000 registros. Veja o exemplo a seguir.
	`---------- 2023-05-15 21:21:46.322253 | Local Json file | -local-json | sample-data/cobpack2-list.json 2023-05-15 21:21:47.034556 | Records processed | 10000 2023-05-15 21:21:47.736434 | Records processed | 20000 2023-05-15 21:21:48.441696 | Records processed | 30000`
		AWS geral

Tarefa	Descrição	Habilidades necessárias
	2023-05-15 21:21:49. 173781 | Records processed | 40000 2023-05-15 21:21:49. 874779 | Records processed | 50000 2023-05-15 21:21:50. 705873 | Records processed | 60000 2023-05-15 21:21:51. 609335 | Records processed | 70000 2023-05-15 21:21:52. 292989 | Records processed | 80000 2023-05-15 21:21:52. 938366 | Records processed | 89280 2023-05-15 21:21:52. 938448 Seconds 6.616232 Para obter informações sobre como alterar a frequência de impressão, consulte o arquivo README no GitHub repositór io.	

Tarefa	Descrição	Habilidades necessárias
Examinar o arquivo ASCII.	1. Verifique a hora de criação do arquivo extract-ebcdic-to-ascii/COBPACK.ASCII.txt para verificar se ele foi criado recentemente. 2. No EC2 console da Amazon, insira o seguinte comando. Isso abre o primeiro registro do arquivo ASCII. `head sample-data/COBPACK.ASCII.txt -n 1| xxd` 3. Examine o conteúdo do primeiro registro. Como os arquivos EBCDIC geralmente são binários, eles não têm caracteres especiais de retorno de carro e alimentação de linha (CRLF). O script extract_ebcdic_to_ascii.py adiciona um caractere de barra vertical como separador de colunas, que é definido nos parâmetros do script. Se você usou o arquivo EBCDIC de amostra fornecido, o seguinte é o primeiro registro no arquivo ASCII.	AWS geral, Linux

Tarefa	Descrição	Habilidades necessárias
	00000000: 2d30 3030 3030 3030 3030 3130 3030 3030 -000000000100000 00000010: 3030 307c 3030 3030 3030 3030 3031 3030 000|00000 0000100 00000020: 3030 3030 3030 7c2d 3030 3030 3030 3030 000000|-0 0000000 00000030: 3031 3030 3030 3030 3030 7c30 7c30 7c31 0100000000| 0|0|1 00000040: 3030 3030 3030 3030 7c2d 3130 3030 3030 00000000| -100000 00000050: 3030 307c 3130 3030 3030 3030 307c 2d31 000|10000 0000|-1 00000060: 3030 3030 3030 3030 7c30 3030 3030 7c30 00000000| 00000|0 00000070: 3030 3030 7c31 3030 3030 3030 3030 7c2d 0000|1000 00000|- 00000080: 3130 3030 3030 3030 307c 3030 3030 3030 100000000| 000000 00000090: 3030 3030 3130 3030 3030 3030 307c 2d30 000010000 0000|-0 000000a0: 3030 3030 3030 3030 3031 3030	

Tarefa	Descrição	Habilidades necessárias
	3030 3030 000000000 1000000 000000b0: 3030 7c41 7c41 7c0a 00|A|A|.	

Tarefa	Descrição	Habilidades necessárias
Avalie o arquivo EBCDIC.	No EC2 console da Amazon, insira o seguinte comando. Isso abre o primeiro registro do arquivo EBCDIC. `head sample-data/COBPACK.OUTFILE.txt -c 150 | xxd` Se você usou o arquivo EBCDIC de amostra, o resultado é o seguinte. `00000000: 60f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 f0f0 `........ ....` `00000010: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 ....` `00000020: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 ....` `00000030: f0f0 f0f0 f0f0 d000 0000 0005 f5e1 00fa ....` `00000040: 0a1f 0000 0000 0005 f5e1 00ff ffff fffa ....` `00000050: 0a1f 0000 000f 0000 0c10 0000 000f 1000 ....` `00000060: 0000 0d00 0000 0000 1000 0000`	AWS geral, Linux, EBCDIC

Tarefa	Descrição	Habilidades necessárias
	0f00 0000 .... 00000070: 0000 1000 0000 0dc1 c100 0000 0000 0000 .... 00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .... 00000090: 0000 0000 0000 ...... Para avaliar a equivalência entre os arquivos de origem e de destino, é necessário um conhecimento abrangent e do EBCDIC. Por exemplo, o primeiro caractere do arquivo EBCDIC de amostra é um hífen (-). Na notação hexadecimal do arquivo EBCDIC, esse caractere é representado por 60, e na notação hexadecimal do arquivo ASCII, esse caractere é representado por 2D. Para obter uma tabela EBCDIC-to-ASCII de conversão, consulte EBCDIC para ASCII no site da IBM.	

Recursos relacionados

Referências

- O conjunto de caracteres EBCDIC (documentação da IBM)

- EBCDIC para ASCII (documentação da IBM)
- COBOL (documentação da IBM)
- Conceitos básicos de JCL (documentação da IBM)
- Conecte-se à sua instância Linux (EC2 documentação da Amazon)

Tutoriais

- Agendamento de trabalhos SSH usando o AWS Lambda (publicação no blog da AWS)
- Uso de um acionador do Amazon S3 para invocar uma função do Lambda (documentação do AWS Lambda)

Converta arquivos de mainframe do formato EBCDIC para o formato ASCII delimitado por caracteres no Amazon S3 usando o AWS Lambda

Criado por Luis Gustavo Dantas (AWS)

Resumo

Esse padrão mostra como iniciar uma função do AWS Lambda que converte automaticamente arquivos EBCDIC (Extended Binary Coded Decimal Interchange Code) do mainframe em arquivos ASCII (American Standard Code for Information Interchange) delimitados por caracteres. A função do Lambda é executada depois do upload dos arquivos ASCII em um bucket do Amazon Simple Storage Service (Amazon S3). Após a conversão do arquivo, você pode ler os arquivos ASCII em workloads baseadas em x86 ou carregar os arquivos em bancos de dados modernos.

A abordagem de conversão de arquivos demonstrada nesse padrão pode ajudar a superar os desafios de trabalhar com arquivos EBCDIC em ambientes modernos. Os arquivos codificados em EBCDIC geralmente contêm dados representados em formato binário ou decimal compactado, e os campos têm tamanho fixo. Essas características criam obstáculos, porque workloads modernas baseadas em x86 ou ambientes distribuídos geralmente funcionam com dados codificados em ASCII e não conseguem processar arquivos EBCDIC.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do S3
- Um usuário do AWS Identity and Access Management (IAM) com permissões administrativas
- AWS CloudShell
- Python 3.8.0 ou superior
- Um arquivo simples codificado em EBCDIC e sua estrutura de dados correspondente em um copybook de linguagem comum orientada a negócios (COBOL)

> **Note**
>
> Esse padrão usa um arquivo EBCDIC de amostra (Client.EBCDIC.txt) e seu caderno COBOL correspondente (COBKS05.cpy). Ambos os arquivos estão disponíveis no GitHub mainframe-data-utilitiesrepositório.

Limitações

- Os copybooks de COBOL geralmente contêm várias definições de layout. O mainframe-data-utilitiesprojeto pode analisar esse tipo de caderno, mas não consegue inferir qual layout considerar na conversão de dados. Isso ocorre porque os copybooks não mantêm essa lógica (que, em vez disso, permanece nos programas COBOL). Consequentemente, você deve configurar manualmente as regras para selecionar layouts depois de analisar o copybook.
- Esse padrão está sujeito às cotas do Lambda.

Arquitetura

Pilha de tecnologia de origem

- IBM z/OS, IBM i e outros sistemas EBCDIC
- Arquivos sequenciais com dados codificados em EBCDIC (como descarregamentos do IBM Db2)
- Copybook de COBOL

Pilha de tecnologias de destino

- Amazon S3
- Notificação de eventos do Amazon S3
- IAM
- Função do Lambda
- Python 3.8 ou superior
- Utilitários de dados de mainframe
- Metadados JSON
- Arquivos ASCII delimitados por caracteres

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para converter arquivos EBCDIC de mainframe em arquivos ASCII.

O diagrama mostra o seguinte fluxo de trabalho:

1. O usuário executa o script do analisador de copybook para converter o copybook de COBOL em um arquivo JSON.
2. O usuário faz o upload dos metadados JSON em um bucket do S3. Isso torna os metadados legíveis pela função do Lambda de conversão de dados.
3. O usuário ou um processo automatizado faz o upload do arquivo EBCDIC no bucket do S3.
4. O evento de notificação do S3 aciona a função do Lambda de conversão de dados.
5. A AWS verifica as permissões de leitura e gravação do bucket do S3 para a função do Lambda.
6. O Lambda lê o arquivo do bucket do S3 e converte localmente o arquivo de EBCDIC para ASCII.
7. O Lambda registra o status do processo na Amazon. CloudWatch
8. O Lambda grava o arquivo ASCII de volta no Amazon S3.

> **Note**
>
> O script do analisador do copybook é executado somente uma vez, depois de converter os metadados em JSON e, em seguida, fazer o upload desses dados em um bucket do S3. Após a conversão inicial, qualquer arquivo EBCDIC que usa o mesmo arquivo JSON carregado no bucket do S3 usará os mesmos metadados.

Ferramentas

Ferramentas da AWS

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

- CloudShellA AWS é um shell baseado em navegador que você pode usar para gerenciar serviços da AWS usando a AWS Command Line Interface (AWS CLI) e uma variedade de ferramentas de desenvolvimento pré-instaladas.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. O Lambda executa seu código somente quando necessário e escala automaticamente, e, assim, você paga apenas pelo tempo de computação usado.

Outras ferramentas

- GitHubé um serviço de hospedagem de código que fornece ferramentas de colaboração e controle de versão.
- O Python é uma linguagem de programação de alto nível.

Código

O código desse padrão está disponível no GitHub mainframe-data-utilitiesrepositório.

Práticas recomendadas

Considere as seguintes práticas recomendadas:

- Defina as permissões necessárias no nível do nome do recurso da Amazon (ARN).
- Sempre conceda permissões de privilégio mínimo para políticas do IAM. Para obter mais informações, consulte Melhores práticas de segurança no IAM na documentação do IAM.

Épicos

Crie variáveis de ambiente e uma pasta de trabalho

Tarefa	Descrição	Habilidades necessárias
Crie as variáveis de ambiente.	Copie as seguintes variáveis de ambiente para um editor de texto e, em seguida, substitua	AWS geral

Tarefa	Descrição	Habilidades necessárias

	os valores <placeholder> no exemplo a seguir pelos valores do seu recurso:
	
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`
	
	Note
	Posteriormente, você criará referências para seu bucket do S3, conta da AWS e região da AWS.
	
	Para definir variáveis de ambiente, abra o CloudShell console e, em seguida, copie e cole suas variáveis de ambiente atualizadas na linha de comando.
	
	Note
	Você deve repetir essa etapa sempre que a CloudShell sessão for reiniciada.	

Tarefa	Descrição	Habilidades necessárias
Crie uma pasta de trabalho.	Para simplificar o processo de limpeza de recursos posterior mente, crie uma pasta de trabalho CloudShell executand o o seguinte comando: `mkdir workdir; cd workdir` **Note** Você deve alterar o diretório para o diretório de trabalho (`workdir`) toda vez que perder uma conexão com sua CloudShell sessão.	AWS geral

Defina uma política e um perfil do IAM

Tarefa	Descrição	Habilidades necessárias
Crie uma política de confiança para a função do Lambda.	O conversor EBCDIC é executado em uma função do Lambda. A função deve ter um perfil do IAM. Antes de criar um perfil do IAM, você deve definir um documento de política de confiança que permita que os recursos assumam essa política.	AWS geral

Tarefa	Descrição	Habilidades necessárias

	Na pasta de CloudShell trabalho, crie um documento de política executando o seguinte comando:
	
	`E2ATrustPol=$(cat <<EOF`
	`{`
	`  "Version":`
	`"2012-10-17",`
	`  "Statement": [`
	`  {`
	`  "Effect":`
	`"Allow",`
	`  "Principa`
	`l": {`
	`"Service": "lambda.a`
	`mazonaws.com"`
	`  },`
	`  "Action":`
	`"sts:AssumeRole"`
	`  }`
	`  ]`
	`}`
	`EOF`
	`)`
	`printf "$E2ATrustPol" >`
	`E2ATrustPol.json`	

Tarefa	Descrição	Habilidades necessárias
Crie o perfil do IAM para conversão do Lambda.	Para criar uma função do IAM, execute o seguinte comando da AWS CLI na pasta de CloudShell trabalho: `aws iam create-role --role-name E2AConvLambdaRole --assume-role-policy-document file://E2ATrustPol.json`	AWS geral

Tarefa	Descrição	Habilidades necessárias

Crie o documento de política do IAM para a função do Lambda.	A função Lambda deve ter acesso de leitura e gravação ao bucket do S3 e permissões de gravação para o Amazon Logs. CloudWatch
	
	Para criar uma política do IAM, execute o seguinte comando na pasta de CloudShell trabalho:
	
	`E2APolicy=$(cat <<EOF`
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Sid": "Logs",`
	`"Effect": "Allow",`
	`"Action": [`
	`"logs:PutLogEvents",`
	`"logs:CreateLogStream",`
	`"logs:CreateLogGroup"`
	`],`
	`"Resource": [`
	`"arn:aws:logs:*:*:log-group:*",`
	`"arn:aws:logs:*:*:log-group:*:log-stream:*"`
	`]
		AWS geral

Tarefa	Descrição	Habilidades necessárias

	<pre> },
	        {
	            "Sid": "S3",
	            "Effect":
	"Allow",
	            "Action": [
	
	"s3:GetObject",
	
	"s3:PutObject",
	
	"s3:GetObjectVersion"
	            ],
	            "Resource":
	[
	
	"arn:aws:s3:::%s/*",
	
	"arn:aws:s3:::%s"
	            ]
	        }
	    ]
	}
	EOF
	)
	printf "$E2APolicy"
	"$bucket" "$bucket"
	> E2AConvLambdaPolic
	y.json</pre>	

Tarefa	Descrição	Habilidades necessárias
Anexe o documento da política do IAM ao perfil do IAM.	Para anexar a política do IAM à função do IAM, execute o seguinte comando na sua pasta de CloudShell trabalho: `aws iam put-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy --policy-document file://E2AConvLambdaPolicy.json`	AWS geral

Crie a função do Lambda para conversão de EBCDIC

Tarefa	Descrição	Habilidades necessárias
Baixe o código-fonte da conversão EBCDIC.	Na pasta de CloudShell trabalho, execute o comando a seguir para baixar o mainframe-data-utilities código-fonte de GitHub: `git clone https://github.com/aws-samples/mainframe-data-utilities.git mdu`	AWS geral
Crie o pacote ZIP.	Na pasta de CloudShell trabalho, execute o comando a seguir para criar o pacote ZIP que cria a função Lambda para conversão EBCDIC:	AWS geral

Tarefa	Descrição	Habilidades necessárias
	`cd mdu; zip ../mdu.zip *.py; cd ..`	
Criar a função do Lambda.	Na pasta de CloudShell trabalho, execute o seguinte comando para criar a função Lambda para conversão EBCDIC: `aws lambda create-function \ --function-name E2A \ --runtime python3.9 \ --zip-file fileb://mdu.zip \ --handler extract_ebcdic_to_ascii.lambda_handler \ --role arn:aws:iam::$account:role/E2AConvLambdaRole \ --timeout 10 \ --environment "Variables={layout=$bucket/layout/}"` **Note** O layout da variável de ambiente informa à função Lambda onde residem os metadados JSON.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie a política baseada em recursos para a função do Lambda.	Na pasta de CloudShell trabalho, execute o seguinte comando para permitir que sua notificação de eventos do Amazon S3 acione a função Lambda para conversão EBCDIC: `aws lambda add-permi ssion \ --function-name E2A \ --action lambda:In vokeFunction \ --principal s3.amazon aws.com \ --source-arn arn:aws:s 3:::$bucket \ --source-account $account \ --statement-id 1`	AWS geral

Crie a notificação de evento do Amazon S3

Tarefa	Descrição	Habilidades necessárias
Crie o documento de configura ção para a notificação de evento do Amazon S3.	A notificação de evento do Amazon S3 inicia a função do Lambda de conversão do EBCDIC quando os arquivos são colocados na pasta de entrada. Na pasta de CloudShell trabalho, execute o seguinte comando para criar o documento JSON para a	AWS geral

Tarefa	Descrição	Habilidades necessárias
	notificação de eventos do Amazon S3: `{ "LambdaFunctionConfigurations": [{ "Id": "E2A", "LambdaFunctionArn": "arn:aws:lambda:%s:%s:function:E2A", "Events": ["s3:ObjectCreated:Put"], "Filter": { "Key": { "FilterRules": [{ "Name": "prefix", "Value": "input/" }] } } }] } EOF) printf "$S3E2AEvent" "$region" "$account" > S3E2AEvent.json`	

Tarefa	Descrição	Habilidades necessárias
Crie a notificação de evento do Amazon S3.	Na pasta de CloudShell trabalho, execute o seguinte comando para criar a notificação de eventos do Amazon S3: `aws s3api put-bucket-notification-configuration --bucket $bucket --notification-configuration file://S3E2AEvent.json`	AWS geral

Crie e faça o upload dos metadados JSON

Tarefa	Descrição	Habilidades necessárias

Analise o copybook de COBOL.	Na pasta de CloudShell trabalho, execute o comando a seguir para analisar um exemplo de caderno COBOL em um arquivo JSON (que define como ler e dividir o arquivo de dados corretamente):
	`python3 mdu/parse_copybook_to_json.py \`
	`-copybook mdu/LegacyReference/COBKS05.cpy \`
	`-output CLIENT.json \`
	`-output-s3key CLIENT.ASCII.txt \`
		AWS geral

Tarefa	Descrição	Habilidades necessárias

	`-output-s3bkt $bucket \`
	`-output-type  s3 \`
	`-print  25`	

Adicione a regra de transform ação.	O arquivo de dados de amostra e seu copybook de COBOL correspondente são arquivos com vários layouts. Isso significa que a conversão deve dividir os dados com base em determinadas regras. Nesse caso, os bytes nas posições 3 e 4 em cada linha definem o layout.
	
	Na pasta de CloudShell trabalho, edite o `CLIENT.json` arquivo e altere o conteúdo `"transf-rule": [],` para o seguinte:
	
	`"transf-rule": [`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0002",`
	`"transf": "transf1"`
	`},`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0000",`
	`"transf": "transf2"`
	`}`
	`],`
		AWS geral, IBM Mainframe, Cobol

Tarefa	Descrição	Habilidades necessárias
Faça o upload dos metadados JSON no bucket do S3.	Na pasta de CloudShell trabalho, execute o seguinte comando da AWS CLI para carregar os metadados JSON em seu bucket do S3: `aws s3 cp CLIENT.json s3://$bucket/layout/CLIENT.json`	AWS geral

Converta o arquivo EBCDIC

Tarefa	Descrição	Habilidades necessárias
Envie o arquivo EBCDIC para o bucket do S3.	Na pasta de CloudShell trabalho, execute o comando a seguir para enviar o arquivo EBCDIC para o bucket do S3: `aws s3 cp mdu/sample-data/CLIENT.EBCDIC.txt s3://$bucket/input/` **Note** Recomendamos que você defina pastas diferentes para arquivos de entrada (EBCDIC) e saída (ASCII) para evitar chamar a função de conversão do Lambda novamente quando	AWS geral

Tarefa	Descrição	Habilidades necessárias
	o arquivo ASCII for carregado no bucket do S3.	

Tarefa	Descrição	Habilidades necessárias

Verifique a saída.	Na pasta de CloudShell trabalho, execute o comando a seguir para verificar se o arquivo ASCII foi gerado no seu bucket do S3:
	`awss3 ls s3://$bucket/`
	Note
	A conversão de dados pode levar alguns segundos para acontecer. Recomendamos que você verifique o arquivo ASCII algumas vezes.
	Depois que o arquivo ASCII estiver disponível, execute o comando a seguir para baixar o arquivo do bucket do S3 para a pasta atual:
	`aws s3 cp s3://$bucket/ CLIENT.ASCII.txt .`
	Verifique o conteúdo do arquivo ASCII:
	`head CLIENT.ASCII.txt`
		AWS geral

Limpe o ambiente

Tarefa	Descrição	Habilidades necessárias

(Opcional) Prepare as variáveis e a pasta.	Se você perder a conexão com CloudShell, reconecte-se e execute o seguinte comando para alterar o diretório para a pasta de trabalho:
	`cd workdir`
	Certifique-se de que as variáveis de ambiente estejam definidas:
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`
		AWS geral

Remova a configuração de notificação para o bucket.	Na pasta de CloudShell trabalho, execute o seguinte comando para remover a configuração de notificação de eventos do Amazon S3:
	`aws s3api put-bucket-notification-configuration \`
	`--bucket=$bucket \`
	`--notification-configuration="{}"`
		AWS geral

Exclua a função do Lambda.	Na pasta de CloudShell trabalho, execute o seguinte	AWS geral

Tarefa	Descrição	Habilidades necessárias
	comando para excluir a função Lambda para o conversor EBCDIC: `awslambdadelete-function--function-nameE2A`	

Exclua a política e o perfil do IAM.	Na pasta de CloudShell trabalho, execute o comando a seguir para remover a função e a política do conversor EBCDIC:
	
	`aws iam delete-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy`
	
	`aws iam delete-role --role-name E2AConvLambdaRole`
		AWS geral

Exclua os arquivos gerados no bucket do S3.	Na pasta de CloudShell trabalho, execute o comando a seguir para excluir os arquivos gerados no bucket do S3:
	
	`aws s3 rm s3://$bucket/layout --recursive`
	`aws s3 rm s3://$bucket/input --recursive`
	`aws s3 rm s3://$bucket/CLIENT.ASCII.txt`
		AWS geral

Tarefa	Descrição	Habilidades necessárias
Exclua a pasta de trabalho.	Na pasta de CloudShell trabalho, execute o seguinte comando para remover `workdir` e seu conteúdo: `cd ..; rm -Rf workdir`	AWS geral

Recursos relacionados

- Utilitários de dados de mainframe README () GitHub
- O conjunto de caracteres EBCDIC (documentação da IBM)
- EBCDIC para ASCII (documentação da IBM)
- COBOL (documentação da IBM)
- Uso de um acionador do Amazon S3 para invocar uma função do Lambda (documentação do AWS Lambda)

Converta arquivos de dados de mainframe com layouts de registro complexos usando o Micro Focus

Criado por Peter West

Resumo

Este padrão mostra como converter arquivos de dados de mainframe com dados não textuais e layouts de registro complexos da codificação de caracteres EBCDIC (Extended Binary Coded Decimal Interchange Code) para a codificação de caracteres ASCII (American Standard Code for Information Interchange) usando um arquivo de estrutura do Micro Focus. Para concluir a conversão do arquivo, você deve fazer o seguinte:

1. Prepare um único arquivo de origem que descreva todos os itens de dados e layouts de registro em seu ambiente de mainframe.
2. Crie um arquivo de estrutura que contenha o layout de registro dos dados usando o Micro Focus Data File Editor como parte do Micro Focus Classic Data File Tools ou Data File Tools. O arquivo de estrutura identifica os dados não textuais para que você possa converter corretamente seus arquivos de mainframe de EBCDIC para ASCII.
3. Teste o arquivo de estrutura usando o Classic Data File Tools ou Data File Tools.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Micro Focus Enterprise Developer para Windows, disponível por meio da AWS Mainframe Modernization

Versões do produto

- Micro Focus Enterprise Server 7.0 e mais recente

Ferramentas

- O Micro Focus Enterprise Server fornece o ambiente de execução para aplicativos criados com qualquer variante de ambiente de desenvolvimento integrado (IDE) do Enterprise Developer.

- O Classic Data File Tools do Micro Focus ajuda você a converter, navegar, editar e criar arquivos de dados. O Classic Data File Tools inclui Data File Converter, Record Layout Editor e Data File Editor.
- O Data File Tools do Micro Focus ajuda você a criar, editar e mover arquivos de dados. O Data File Tools inclui o Data File Editor, File Conversion Utilities e o Data File Structure Command Line Utility.

Épicos

Preparar o arquivo de origem

Tarefa	Descrição	Habilidades necessárias
Identifique os componentes de origem.	Identifique todos os layouts de registro possíveis para o arquivo, incluindo quaisquer redefinições que contenham dados não textuais. Se você tiver layouts que contenham redefinições, você deve reduzir esses layouts a layouts exclusivos que descrevam cada permutaçã o possível da estrutura de dados. Normalmente, os layouts de registro de um arquivo de dados podem ser descritos pelos seguintes arquétipos: • Layout de registro somente com dados de texto • Layout de registro com dados não textuais • Layout de registro com dados não textuais	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	subordinados a uma cláusula REDEFINES Para obter mais informaçõ es sobre a criação de layouts de registro nivelados para arquivos que contêm layouts de registro complexos , consulte Redefinir a hospedagem de aplicativos EBCDIC em ambientes ASCII para migrações de mainframe.	

Tarefa	Descrição	Habilidades necessárias

Identifique as condições do layout do registro.	Para arquivos com vários layouts de registro ou arquivos que contêm layouts complexos com uma cláusula REDEFINES, identifique os dados e as condições em um registro que você pode usar para definir qual layout usar durante a conversão. Recomendamos que você discuta essa tarefa com um especialista no assunto (SME - subject matter expert) que entenda os programas que processam esses arquivos.
	
	Por exemplo, um arquivo pode conter dois tipos de registro que contêm dados não textuais. Você pode inspecion ar a fonte e possivelm ente encontrar um código semelhante ao seguinte:
	
	`MOVE "M" TO PART-TYPE`
	`MOVE "MAIN ASSEMBLY" TO`
	`PART-NAME`
	`MOVE "S" TO PART-TYPE`
	`MOVE "SUB ASSEMBLY 1"`
	`TO PART-NAME`
	
	O código ajuda você a identific ar o seguinte:
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	• O campo “PART-TYPE” é usado para determinar o tipo de registro • O valor “M” é usado para o “M-PART-RECORD” • O valor “S” é usado para o “S-PART-RECORD” Você pode documentar os valores usados por esse campo para associar os layouts de registro aos registros de dados corretos no arquivo.	

Tarefa	Descrição	Habilidades necessárias
Crie o arquivo de origem.	Se o arquivo estiver descrito em vários arquivos de origem ou se o layout do registro contiver dados não textuais subordinados a uma cláusula REDEFINES, crie um novo arquivo de origem que contenha os layouts do registro. O novo programa não precisa descrever o arquivo usando as instruções SELECT e FD. O programa pode simplesmente conter as descrições dos registros em 01 nível no Working-Storage. **Note** Você pode criar um arquivo de origem para cada arquivo de dados ou criar um arquivo de origem mestre que descreva todos os arquivos de dados.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Compilar o arquivo de origem.	Compile o arquivo de origem para criar o dicionário de dados. Recomendamos que você compile o arquivo de origem usando o conjunto de caracteres EBCDIC. Se a diretiva IBMCOMP ou as diretivas ODOSLIDE estiverem sendo usadas, você também deverá usar essas diretivas no arquivo de origem. **Note** O IBMCOMP afeta o armazenamento de bytes dos campos COMP e o ODOSLIDE afeta o preenchim ento nas estruturas OCCUS VARYING. Se essas diretivas forem definidas incorreta mente, a ferramenta de conversão não lerá o registro de dados corretamente. Isso resulta em dados incorretos no arquivo convertido.	Desenvolvedor de aplicativos

(Opção A) Crie o arquivo de estrutura usando o Classic Data File Tools

Tarefa	Descrição	Habilidades necessárias
Inicie a ferramenta e carregue o dicionário.	1. Escolha o ícone do menu Iniciar do Windows, pesquise e escolha Micro Focus Enterprise Developer e, em seguida, escolha Classic Data File Tools. 2. Escolha Arquivo e, em seguida, escolha Layout de registro. 3. Na caixa de diálogo Selecionar um arquivo para criar os layouts de, em Nome do arquivo, selecione o arquivo IDY (`.idy`) que foi criado quando você compilou o arquivo de origem anteriormente. Em seguida, selecione Open (Abrir). 4. Para confirmar se o Classic Data File Tools está usando EBCDIC, na caixa de diálogo do Data File Tools, escolha SIM se o arquivo IDY estiver definido como EBCDIC e o Datatools estiver definido como ANSI.	Desenvolvedor de aplicativos
Crie o layout de registro padrão.	Use o layout de registro padrão para todos os registros que não correspondam a nenhum layout condicional.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	1. Na janela Layout, expanda a estrutura de dados e localize o nível 01 usado para o layout padrão. 2. Clique com o botão direito do mouse no item 01 e escolha Novo layout. 3. Na caixa de diálogo Assistente para novo layout de registro, escolha Layout padrão e, em seguida, escolha Avançar. 4. Escolha Terminar. O layout padrão aparece no painel Layouts e pode ser identificado pelo ícone de pasta vermelha.	

Tarefa	Descrição	Habilidades necessárias
Crie um layout de registro condicional.	Use o layout de registro condicional quando houver mais de um layout de registro em um arquivo. 1. No painel Layouts, expanda a estrutura de dados e localize o nível 01 usado para o layout condicional. 2. Clique com o botão direito do mouse no item 01 e escolha Novo layout. 3. Na caixa de diálogo Assistente para novo layout de registro, escolha Layout condicional e, em seguida, escolha Avançar. 4. Escolha Terminar. O layout condicional aparece no painel Layouts e pode ser identificado pelo ícone de pasta amarela. 5. Expanda o layout condicional, clique com o botão direito do mouse no campo em que você deve colocar uma condição e escolha Propriedades. 6. Na caixa de diálogo Propriedades do campo, insira a condição. Confirme se o conjunto de caracteres está definido como EBCDIC e escolha OK. Uma marca	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	de seleção aparece ao lado do campo que tem uma condição definida. 7. Repita as etapas de 5 a 6 para qualquer outro campo que exija condições para esse layout. 8. Repita as etapas de 1 a 6 para qualquer outro layout condicional que precise ser adicionado. 9. Escolha Arquivo, escolha Salvar como e, em seguida, salve o arquivo de estrutura no disco.	

(Opção B) Crie o arquivo de estrutura usando o Data File Tools

Tarefa	Descrição	Habilidades necessárias
Inicie a ferramenta e carregue o dicionário.	1. Escolha o ícone do menu Iniciar do Windows, pesquise e escolha Micro Focus Enterprise Developer e, em seguida, escolha Data File Tools. 2. Escolha Arquivo, Novo, Arquivo de estrutura. 3. Na caixa de diálogo Abrir, em Nome do arquivo, selecione o arquivo IDY (`.idy`) que foi criado quando você compilou	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	o arquivo de origem anteriormente. Em seguida, selecione Open (Abrir). 4. Para confirmar se o Data File Tools está usando o EBCDIC, confirme se o menu suspenso na seção Arquivo de depuração está definido como EBCDIC.	
Crie o layout de registro padrão.	Use o layout de registro padrão para todos os registros que não correspondam a nenhum layout condicional. 1. Na seção Layouts disponíveis no painel esquerdo, expanda a estrutura de dados e localize o nível 01 usado para o layout padrão. 2. Clique com o botão direito do mouse no item 01 e escolha Criar layout padrão. O layout padrão aparece no painel Layouts e pode ser identificado pelo ícone azul “D”.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Crie um layout de registro condicional.	Use o layout de registro condicional quando houver mais de um layout de registro em um arquivo. 1. Na seção Layouts seleciona dos no painel direito, expanda a estrutura de dados e localize o nível 01 usado para o layout condicional. 2. Clique com o botão direito do mouse no item 01 e escolha Criar layout condicional. O layout condicional aparece no painel Layouts no lado direito e pode ser identific ado pelo ícone verde “C”. 3. Expanda o layout condicion al, clique com o botão direito do mouse no campo em que você deve colocar uma condição e escolha Propriedades. 4. Na caixa de diálogo Propriedades do campo, insira a condição. Confirme se o conjunto de caracteres está definido como EBCDIC e escolha OK. Um ícone vermelho “IF” aparece ao lado do campo que tem uma condição definida.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	5. Repita as etapas de 3 a 4 para qualquer outro campo que exija condições para esse layout. 6. Repita as etapas de 1 a 4 para qualquer outro layout condicional que precise ser adicionado. 7. Escolha Arquivo, escolha Salvar como e, em seguida, salve o arquivo de estrutura no disco.	

(Opção A) Teste o arquivo de estrutura usando o Classic Data File Tools

Tarefa	Descrição	Habilidades necessárias
Teste um arquivo de dados EBCDIC.	Confirme se você pode usar seu arquivo de estrutura para visualizar um arquivo de dados de teste EBCDIC corretamente. 1. Escolha o ícone do menu Iniciar do Windows, localize e escolha Micro Focus Enterprise Developer e, em seguida, escolha Classic Data Tools. 2. Escolha Arquivo e depois escolha Abrir. 3. Na caixa de diálogo Abrir, em Nome do arquivo, selecione o conjunto de	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	dados EBCDIC e escolha Abrir. 4. Escolha Arquivo, Editor de arquivo de dados, Carregar layouts de registro. 5. Na caixa de diálogo Abrir, em Nome do arquivo, selecione o arquivo de estrutura e escolha Abrir. 6. Para confirmar se o modo de conjunto de caractere s está definido como EBCDIC, confirme se o menu suspenso está definido como EBCDIC. Você pode ver os dados brutos do registro no painel esquerdo e os dados formatados no painel direito. 7. Escolha vários registros para garantir que todos os formatos sejam renderiza dos com o layout correto.	

(Opção B) Teste o arquivo de estrutura usando o Data File Tools

Tarefa	Descrição	Habilidades necessárias
Teste um arquivo de dados EBCDIC.	Confirme se você pode usar seu arquivo de estrutura para visualizar um arquivo	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	de dados de teste EBCDIC corretamente. 1. Escolha o ícone do menu Iniciar do Windows, localize e selecione Micro Focus Enterprise Developer e, em seguida, escolha Data File Tools. 2. Escolha Arquivo, Abrir, Arquivo de dados. 3. Na caixa de diálogo Abrir arquivo de dados, na guia Local, em Nome do arquivo, escolha Procurar para encontrar a localização do arquivo de teste EBCDIC. 4. Em Arquivo de estrutura (opcional), escolha Procurar para encontrar a localizaç ão do arquivo de estrutura. 5. Na seção Detalhes do arquivo, insira os detalhes do arquivo e confirme se a Codificação está definida como EBCDIC. 6. Escolha o modo Abrir compartilhado ou Abrir exclusivo, dependendo de suas necessidades. 7. Confirme se o menu suspenso na seção Aparência da barra de ferramentas está definido	

Tarefa	Descrição	Habilidades necessárias
	como EBCDIC. Você vai ver os dados brutos do registro no painel esquerdo e os dados formatados no painel direito. 8. Escolha vários registros para garantir que todos os formatos sejam renderizados com o layout correto.	

Teste a conversão do arquivo de dados

Tarefa	Descrição	Habilidades necessárias
Teste a conversão de um arquivo EBCDIC.	1. Escolha o ícone do menu Iniciar do Windows, localize e selecione Micro Focus Enterprise Developer e, em seguida, escolha Classic Data Tools. 2. Escolha Ferramentas e, em seguida, Console. 3. Na caixa de diálogo Data File Convert, na seção Arquivo de entrada, em Nome do arquivo, escolha Procurar para localizar e selecionar o arquivo de entrada EBCDIC. Confirme se o Conjunto de caracteres está definido como EBCDIC.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	4. Na seção Conversão de conjunto de caractere s, marque as caixas de seleção Converter conjunto de caracteres e Registros contêm itens de dados não textuais. Escolha Seleciona r layout para conversão e, em seguida, escolha Procurar para localizar e selecionar o arquivo de estrutura. 5. Na seção Novo arquivo, em Nome do arquivo, insira o caminho e o nome do arquivo de saída ASCII que você deseja criar. Por padrão, a ferramenta de conversão usa o mesmo formato do arquivo de entrada. Para o teste, deixe as opções com seus valores padrão. 6. Escolha Converter. 7. Siga as etapas na seção (Opção A) Teste o arquivo de estrutura usando o Classic Data File Tools ou (Opção B) Teste o arquivo de estrutura usando o Data File Tools, mas carregue o arquivo de saída ASCII em vez do arquivo EBCDIC.	

Tarefa	Descrição	Habilidades necessárias
	8. Carregue os arquivos EBCDIC e ASCII no Editor de arquivos de dados e compare os arquivos lado a lado para verificar a precisão da conversão.	

Recursos relacionados

- Micro Focus (documentação da Micro Focus)
- Mainframe e código antigo (publicações do Blog da AWS)
- Recomendações da AWS (documentação da AWS)
- Documentação da AWS (documentação da AWS)
- Referência geral da AWS (documentação da AWS)
- Glossário da AWS (documentação da AWS)

Implante um ambiente para aplicativos Blu Age conteinerizados usando o Terraform

Criado por Richard Milner-Watts (AWS)

Resumo

A migração de workloads de mainframe legadas para arquiteturas de nuvem modernas pode eliminar os custos de manutenção de um mainframe — custos que só aumentam à medida que o ambiente envelhece. No entanto, migrar trabalhos de um mainframe pode representar desafios únicos. Os recursos internos podem não estar familiarizados com a lógica do trabalho, e o alto desempenho dos mainframes nessas tarefas especializadas pode ser difícil de replicar quando comparado ao padrão generalizado. CPUs Reescrever esses trabalhos pode ser uma grande tarefa e exigir um esforço significativo.

O Blu Ags converte as workloads antigas de mainframe em código Java moderno, que você pode então executar como um contêiner.

Esse padrão fornece um exemplo de arquitetura de tecnologia sem servidor para executar um aplicativo em contêiner que foi modernizado com a ferramenta Blu Age. Os arquivos HashiCorp Terraform incluídos criarão uma arquitetura segura para a orquestração de contêineres Blu Age, suportando tarefas em lote e serviços em tempo real.

Para obter mais informações sobre a modernização de suas workloads usando o Blu Age e os serviços da AWS, consulte estas publicações de Recomendações da AWS:

- Executando workloads modernizadas de mainframe Blu Age em uma infraestrutura AWS de tecnologia sem servidor
- Containerize workloads de mainframe que foram modernizadas pela Blu Age

Para obter ajuda com o uso do Blu Age para modernizar suas workloads de mainframe, entre em contato com a equipe da Blu Age escolhendo Entre em contato com nossos especialistas no site da Blu Age. Para obter ajuda para migrar suas workloads modernizadas para a AWS, integrá-las aos serviços da AWS e colocá-las em produção, entre em contato com seu gerente de contas da AWS ou preencha o formulário AWS Professional Services.

Pré-requisitos e limitações

Pré-requisitos

- O exemplo do aplicativo Blu Age conteinerizado fornecido pelo padrão Workloads do mainframe Containerize que foram modernizadas pelo Blu Age. O aplicativo de amostra fornece a lógica para lidar com o processamento de entrada e saída para o aplicativo modernizado e pode se integrar a essa arquitetura.
- O Terraform é necessário para implantar esses recursos.

Limitações

- O Amazon Elastic Container Service (Amazon ECS) impõe limites aos recursos de tarefa que podem ser disponibilizados para o contêiner. Esses recursos incluem CPU, RAM e armazenamento. Por exemplo, ao usar o Amazon ECS com o AWS Fargate, os limites de recursos da tarefa se aplicam.

Versões do produto

Essa solução foi testada com as seguintes versões:

- Terraform 1.3.6
- Provedor Terraform AWS 4.46.0

Arquitetura

Pilha de tecnologia de origem

- Blu Age
- Terraform

Pilha de tecnologias de destino

- Amazon Aurora Edição Compatível com PostgreSQL
- AWS Backup
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- AWS Identity and Access Management Service (IAM)
- AWS Key Management Server (AWS KMS)

- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager

Arquitetura de destino

O diagrama a seguir mostra a arquitetura da solução.

1. A solução implanta os seguintes perfis do IAM:
   - Perfil da tarefa de lote
   - Perfil de execução de tarefas em lote
   - Perfil da tarefa de serviço
   - Perfil de execução da tarefa do serviço
   - Perfil dos Perfis da etapa
   - Perfil do AWS Backup
   - Perfil de monitoramento avançado do RDS.

   Os perfis estão em conformidade com os princípios de acesso com privilégio mínimo.
2. O Amazon ECR é usado para armazenar a imagem do contêiner que é orquestrada por esse padrão.
3. O AWS Systems Manager Parameter Store fornece dados de configuração sobre cada ambiente para a definição de tarefa do Amazon ECS em runtime.
4. O AWS Secrets Manager fornece dados de configuração confidenciais sobre o ambiente para a definição de tarefas do Amazon ECS em runtime. Os dados foram criptografados pelo AWS KMS.
5. Os módulos do Terraform criam definições de tarefas do Amazon ECS para todas as tarefas em tempo real e em lote.
6. O Amazon ECS executa uma tarefa em lote usando o AWS Fargate como mecanismo de computação. Essa é uma tarefa de curta duração, iniciada conforme exigido pelo AWS Step Functions.

7. Compatível com o Amazon Aurora PostgreSQL fornece um banco de dados para dar suporte ao aplicativo modernizado. Isso substitui bancos de dados de mainframe, como IBM Db2 ou IBM IMS DB.
8. O Amazon ECS executa um serviço de longa duração para fornecer uma workload modernizada em tempo real. Esses aplicativos sem estado são executados permanentemente com contêineres espalhados pelas zonas de disponibilidade.
9. Um Network Load Balancer é usado para conceder acesso à workload em tempo real. O Network Load Balancer é compatível com protocolos anteriores, como o IBM CICS. Como alternativa, você pode usar um Application Load Balancer para workloads baseadas em HTTP.
10. O Amazon S3 fornece armazenamento de objetos para entradas e saídas de trabalhos. O contêiner deve lidar com as operações de pull e push no Amazon S3 para preparar o diretório de trabalho para o aplicativo Blu Age.
11. O serviço AWS Step Functions é usado para orquestrar a execução das tarefas do Amazon ECS para processar workloads em lote.
12. Os tópicos do SNS para cada workload em lote são usados para integrar o aplicativo modernizado a outros sistemas, como e-mail, ou para iniciar ações adicionais, como entregar objetos de saída do Amazon S3 para o FTP.

> **Note**
>
> Por padrão, a solução não tem acesso à Internet. Esse padrão supõe que a nuvem privada virtual (VPC) será conectada a outras redes usando um serviço como o AWS Transit Gateway. Dessa forma, vários endpoints da VPC de interface são implantados para conceder acesso aos serviços da AWS usados pela solução. Para ativar o acesso direto à Internet, você pode usar o botão no módulo Terraform para substituir os endpoints da VPC por um gateway da Internet e os recursos associados.

Automação e escala

O uso de recursos de tecnologia sem servidor em todo esse padrão ajuda a garantir que, ao escalar, haja poucos limites na escala desse design. Isso reduz as preocupações ruidosas dos vizinhos, como a competição por recursos computacionais que podem existir no mainframe original. As tarefas em lote podem ser programadas para serem executadas simultaneamente, conforme necessário.

Os contêineres individuais são limitados pelos tamanhos máximos suportados pelo Fargate. Para obter mais informações, consulte a seção CPU e memória da tarefa na documentação do Amazon ECS.

Para escalar cargas de trabalho em tempo real horizontalmente, você pode adicionar contêineres.

Ferramentas

Serviços da AWS

- O Amazon Aurora Edição Compatível com PostgreSQL é um mecanismo de banco de dados relacional totalmente gerenciado e compatível com ACID que ajuda você a configurar, operar e escalar implantações do PostgreSQL.
- O AWS Backup é um serviço totalmente gerenciado que ajuda você a centralizar e automatizar a proteção de dados na nuvem e no local. Serviços da AWS
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos, controlando quem está autenticado e autorizado a usá-los.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Step Functions é um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.

- O AWS Systems Manager Parameter Store oferece armazenamento hierárquico seguro para o gerenciamento de dados de configuração e gerenciamento de segredos.

Outros serviços

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem. Esse padrão usa o Terraform para criar a arquitetura de amostra.

Repositório de código

O código-fonte desse padrão está disponível no repositório GitHub Blu Age Sample ECS Infrastructure (Terraform).

Práticas recomendadas

- Para ambientes de teste, use atributos como a opção `forceDate` de configurar o aplicativo modernizado para gerar resultados de teste consistentes, sempre executando por um período de tempo conhecido.
- Ajuste cada tarefa individualmente para consumir a quantidade ideal de recursos. Você pode usar o Amazon CloudWatch Container Insights para obter orientação sobre possíveis gargalos.

Épicos

Prepare o ambiente para implantação

Tarefa	Descrição	Habilidades necessárias
Clone o código-fonte da solução.	Clone o código da solução do GitHub projeto.	DevOps engenheiro
Inicialize o ambiente implantando recursos para armazenar o estado do Terraform.	1. Abra uma janela do terminal e confirme se o Terraform está instalado e se AWS as credenciais estão disponíveis.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	2. Navegue para a pasta `bootstrap-terraform` . 3. Edite o arquivo `main.tf` se quiser alterar os nomes do bucket do S3 (`<accountId>-terraform-backend`) e da tabela do Amazon DynamoDB (`terraform-lock`). 4. Execute o comando `terraform apply` para implantar os recursos. Anote os nomes do bucket do S3 e da tabela do DynamoDB.	

Implante a infraestrutura da solução

Tarefa	Descrição	Habilidades necessárias
Revise e atualize a configuração do Terraform.	No diretório raiz, abra o arquivo `main.tf`, , revise o conteúdo e considere fazer as seguintes atualizações: 1. Atualize o Região da AWS pesquisando e substituindo a string `eu-west-1` pela região desejada que você deseja usar. 2. Atualize o nome do bucket no `Terraform Backend`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	bloco se o padrão tiver sido alterado no épico anterior. 3. Atualize o `dynamodb_table` valor se o padrão foi alterado no épico anterior. 4. Atualize o valor da variável `stack_prefix` para a string desejada. Essa string será anexada aos nomes de todos os recursos criados por esse padrão. 5. Atualize o valor do `vpc_cidr` Isso deve ser pelo menos um intervalo de endereços `/24`. 6. Revise a `Locals` seção. Isso é usado para definir as tarefas do Blu Age que serão implantadas. A solução iterará sobre o objeto da lista `bluage_batch_modules` , criando os recursos associados (máquina de estado do Step Functions, definição de tarefa e tópico do SNS) para cada elemento da lista. Em alguns casos, convém ajustar variáveis para ambientes diferentes. Por exemplo, para forçar o runtime em ambientes de teste, você pode alterar	

Tarefa	Descrição	Habilidades necessárias
	o valor da `force_execution_time` variável. 7. Para ativar o acesso à Internet, altere o valor `direct_internet_access_required` de `false` para `true`. Isso implantará um gateway da Internet, junto com os gateways NAT e tabelas de rotas que ativam o acesso público à Internet para a infraestrutura. Por padrão, a solução implantará endpoints da VPC de interface em uma VPC sem acesso direto à Internet. 8. Para conceder acesso a qualquer workloads cliente-servidor que seja atendida por meio do Elastic Load Balancing, atualize os valores `additional_nlb_igress_cidrs` de com as redes CIDR que devem ser permitidas.	

Tarefa	Descrição	Habilidades necessárias
Implantar o arquivo Terraform.	No seu terminal, executar o `terraform apply` comando para implantar todos os recursos. Revise as alteraçõe s geradas pelo Terraform e digite sim para iniciar a construção. Observe que a implantação dessa infraestrutura pode levar mais de 15 minutos.	DevOps engenheiro

(Opcional) Implante uma aplicação conteinerizada Blu Age válida

Tarefa	Descrição	Habilidades necessárias
Envie a imagem do contêiner do Blu Age para o Amazon ECR.	Envie o contêiner para o repositório do Amazon ECR que você criou no épico anterior. Para obter instruçõe s, consulte a Documentação do Amazon ECR. Anote o URI da imagem do contêiner.	DevOps engenheiro
Atualize o Terraform para referenciar a imagem do contêiner Blu Age.	Atualize o arquivo `main.tf` para referenciar a imagem do contêiner que você carregou.	DevOps engenheiro
Reimplante o arquivo Terraform.	No seu terminal, executar `terraform apply` para implantar todos os recursos. Analise as atualizações sugeridas pelo Terraform e,	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	em seguida, insira sim para continuar com a implantação.	

Recursos relacionados

- Blu Age
- Como executar workloads modernizadas de mainframe Blu Age em uma infraestrutura AWS de tecnologia sem servidor
- Containerize workloads de mainframe que foram modernizadas pela Blu Age

Gere insights de dados do Db2 z/OS usando o AWS Mainframe Modernization Amazon Q em QuickSight

Criado por Shubham Roy (AWS), Roshna Razack (AWS) e Santosh Kumar Singh (AWS)

Resumo

Se sua organização está hospedando dados essenciais para os negócios em um ambiente de mainframe IBM Db2, obter insights desses dados é crucial para impulsionar o crescimento e a inovação. Ao desbloquear dados do mainframe, você pode criar inteligência de negócios mais rápida, segura e escalável para acelerar a tomada de decisões, o crescimento e a inovação orientados por dados na nuvem da Amazon Web Services ().AWS

Esse padrão apresenta uma solução para gerar insights de negócios e criar narrativas compartilháveis a partir de dados de mainframe nas tabelas do IBM Db2 for z/OS. As alterações nos dados do mainframe são transmitidas para o tópico Amazon Managed Streaming for Apache Kafka (AmazonAWS Mainframe Modernization MSK) usando a replicação de dados com o Preciously. Usando a ingestão de streaming do Amazon Redshift, os dados de tópicos do Amazon MSK são armazenados em tabelas de armazém de dados do Amazon Redshift Serverless para análise na Amazon. QuickSight

Depois que os dados estiverem disponíveis QuickSight, você poderá usar solicitações em linguagem natural com o Amazon Q in QuickSight para criar resumos dos dados, fazer perguntas e gerar histórias de dados. Você não precisa escrever consultas SQL ou aprender uma ferramenta de business intelligence (BI).

Contexto de negócios

Esse padrão apresenta uma solução para casos de uso de análises de dados de mainframe e insights de dados. Usando o padrão, você cria um painel visual para os dados da sua empresa. Para demonstrar a solução, esse padrão usa uma empresa de assistência médica que fornece planos médicos, odontológicos e oftalmológicos para seus membros nos EUA. Neste exemplo, as informações demográficas e do plano dos membros são armazenadas nas tabelas de dados do IBM Db2 for z/OS. O painel visual mostra o seguinte:

- Distribuição de membros por região
- Distribuição de membros por gênero
- Distribuição de membros por idade
- Distribuição de membros por tipo de plano

- Membros que não concluíram a imunização preventiva

Para exemplos de distribuição de membros por região e membros que não concluíram a imunização preventiva, consulte a seção Informações adicionais.

Depois de criar o painel, você gera uma história de dados que explica os insights da análise anterior. A história dos dados fornece recomendações para aumentar o número de membros que concluíram as imunizações preventivas.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS. Essa solução foi criada e testada no Amazon Linux 2 no Amazon Elastic Compute Cloud (Amazon EC2).
- Uma nuvem privada virtual (VPC) com uma sub-rede que pode ser acessada pelo seu sistema de mainframe.
- Um banco de dados de mainframe com dados comerciais. Para ver os dados de exemplo usados para criar e testar essa solução, consulte a seção Anexos.
- Captura de dados de alteração (CDC) ativada nas tabelas do Db2 z/OS. Para habilitar o CDC no Db2 z/OS, consulte a documentação da IBM.
- Conecte com precisão o CDC for z/OS instalado no sistema z/OS que está hospedando os bancos de dados de origem. A imagem Preciously Connect CDC for z/OS é fornecida como um arquivo zip dentro do AWS Mainframe Modernization - Data Replication for IBM z/OS Amazon Machine Image (AMI). Para instalar o Preciously Connect CDC for z/OS no mainframe, consulte a documentação de instalação do Precisely Connect.

Limitações

- Os dados do seu mainframe Db2 devem estar em um tipo de dados compatível com o Precisely Connect CDC. Para obter uma lista dos tipos de dados compatíveis, consulte a documentação do CDC do Precisely Connect.
- Seus dados no Amazon MSK devem estar em um tipo de dados compatível com o Amazon Redshift. Para obter uma lista dos tipos de dados compatíveis, consulte a documentação do Amazon Redshift.
- O Amazon Redshift tem comportamentos e limites de tamanho diferentes para diferentes tipos de dados. Para obter mais informações, consulte a documentação do Amazon Redshift.

- Os dados recebidos quase em tempo real QuickSight dependem do intervalo de atualização definido para o banco de dados do Amazon Redshift.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. No momento, o Amazon Q in QuickSight não está disponível em todas as regiões que oferecem suporte QuickSight. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Versões do produto

- AWS Mainframe Modernization Replicação de dados com a versão 4.1.44 do Precision
- Python versão 3.6 ou posterior
- Apache Kafka versão 3.5.1

Arquitetura

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para gerar insights de negócios a partir de dados de mainframe usando a replicação de AWS Mainframe Modernization dados com o Precisely e o Amazon Q in. QuickSight

O diagrama mostra o seguinte fluxo de trabalho:

1. O Preciously Log Reader Agent lê dados dos registros do Db2 e grava os dados em armazenamento temporário em um sistema de arquivos OMVS no mainframe.
2. O Publisher Agent lê os registros brutos do Db2 do armazenamento temporário.
3. O daemon do controlador local autentica, autoriza, monitora e gerencia as operações.
4. O Apply Agent é implantado na Amazon EC2 usando a AMI pré-configurada. Ele se conecta ao Publisher Agent por meio do daemon do controlador usando TCP/IP. O Apply Agent envia dados para o Amazon MSK usando vários trabalhadores para obter uma alta taxa de transferência.
5. Os trabalhadores gravam os dados no tópico do Amazon MSK no formato JSON. Como destino intermediário para as mensagens replicadas, o Amazon MSK fornece recursos de failover automatizados e altamente disponíveis.

6. A ingestão de streaming do Amazon Redshift fornece ingestão de dados de baixa latência e alta velocidade do Amazon MSK para um banco de dados Amazon Redshift Serverless. Um procedimento armazenado no Amazon Redshift realiza a reconciliação dos dados de alteração do mainframe (insert/update/deletes) nas tabelas do Amazon Redshift. Essas tabelas do Amazon Redshift servem como fonte de análise de dados para. QuickSight
7. Os usuários acessam os dados QuickSight para análises e insights. Você pode usar o Amazon Q in QuickSight para interagir com os dados usando prompts em linguagem natural.

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode iniciar quantos servidores virtuais precisar e escalá-los rapidamente para cima ou para baixo.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- O Amazon Managed Streaming for Apache Kafka (Amazon MSK) é um serviço totalmente gerenciado que ajuda você a criar e executar aplicações que usam o Apache Kafka para processar dados em streaming.
- QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel. Esse padrão usa os recursos generativos de BI do Amazon Q in QuickSight.
- O Amazon Redshift Serverless é uma opção sem servidor do Amazon Redshift que torna mais eficiente executar e escalar análises em segundos, sem a necessidade de configurar e gerenciar a infraestrutura de data warehouse.
- O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação.

Outras ferramentas

- O Precisely Connect CDC coleta e integra dados de sistemas legados em plataformas de nuvem e dados.

Repositório de código

O código desse padrão está disponível no repositório GitHub Mainframe_ DataInsights _change_data_reconciliation. O código é um procedimento armazenado no Amazon Redshift. Esse procedimento armazenado reconcilia as alterações de dados do mainframe (inserções, atualizações e exclusões) do Amazon MSK com as tabelas do Amazon Redshift. Essas tabelas do Amazon Redshift servem como fonte de análise de dados para. QuickSight

Práticas recomendadas

- Siga as melhores práticas ao configurar seu cluster Amazon MSK.
- Siga as melhores práticas de análise de dados do Amazon Redshift para melhorar o desempenho.
- Ao criar as funções AWS Identity and Access Management (IAM) para a configuração do Preciously, siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e Práticas recomendadas de segurança na documentação do IAM.

Épicos

Configure a replicação AWS Mainframe Modernization de dados com o Precisely on Amazon EC2

Tarefa	Descrição	Habilidades necessárias

Configure um grupo de segurança.	Para se conectar ao daemon do controlador e ao cluster Amazon MSK, crie um grupo de segurança para a instância . EC2 Adicione as seguintes regras de entrada e saída:
	• Regra de entrada 1:
	  • Em Tipo, escolha TCP personalizado.
	  • Para Protocolo, escolha TCP.
	  • Em Intervalo de portas, escolha 2626 (porta padrão para o daemon do controlador Preciousl
		DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	y) ou o número da porta do daemon do controlador em execução no mainframe. • Em Source, escolha Bloco CIDR. • Regra de entrada 2: • Em Type (Tipo), escolha Custom TCP (TCP personalizada). • Em Protocolo, escolha SSH. • Em Intervalo de portas, escolha 22. • Em Origem, escolha endereço IP ou lista de prefixos. • Regra de entrada 3: • Em Type (Tipo), escolha Custom TCP (TCP personalizada). • Para Protocolo, escolha TCP. • Em Intervalo de portas, escolha 9092-9098. • Em Source, escolha Bloco CIDR. • Regra de saída 1: • Em Type (Tipo), escolha Custom TCP (TCP personalizada).	

Tarefa	Descrição	Habilidades necessárias
	• Para Protocolo, escolha TCP. • Em Intervalo de portas, escolha 9092-9098. • Em Source, escolha Bloco CIDR. • Regra de saída 2: • Em Type (Tipo), escolha Custom TCP (TCP personalizada). • Para Protocolo, escolha TCP. • Em Intervalo de portas, escolha 2626 (porta padrão para o daemon do controlador Preciousl y) ou o número da porta do daemon do controlad or em execução no mainframe. • Em Source, escolha Bloco CIDR. Anote o nome do grupo de segurança. Você precisará referenciar o nome ao iniciar a EC2 instância e configurar o cluster Amazon MSK.	

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM e uma função do IAM.	1. Para criar uma política do IAM e uma função do IAM, siga as instruções na documentação da AWS. A política do IAM concede acesso para criar tópicos no cluster Amazon MSK e enviar dados para esses tópicos. 2. Depois de criar a função do IAM, associe a política a ela. Observe o nome da função do IAM. Essa função será usada como o perfil da instância do IAM quando você executar a EC2 instância.	DevOps engenheiro, administrador de sistemas da AWS

Tarefa	Descrição	Habilidades necessárias
Provisione uma EC2 instância.	Para provisionar uma EC2 instância para executar o Precisely CDC e conectar-se ao Amazon MSK, faça o seguinte: 1. Faça login no AWS Marketplace e assine o AWS Mainframe Modernization – Replicação de dados para IBM z/OS. 2. Selecione a AMI nas assinaturas gerenciadas e escolha Launch new instance. 3. Forneça outros detalhes de configuração, como nome da instância, tipo de instância, key pair, VPC e sub-redes. Para obter mais informações, consulte a EC2 documentação da Amazon. 4. Na lista suspensa, escolha o grupo de segurança que você criou anteriormente. 5. Em Detalhes avançados, perfil da instância do IAM, você deve selecionar a função que você criou anteriormente. 6. Escolha Iniciar instância.	Administrador e DevOps engenheiro da AWS

Configurar o Amazon MSK

Tarefa	Descrição	Habilidades necessárias
Crie o cluster do Amazon MSK.	Para criar um cluster Amazon MSK, faça o seguinte: 1. Faça login no AWS Management Console e abra o console do Amazon MSK em https://console.aws.amazon.com/msk/. 2. Selecione Criar cluster. 3. Para o método de criação de cluster, escolha Criação personalizada e, para o tipo de cluster, escolha Provisionado. 4. Forneça um nome para o cluster. 5. Atualize as configurações do cluster conforme necessário e mantenha os padrões para as outras configurações. 6. Observe a versão < Kafka>. Você precisará dele durante a configuração do cliente Kafka. 7. Escolha Próximo. 8. Escolha a mesma VPC e sub-redes que você usou para a EC2 instância Preciously e escolha o grupo de segurança que você criou anteriormente.	AWS DevOps, administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	9. Na seção Configurações de segurança, ative a autenticação baseada em funções SASL/SCRAM e IAM. O CDC do Precision Connect usa SASL/SCRAM (Simple Authentication and Security Layer/Salted Challenge Response Mechanism), e o IAM é necessário para se conectar ao Amazon Redshift. 10. Escolha Próximo. 11. Para análise, escolha o método de monitoramento e entrega de registros do Broker. 12. Escolha Avançar e, em seguida, escolha Criar o cluster. Um cluster provisionado típico leva até 15 minutos para ser criado. Depois que o cluster é criado, seu status muda de Criando para Ativo.	

Tarefa	Descrição	Habilidades necessárias
Configure a autenticação SASL/SCRAM.	Para configurar a autentica ção SASL/SCRAM para um cluster Amazon MSK, faça o seguinte: 1. Para configurar um segredo no Secrets Manager, siga as instruções na AWS documentação. 2. Abra o console do Amazon MSK e selecione o cluster do Amazon MSK que você criou anteriormente. 3. Escolha a guia Properties (Propriedades). 4. Escolha Associar segredos, Escolha os segredos, selecione a chave secreta que você criou e escolha Associar segredos. Você verá uma mensagem de sucesso semelhante à seguinte: `Successfully associated 1 secret for cluster <chosen cluster name>` 5. Escolha o nome do cluster. 6. No resumo do cluster, escolha Exibir informações do cliente.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	7. Observe a cadeia de conexão privada do endpoint para o tipo de autenticação SASL/SCRAM.	

Tarefa	Descrição	Habilidades necessárias

Crie o tópico do Amazon MSK.	Para criar o tópico do Amazon MSK, faça o seguinte:
	1. Conecte-se à EC2 instância que você criou anteriormente e instale as atualizações mais recentes executando o seguinte comando:
	`sudo yum update -y`
	2. Instale a biblioteca Java e Kafka executando o seguinte comando:
	`sudo yum install -y java-11 librdkafka librdkafka-devel`
	3. Para criar uma pasta chamada `kafka` in`/home/ec2-user` , navegue até essa pasta e execute o seguinte comando:
	`mkdir kafka;cd kafka`
	4. Faça o download da biblioteca do `kafka` cliente para a `kafka` pasta, `<YOUR MSK VERSION>` substituindo-a pela versão do Kafka que você anotou durante a criação do cluster Amazon MSK:
		Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	`wget https://archive.apache.org/dist/kafka//kafka_2.13-<YOUR MSK VERSION>.tgz`
	5. Para extrair o arquivo baixado, execute o seguinte comando, substituindo`YOUR MSK VERSION>`:
	`tar -xzf kafka_2.13-<YOUR MSK VERSION>.tgz`
	6. Para navegar até o `kafka libs` diretório e baixar o arquivo Java Archive (JAR) de autenticação do Java IAM, execute os seguintes comandos, substituindo`<YOUR MSK VERSION>`:
	`cd kafka_2.13-<YOUR MSK VERSION>/libs`
	`wget https://github.com/aws/aws-msk-iam-auth/releases/download/v1.1.1/aws-msk-iam-auth-1.1.1-all.jarkafka`
	7. Para navegar até o `bin` diretório do Kafka e criar o `client.properties`	

Tarefa	Descrição	Habilidades necessárias

	arquivo, execute os seguintes comandos:
	`cd /home/ec2-user/kafka/kafka_2.13-<YOUR MSK VERSION>/bin`
	`cat >client.properties`
	8. Atualize o `client.properties` arquivo com o seguinte conteúdo:
	`security.protocol=SASL_SSL`
	`sasl.mechanism=AWS_MSK_IAM`
	`sasl.jaas.config=software.amazon.msk.auth.iam.IAMLoginModule required;`
	`sasl.client.callback.handler.class=software.amazon.msk.auth.iam.IAMClientCallbackHandler`
	9. Para criar um tópico do Kafka, navegue até o compartimento do Kafka e execute o seguinte comando, <kafka broker> substituindo-o pelo endpoint privado do servidor de bootstrap do IAM que você observou durante a criação do cluster Amazon MSK:	

Tarefa	Descrição	Habilidades necessárias
	`./kafka-topics.sh --bootstrap-server <kafka broker> --command-config client.properties --create --replication-factor 3 –partitions 6 --topic <topic name>` 10. Quando a mensagem `Created topic <topic name>` aparecer, anote o nome do tópico.	

Configure o mecanismo de aplicação precisa na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Configure os scripts Precisely para replicar as alterações nos dados.	Para configurar os scripts do CDC Precisely Connect para replicar dados alterados do mainframe para o tópico do Amazon MSK, faça o seguinte: 1. Para criar um nome de pasta com precisão e mudar para essa pasta, execute o seguinte comando: `mkdir /home/ec2-user/precisely;cd /home/ec2-user/precisely`	Desenvolvedor de aplicativos, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias

	2. Para criar duas pastas dentro precisamente chamadas de `scripts` e `eddls`, em seguida, mudar para a `scripts` pasta, execute o seguinte comando:
	`mkdir scripts;mkdir ddls;cd scripts`
	3. Para criar um arquivo nomeado `sqdata_kafka_producer.conf` na `scripts` pasta, execute o seguinte comando:
	`cat >sqdata_kafka_producer.conf`
	4. Atualize o `sqdata_kafka_producer.conf` arquivo com o seguinte conteúdo:
	`builtin.features=SASL_SCRAM`
	`security.protocol=SASL_SSL`
	`sasl.mechanism=SCRAM-SHA-512`
	`sasl.username=<User Name>`
	`sasl.password=<Password>`
	`metadata.broker.list=<SASL/SCRAM Bootstrap servers>`	

Tarefa	Descrição	Habilidades necessárias
	Note Atualize `<SASL/SCRAM Bootstrap servers>` com a lista de agentes Amazon MSK SASL/SCRAM que você configuro u anteriorm ente. Atualize `<User Name>` e `<Password>` com o nome de usuário e senha que você configuro u anteriormente no Secrets Manager. 5. Crie um `script.sqd` arquivo na `scripts` pasta. `cat >script.sqd` O Apply Engine usa `script.sqd` para processar dados de origem e replicar os dados de origem para o destino. Para ver um exemplo de script do Apply Engine, consulte a seção Informaçõ es adicionais.	

Tarefa	Descrição	Habilidades necessárias

	6. Para mudar para a `ddls` pasta e criar um arquivo.ddl para cada tabela do Db2, execute os seguintes comandos:
	
	`cd /home/ec2-user/precisely/ddls`
	`cat >mem_details.ddl`
	`cat >mem_plans.ddl`
	
	Por exemplo, arquivos.ddl, consulte a seção Informações adicionais.	

Tarefa	Descrição	Habilidades necessárias

Gere a chave ACL da rede.	Para gerar a chave da lista de controle de acesso à rede (Network ACL), faça o seguinte:
	
	1. Para exportar o caminho de `sqdata` instalação, execute o seguinte comando:
	
	`export PATH=$PATH:/usr/sbin:/opt/precisely/di/sqdata/bin`
	
	2. Para mudar para o `/home/ec2-user` diretório e gerar a chave ACL de rede, execute os seguintes comandos:
	
	`cd /home/ec2-user`
	`sqdutil keygen --force`
	
	Depois que as chaves públicas e privadas são geradas, a seguinte mensagem é exibida:
	
	`SQDUT04I Generating a private key in file /home/ec2-user/.nacl/id_nacl`
	`SQDC017I sqdutil(pid=27344) terminated successfully`
		Arquiteto de nuvem, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	3. Observe a chave pública gerada que está armazenada na `.nacl` pasta.	

Prepare o ambiente de origem do mainframe

Tarefa	Descrição	Habilidades necessárias
Configure os padrões na tela do ISPF.	Para definir as configurações padrão no Interactive System Productivity Facility (ISPF), siga as instruções na documentação do Precisely.	Administrador do sistema de mainframe
Configure o daemon do controlador.	Para configurar o daemon do controlador, faça o seguinte: 1. Na tela do menu principal do SQData z/OS, escolha a opção 2. 2. Na tela Adicionar Daemon à Lista, no campo Nome do Daemon, insira um nome para o daemon e pressione Enter.	Administrador do sistema de mainframe
Configure o editor.	Para configurar o editor, faça o seguinte: 1. Na tela do menu principal do SQData z/OS, escolha a opção 3. Isso leva você para a tela de resumo do Capture/Publisher.	Administrador do sistema de mainframe

Tarefa	Descrição	Habilidades necessárias
	2. Escolha a opção para adicionar um arquivo CAB. Isso o levará para a tela Adicionar arquivo CAB à lista. 3. No campo Nome, insira um nome para o arquivo CAB. Para Db2, insira o Tipo comoD. 4. Pressione Enter. Isso leva você para a tela Create New Db2 Capture CAB File. 5. No campo zFS Dir, especifique o ponto de montagem do armazenam ento. 6. Pressione Enter para salvar e continuar.	

Tarefa	Descrição	Habilidades necessárias
Atualize o arquivo de configuração do daemon.	Para atualizar os detalhes do editor no arquivo de configuração do daemon do controlador, faça o seguinte: 1. Na tela do menu principal do SQData z/OS, escolha a opção 2. 2. Entre S perto do daemon que você criou para ver os detalhes do daemon. 3. Enter e1, em seguida, pressione Enter para editar o arquivo do agente. 4. Adicione os detalhes do seu arquivo CAB. O exemplo a seguir mostra os detalhes de um arquivo CAB chamado`DB2ZTOMSK`. Use seu ID de usuário do mainframe em vez de. `<userid>` `ÝDB2ZTOMSK¨ type=capture cab=/u/<userid>/sqdata/DB2ZTOMSK.cab` 5. Pressione F3. 6. Digite 2 para editar o arquivo ACL. Adicione seu `userid` ao arquivo `acl` de configuração conforme mostrado no exemplo a seguir:	Administrador do sistema de mainframe

Tarefa	Descrição	Habilidades necessárias
	`Ýacls¨ prod=admin,<userid>` 7. Pressione F3 para salvar e sair.	
Crie o trabalho para iniciar o daemon do controlador.	Para criar o trabalho, faça o seguinte: 1. Em Opções, insira`G`. 2. Insira o cartão de trabalho, as bibliotecas de tarefas e processos e os detalhes `Db2 load` da biblioteca. 3. Insira os detalhes do arquivo ACL de rede e insira a opção 2 para gerar o arquivo de linguagem de controle de tarefas (JCL) na biblioteca de tarefas especificada.	Administrador do sistema de mainframe

Tarefa	Descrição	Habilidades necessárias
Gere o arquivo JCL do editor de captura.	Para gerar o arquivo JCL do editor de captura, faça o seguinte: 1. Na tela do menu principal do SQData z/OS, escolha a opção 3. Isso leva você para a tela de resumo do Capture/Publisher. 2. Digite `S` ao lado do arquivo CAB para selecioná-lo. Isso leva você para a tela de detalhes do Db2 Capture/Publisher. 3. Em Opções, insira `G` as opções para gerar o `capture/publisher` trabalho. 4. Insira o cartão JOB, as bibliotecas de tarefas e procedimentos e os detalhes da biblioteca de carga do Db2. 5. Para criar o trabalho, escolha a opção 4. O trabalho é criado na biblioteca de trabalhos especificada na biblioteca de trabalhos.	Administrador do sistema de mainframe

Tarefa	Descrição	Habilidades necessárias

Verifique e atualize o CDC.	1. Verifique o `DATACAPTURE` sinalizador da tabela Db2 executando a consulta a seguir, alterando `<table name>` para o nome da tabela Db2:
	`SELECT DATACAPTURE FROM SYSIBM.SYSTABLES WHERE NAME='<table name>';`
	Confirme se o resultado é exibido `DATACAPTURE` como`Y`.
	2. Se não `DATACAPTURE` estiver`Y`, execute a consulta a seguir para habilitar o CDC na tabela Db2, alterando `<table name>` para o nome da tabela Db2:
	`ALTER TABLE <table name> DATA CAPTURE CHANGES;`
		Administrador do sistema de mainframe

Tarefa	Descrição	Habilidades necessárias
Envie os arquivos JCL.	Envie os seguintes arquivos JCL que você configurou nas etapas anteriores: • Arquivo JCL para iniciar o daemon do controlador • Arquivo JCL para iniciar a captura e publicação Depois de enviar os arquivos JCL, você pode iniciar o Apply Engine em Precisly na EC2 instância.	Administrador do sistema de mainframe

Execute e valide o CDC

Tarefa	Descrição	Habilidades necessárias
Inicie o Apply Engine e valide o CDC.	Para iniciar o Apply Engine na EC2 instância e validar o CDC, faça o seguinte: 1. Para se conectar à EC2 instância, siga as instruções na AWS documentação. 2. Vá para o diretório que contém o `script.sqd` arquivo: `cd /home/ec2-user/precisely/scripts`	Arquiteto de nuvem, desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	3. Para iniciar o Apply Engine, execute o seguinte comando `sqdeng` start: `sqdeng -s script.sqd --identity=/home/ec2-user/.nacl/id_nacl` O Apply Engine começará a aguardar atualizações da fonte do mainframe. 4. Para testar o CDC, faça algumas inserções ou atualizações de registros na tabela Db2. 5. Verifique se o registro do Apply Engine mostra o número de registros capturados e gravados no destino.	

Tarefa	Descrição	Habilidades necessárias

Valide os registros no tópico do Amazon MSK.	Para ler a mensagem do tópico Kafka, faça o seguinte:
	1. Para mudar para o `bin` diretório do caminho de instalação do cliente Kafka na EC2 instância, execute o comando a seguir, `<Kafka version>` substituindo-o pela sua versão:
	`cd /home/ec2-user/kafka/kafka_2.13-<Kafka version>/bin`
	2. Para validar o Db2 CDC escrito como mensagens no tópico do Kafka, execute o comando a seguir, substituindo `<kafka broker>` e pelo tópico que você `<Topic Name>` criou anteriormente:
	`./kafka-console-consumer.sh --bootstrap-server <kafka broker>:9098 --topic <Topic Name> --from-beginning --consumer.config client.properties`
	3. Valide se as mensagens correspondem ao número
		Desenvolvedor de aplicativos, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	de registros atualizados na tabela Db2.	

Armazene dados de alteração do mainframe em um armazém de dados sem servidor do Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Configure o Amazon Redshift Serverless.	Para criar um armazém de dados sem servidor do Amazon Redshift, siga as instruções na documentação.AWS No painel do Amazon Redshift Serverless, valide se o namespace e o grupo de trabalho foram criados e estão disponíveis. Para esse exemplo de padrão, o processo pode levar de 2 a 5 minutos.	Engenheiro de dados
Configure a função do IAM e a política de confiança necessárias para a ingestão de streaming.	Para configurar a ingestão de streaming sem servidor do Amazon Redshift a partir do Amazon MSK, faça o seguinte: 1. Crie uma política do IAM para o Amazon Redshift acessar o Amazon MSK. `[region]`Substituindo Região da AWS pelo do Amazon MSK, `[account-`	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	id] pelo seu Conta da AWS ID e [msk-cluster-name] pelo nome do cluster do Amazon MSK, execute o seguinte código: `{"Version": "2012-10-17","Statement": [{"Sid": "MSKIAMpolicy","Effect": "Allow","Action": ["kafka-cluster:ReadData","kafka-cluster:DescribeTopic","kafka-cluster:Connect"],"Resource": ["arn:aws:kafka:[region]:[account-id]:cluster/[msk-cluster-name]/*","arn:aws:kafka:[region]:[account-id]:topic/[msk-cluster-name]/*"]},{"Effect": "Allow","Action": ["kafka-cluster:AlterGroup","kafka-cluster:DescribeGroup"],"Resource": ["arn:aws:kafka:[region]:[account-id]:group/[msk-cluster-name]/*"]}]}`	

Tarefa	Descrição	Habilidades necessárias
	Você pode encontrar o nome do cluster e o Amazon Resource Name (ARN) no console do Amazon MSK. No console, escolha Resumo do cluster e, em seguida, escolha ARN. 2. Para criar uma função do IAM e anexar a política, siga as instruções na AWS documentação. 3. Para anexar a função do IAM ao namespace Amazon Redshift Serverless, faça o seguinte: a. Faça login no console e abra o console do Amazon Redshift em. https://console.aws.amazon.com/redshiftv2/ b. Escolha o Serverless dashboard (Painel do Serverless). c. Escolha Namespace. d. Escolha a guia Segurança e criptografia. e. Escolha Permissão e anexe a função do IAM que você criou.	

Tarefa	Descrição	Habilidades necessárias
	4. Em seu grupo de segurança Amazon Redshift Serverless, crie uma regra de entrada com os seguintes detalhes: • Em Type (Tipo), escolha Custom TCP (TCP personalizada). • Para Protocolo, escolha TCP. • Em Intervalo de portas, escolha 9098, 9198. • Em Source, escolha o grupo de segurança Amazon MSK. 5. No seu grupo de segurança do Amazon MSK, crie uma regra de entrada com os seguintes detalhes: • Em Type (Tipo), escolha Custom TCP (TCP personalizada). • Para Protocolo, escolha TCP. • Em Intervalo de portas, escolha 9098, 9198. • Em Source, escolha o grupo de segurança do Amazon Redshift. Esse padrão usa a porta para autenticação do IAM para a configuração do	

Tarefa	Descrição	Habilidades necessárias
	Amazon Redshift e do Amazon MSK. Para obter mais informações, consulte a AWS documentação (etapa 2). 6. Ative o roteamento de VPC aprimorado para o grupo de trabalho Amazon Redshift Serverless. Para obter mais informações, consulte a documentação do AWS.	
Conecte o Amazon Redshift Serverless ao Amazon MSK.	Para se conectar ao tópico do Amazon MSK, crie um esquema externo no Amazon Redshift Serverless. No editor de consultas v2 do Amazon Redshift, execute o seguinte comando SQL, substituindo `'iam_role_arn'` pela função que você criou anteriormente e substituindo `'MSK_cluster_arn'` pelo ARN do seu cluster. `CREATE EXTERNAL SCHEMA member_schema FROM MSK IAM_ROLE 'iam_role_arn' AUTHENTICATION iam URI 'MSK_cluster_arn';`	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Crie uma visão materializada.	Para consumir os dados do tópico Amazon MSK no Amazon Redshift Serverless, crie uma visualização materializada. No editor de consultas v2 do Amazon Redshift, execute os seguintes comandos SQL, `<MSK_Topic_name>` substituindo-os pelo nome do seu tópico do Amazon MSK. `CREATE MATERIALIZED VIEW member_view AUTO REFRESH YES AS SELECT kafka_partition, kafka_offset, refresh_time, json_parse(kafka_value) AS Data FROM member_schema.<MSK_Topic_name> WHERE CAN_JSON_PARSE(kafka_value);`	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias

Crie tabelas de destino no Amazon Redshift.	As tabelas do Amazon Redshift fornecem a entrada para. QuickSight Esse padrão usa as tabelas `member_dtls` `ememberplans` , que correspondem às tabelas Db2 de origem no mainframe.
	
	Para criar as duas tabelas no Amazon Redshift, execute os seguintes comandos SQL no editor de consultas v2 do Amazon Redshift:
	
	`-- Table 1: members_dtls`
	`CREATE TABLE members_dtls (`
	`memberid INT ENCODE AZ64,`
	`member_name VARCHAR(100) ENCODE ZSTD,`
	`member_type VARCHAR(50) ENCODE ZSTD,`
	`age INT ENCODE AZ64,`
	`gender CHAR(1) ENCODE BYTEDICT,`
	`email VARCHAR(100) ENCODE ZSTD,`
	`region VARCHAR(50) ENCODE ZSTD`
	`) DISTSTYLE AUTO;`
	
	`-- Table 2: member_plans`
	`CREATE TABLE member_plans (`
	`memberid INT ENCODE AZ64,`
		Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	``` medical_plan CHAR(1) ENCODE BYTEDICT, dental_plan CHAR(1) ENCODE BYTEDICT, vision_plan CHAR(1) ENCODE BYTEDICT, preventive_immuniz ation VARCHAR(50) ENCODE ZSTD) DISTSTYLE AUTO; ```	
Crie um procedimento armazenado no Amazon Redshift.	Esse padrão usa um procedimento armazenado para sincronizar dados de alteração (`INSERT`,`UPDATE`,`DELETE`) do mainframe de origem com a tabela de armazenamento de dados de destino do Amazon Redshift para análise em. QuickSight Para criar o procedimento armazenado no Amazon Redshift, use o editor de consultas v2 para executar o código do procedimento armazenado que está no repositório. GitHub	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
Leia a partir da visualização materializada de streaming e carregue nas tabelas de destino.	O procedimento armazenado lê as alterações de dados da visualização materializada de streaming e carrega as alterações de dados nas tabelas de destino. Para executar o procedimento armazenado, use o seguinte comando: `call SP_Members_Load();` Você pode usar EventBridge a Amazon para programar os trabalhos em seu armazém de dados do Amazon Redshift para chamar esse procedimento armazenado com base em seus requisitos de latência de dados. EventBridge executa trabalhos em intervalos fixos. Para monitorar se a chamada anterior para o procedimento foi concluída, talvez seja necessário usar um mecanismo como uma máquina de AWS Step Functionsestado. Para obter mais informações, consulte os seguintes recursos: • Criação de uma EventBridge regra da Amazon que é	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	executada de acordo com um cronograma • Acelere a orquestração de um processo de ELT usando a API de dados do Amazon AWS Step Functions Redshift. Outra opção é usar o editor de consultas v2 do Amazon Redshift para programar a atualização. Para obter mais informações, consulte Agendamento de uma consulta com o editor de consultas v2.	

Conecte-se QuickSight aos dados no Amazon Redshift

Tarefa	Descrição	Habilidades necessárias
Configurar QuickSight.	Para configurar QuickSight, siga as instruções na AWS documentação.	Engenheiro de migração
Configure uma conexão segura entre QuickSight e o Amazon Redshift.	Para configurar uma conexão segura entre o Amazon Redshift QuickSight e o Amazon Redshift, faça o seguinte 1. Para autorizar conexões do QuickSight Amazon Redshift, abra o console do	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	Amazon Redshift e adicione uma regra de entrada no grupo de segurança do Amazon Redshift. A regra deve permitir o tráfego para a porta 5439 (a porta padrão do Redshift) a partir do intervalo CIDR em que você configurou. QuickSight Para obter uma lista de Regiões da AWS e seus endereços IP, consulte Compatível com Regiões da AWS QuickSight. 2. No console do Amazon Redshift, escolha Grupo de trabalho, acesso a dados, rede e segurança e habilite o acesso público.	

Tarefa	Descrição	Habilidades necessárias
Crie um conjunto de dados para QuickSight.	Para criar um conjunto de dados QuickSight do Amazon Redshift, faça o seguinte: 1. No QuickSight console, no painel de navegação , escolha Conjuntos de dados. 2. Na página Conjuntos de dados, escolha Novo conjunto de dados. 3. Escolha Conexão manual do Redshift. 4. Na janela Nova fonte de dados do Redshift, insira as informações de conexão: • Em Nome da fonte de dados, insira um nome para a fonte de dados do Amazon Redshift. • Em Servidor de banco de dados, insira o endpoint do cluster Amazon Redshift. Você pode obter o valor do endpoint no campo Endpoint na seção Informaçõ es gerais do grupo de trabalho do cluster no painel do Amazon Redshift Serverless. O endereço do servidor é a primeira parte do endpoint antes dos	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	dois pontos, conforme mostrado no exemplo a seguir: `mfdata-insights.NNNNNNNN.us-east-1.redshift-serverless.amazonaws.com:5439/dev` • Para a porta, insira `5439` (a porta padrão para o Amazon Redshift). • Insira o nome do banco de dados (após a barra no endpoint). Nesse caso, o nome do banco de dados é `dev`. • Em Nome de usuário e senha, insira o nome de usuário e a senha do banco de dados do Amazon Redshift. 5. Escolha Validar conexão. Se for bem-sucedido, você deverá ver uma marca de seleção verde, que indica validação. Se a validação falhar, consulte a seção Solução de problemas. 6. Escolha Criar fonte de dados.	

Tarefa	Descrição	Habilidades necessárias
Junte-se ao conjunto de dados.	Para criar análises em QuickSight, junte as duas tabelas seguindo as instruções na AWS documentação. No painel Configuração de junção, escolha Esquerda para o tipo de junção. Em Cláusulas de união, use `memberid from member_plans = memberid from members_details` .	Engenheiro de migração

Obtenha insights de negócios a partir dos dados do mainframe usando o Amazon Q em QuickSight

Tarefa	Descrição	Habilidades necessárias
Configure o Amazon Q em QuickSight.	Para configurar o recurso Amazon Q in QuickSight Generative BI, siga as instruções na AWS documentação.	Engenheiro de migração
Analise os dados do mainframe e crie um painel visual.	Para analisar e visualizar seus dados em QuickSight, faça o seguinte: 1. Para criar a análise de dados do mainframe, siga as instruções na AWS documentação. Para o conjunto de dados, escolha o conjunto de dados que você criou.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	2. Na página de análise, escolha Criar visual. 3. Na janela Criar tópico para análise, escolha Atualizar tópico existente. 4. Na lista suspensa Selecionar um tópico, escolha o tópico que você criou anteriormente. 5. Escolha Vinculação de tópicos. 6. Depois de vincular o tópico, escolha Criar visual para abrir a janela Amazon Q Build a Visual. 7. Na barra de prompts, escreva suas perguntas de análise. Os exemplos de perguntas usadas para esse padrão são os seguintes: • Mostrar distribuição de membros por região • Mostrar distribuição de membros por idade • Mostrar distribuição de membros por gênero • Mostrar distribuição de membros por tipo de plano • Mostrar aos membros que não concluíram a imunização preventiva	

Tarefa	Descrição	Habilidades necessárias
	Depois de inserir suas perguntas, escolha Criar. O Amazon Q in QuickSight cria os recursos visuais. 8. Para adicionar os elementos visuais ao seu painel visual, escolha ADICIONAR À ANÁLISE. Ao terminar, você poderá publicar seu painel para compartilhar com outras pessoas em sua organização. Para ver exemplos, consulte Painel visual do mainframe na seção Informações adicionais.	

Crie uma história de dados com o Amazon Q a QuickSight partir de dados do mainframe

Tarefa	Descrição	Habilidades necessárias
Crie uma história de dados.	Crie uma história de dados para explicar os insights da análise anterior e gere uma recomendação para aumentar a imunização preventiva dos membros: 1. Para criar a história de dados, siga as instruções na AWS documentação. 2. Para o prompt da história de dados, use o seguinte:	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	`Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunizat ion. Include 4 points of supportin g data for this pattern.` Você também pode criar seu próprio prompt para gerar histórias de dados para outros insights de negócios. 3. Escolha Adicionar elementos visuais e adicione os elementos visuais que são relevantes para a história dos dados. Para esse padrão, use as imagens que você criou anteriormente. 4. Escolha Criar. 5. Por exemplo, saída da história de dados, consulte Saída da história de dados	

Tarefa	Descrição	Habilidades necessárias
	na seção Informações adicionais.	
Veja a história de dados gerada.	Para ver a história de dados gerada, escolha essa história na página Histórias de dados.	Engenheiro de migração
Edite uma história de dados gerada.	Para alterar a formatação, o layout ou os elementos visuais em uma história de dados, siga as instruções na AWS documentação.	Engenheiro de migração
Compartilhe uma história de dados.	Para compartilhar uma história de dados, siga as instruções na AWS documentação.	Engenheiro de migração

Solução de problemas

Problema	Solução
QuickSight Para a criação do conjunto de dados do Amazon Redshift, `Validate Connection` falhou.	1. Confirme se o grupo de segurança vinculado à instância do Amazon Redshift Serverless permite tráfego de entrada do intervalo de endereços IP associado à região em que você configurou. QuickSight 2. Confirme se a VPC na qual o Amazon Redshift Serverless está implantado está disponível publicamente. 3. Confirme se você está usando o nome de usuário e a senha corretos para o Amazon Redshift. Você pode redefinir o nome de usuário e a senha no console do Amazon Redshift.

Problema	Solução
A tentativa de iniciar o mecanismo de aplicação na EC2 instância retorna o seguinte erro: `-bash: sqdeng: command not found`	Exporte o caminho de `sqdata` instalação executando o seguinte comando: `export PATH=$PATH:/usr/sbin:/opt/precisely/di/sqdata/bin`
A tentativa de iniciar o Apply Engine retorna um dos seguintes erros de conexão: • `SQDD018E Cannot connect to transfer socket(rc==0x18468). Agent:<Agent Name > Socket:/u/./sqdata/.DB2ZTOMSK.cab.data` • `SQDUR06E Error opening url cdc://<VPC end point name>:2626/DB2ZTOMSK/DB2ZTOMSK : errno:1128 (Unknown error 1128)`	Verifique o spool do mainframe para garantir que os trabalhos do daemon do controlador estejam em execução.

Recursos relacionados

- Gere insights usando AWS Mainframe Modernization o Amazon Q in QuickSight (padrão)
- Gere insights de dados usando o AWS Mainframe Modernization Amazon Q in QuickSight (demonstração)
- AWS Mainframe Modernization - Replicação de dados para IBM z/OS
- Ingestão de streaming do Amazon Redshift para uma visualização materializada

Mais informações

Exemplo de arquivos.ddl

members_details.ddl

```
CREATE TABLE MEMBER_DTLS (
memberid INTEGER NOT NULL,
```

```
member_name VARCHAR(50),
member_type VARCHAR(20),
age INTEGER,
gender CHAR(1),
email VARCHAR(100),
region VARCHAR(20)
);
```

planos_do_membros.ddl

```
CREATE TABLE MEMBER_PLANS (
memberid INTEGER NOT NULL,
medical_plan CHAR(1),
dental_plan CHAR(1),
vision_plan CHAR(1),
preventive_immunization VARCHAR(20)
);
```

Exemplo de arquivo.sqd

<kafka topic name>Substitua pelo nome do tópico do Amazon MSK.

script.sqd

```
-- Name: DB2ZTOMSK: DB2z To MSK JOBNAME DB2ZTOMSK;REPORT EVERY 1;OPTIONS
 CDCOP('I','U','D');-- Source Descriptions
JOBNAME DB2ZTOMSK;
REPORT EVERY 1;
OPTIONS CDCOP('I','U','D');

-- Source Descriptions
BEGIN GROUP DB2_SOURCE;
DESCRIPTION DB2SQL /var/precisely/di/sqdata/apply/DB2ZTOMSK/ddl/mem_details.ddl AS
 MEMBER_DTLS;
DESCRIPTION DB2SQL /var/precisely/di/sqdata/apply/DB2ZTOMSK/ddl/mem_plans.ddl AS
 MEMBER_PLANS;
END GROUP;
-- Source Datastore
DATASTORE cdc://<zos_host_name>/DB2ZTOMSK/DB2ZTOMSK
OF UTSCDC
AS CDCIN
DESCRIBED BY GROUP DB2_SOURCE ;
-- Target Datastore(s)
```

```
DATASTORE 'kafka:///<kafka topic name>/key'
OF JSON
AS TARGET
DESCRIBED BY GROUP DB2_SOURCE;
PROCESS INTO TARGET
SELECT
{
REPLICATE(TARGET)
}
FROM CDCIN;
```

Painel visual do mainframe

O visual de dados a seguir foi criado pela Amazon Q QuickSight para a pergunta de análise `show member distribution by region`.

O visual de dados a seguir foi criado pela Amazon Q QuickSight para a pergunta`show member distribution by Region who have not completed preventive immunization, in pie chart`.

Saída da história de dados

As capturas de tela a seguir mostram seções da história de dados criada pela Amazon Q QuickSight para o prompt`Build a data story about Region with most numbers of members. Also show the member distribution by age, member distribution by gender. Recommend how to motivate members to complete immunization. Include 4 points of supporting data for this pattern`.

Na introdução, a história dos dados recomenda escolher a região com mais membros para obter o maior impacto dos esforços de imunização.

A história dos dados fornece uma análise do número de membros das quatro regiões. As regiões Nordeste, Sudoeste e Sudeste têm o maior número de membros.

A história dos dados apresenta uma análise dos membros por idade.

A história dos dados se concentra nos esforços de imunização no Centro-Oeste.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Gere insights de dados usando o AWS Mainframe Modernization e o Amazon Q em QuickSight

Criado por Shubham Roy (AWS), Roshna Razack (AWS) e Santosh Kumar Singh (AWS)

Resumo

Se sua organização está hospedando dados essenciais para os negócios em um ambiente de mainframe, obter insights desses dados é crucial para impulsionar o crescimento e a inovação. Ao desbloquear dados do mainframe, você pode criar inteligência de negócios mais rápida, segura e escalável para acelerar a tomada de decisões, o crescimento e a inovação orientados por dados na nuvem da Amazon Web Services ().AWS

Esse padrão apresenta uma solução para gerar insights de negócios e criar narrativas compartilháveis a partir de dados de mainframe usando o AWS Mainframe Modernization File Transfer com BMC e Amazon Q in. QuickSight Os conjuntos de dados de mainframe são transferidos para o Amazon Simple Storage Service (Amazon S3) usando o AWS Mainframe Modernization File Transfer com a BMC. Uma AWS Lambda função formata e prepara o arquivo de dados do mainframe para carregamento na Amazon. QuickSight

Depois que os dados estiverem disponíveis QuickSight, você poderá usar solicitações em linguagem natural com o Amazon Q in QuickSight para criar resumos dos dados, fazer perguntas e gerar histórias de dados. Você não precisa escrever consultas SQL ou aprender uma ferramenta de business intelligence (BI).

Contexto de negócios

Esse padrão apresenta uma solução para casos de uso de análises de dados de mainframe e insights de dados. Usando o padrão, você cria um painel visual para os dados da sua empresa. Para demonstrar a solução, esse padrão usa uma empresa de assistência médica que fornece planos médicos, odontológicos e oftalmológicos para seus membros nos EUA. Neste exemplo, as informações demográficas e do plano dos membros são armazenadas nos conjuntos de dados do mainframe. O painel visual mostra o seguinte:

- Distribuição de membros por região
- Distribuição de membros por gênero
- Distribuição de membros por idade
- Distribuição de membros por tipo de plano

- Membros que não concluíram a imunização preventiva

Depois de criar o painel, você gera uma história de dados que explica os insights da análise anterior. A história dos dados fornece recomendações para aumentar o número de membros que concluíram as imunizações preventivas.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Conjuntos de dados de mainframe com dados comerciais
- Acesso para instalar um agente de transferência de arquivos no mainframe

Limitações

- Seu arquivo de dados do mainframe deve estar em um dos formatos de arquivo suportados pelo QuickSight. Para obter uma lista dos formatos de arquivo compatíveis, consulte a QuickSight documentação da Amazon.

  Esse padrão usa uma função Lambda para converter o arquivo de mainframe em um formato suportado pelo. QuickSight

Arquitetura

O diagrama a seguir mostra uma arquitetura para gerar insights de negócios a partir de dados de mainframe usando o AWS Mainframe Modernization File Transfer com BMC e Amazon Q in. QuickSight

O diagrama mostra o seguinte fluxo de trabalho:

1. Um conjunto de dados de mainframe contendo dados comerciais é transferido para o Amazon S3 AWS Mainframe Modernization usando o File Transfer with BMC.
2. A função Lambda converte o arquivo que está no bucket S3 de destino da transferência de arquivos para o formato de valores separados por vírgula (CSV).
3. A função Lambda envia o arquivo convertido para o bucket S3 do conjunto de dados de origem.

4. Os dados no arquivo são ingeridos por QuickSight.
5. Os usuários acessam os dados em QuickSight. Você pode usar o Amazon Q in QuickSight para interagir com os dados usando prompts em linguagem natural.

Ferramentas

Serviços da AWS

- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Mainframe Modernization O File Transfer with BMC converte e transfere conjuntos de dados de mainframe para o Amazon S3 para casos de uso de modernização, migração e aumento de mainframe.
- QuickSightA Amazon é um serviço de BI em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel. Esse padrão usa os recursos generativos de BI do Amazon Q in QuickSight.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Práticas recomendadas

- Ao criar as funções AWS Identity and Access Management (IAM) para transferência de AWS Mainframe Modernization arquivos com BMC e a função Lambda, siga o princípio do privilégio mínimo.
- Certifique-se de que seu conjunto de dados de origem tenha tipos de dados compatíveis para QuickSight. Se o conjunto de dados de origem contiver tipos de dados não compatíveis, converta-os em tipos de dados compatíveis. Para obter informações sobre tipos de dados de mainframe não suportados e como convertê-los em tipos de dados compatíveis com o Amazon Q in QuickSight, consulte a seção Recursos relacionados.

Épicos

Configurar a transferência AWS Mainframe Modernization de arquivos com o BMC

Tarefa	Descrição	Habilidades necessárias
Instale o agente de transferência de arquivos.	Para instalar o AWS Mainframe Modernization File Transfer Agent em seu mainframe, siga as instruções na AWS documentação.	Administrador do sistema de mainframe
Crie um bucket S3 para transferência de arquivos de mainframe.	Crie um bucket do S3 para armazenar o arquivo de saída do AWS Mainframe Modernization File Transfer with BMC. No diagrama da arquitetura, esse é o bucket de destino da transferência de arquivos.	Engenheiro de migração
Crie o endpoint de transferência de dados.	1. Crie um bucket S3 para preparar o arquivo de entrada do mainframe para transferência de arquivos com AWS Mainframe Modernization o BMC. 2. Para criar o endpoint de transferência de dados do mainframe, siga as instruções na AWS documentação.	Especialista em modernização de mainframe da AWS

Converta a extensão do nome do arquivo do mainframe para integração QuickSight

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Crie um bucket do S3 para a função Lambda para copiar o arquivo de mainframe convertido do bucket de origem para o bucket de destino final.	Engenheiro de migração
Crie uma função do Lambda.	Para criar uma função Lambda que altere a extensão do arquivo e copie o arquivo do mainframe para o bucket de destino, faça o seguinte: 1. Faça login no e AWS Management Console navegue até o AWS Lambda console. 2. Escolha Criar função e, em seguida, escolha Autor do zero. 3. Em Nome da função, insira um nome para sua função. 4. Na lista suspensa Tempo de execução, escolha Python.3.X. 5. Expanda Alterar função de execução padrão e escolha Criar uma nova função com permissões básicas do Lambda. 6. Escolha a opção Criar função.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	7. Escolha a guia Código e cole o código `S3CopyLambda.py` Python fornecido na seção Informações adicionais. O código Python foi gerado usando o Amazon Q Developer no ambiente de desenvolvimento integrado (IDE) do Microsoft Visual Studio. 8. Edite `destination_bucket_name` o no nome do bucket do S3 que você criou anteriormente e `change destination_file_key` no nome do arquivo do mainframe. 9. Implante a função do Lambda.	

Tarefa	Descrição	Habilidades necessárias
Crie um gatilho do Amazon S3 para invocar a função Lambda.	Para configurar um gatilho que invoca a função Lambda, faça o seguinte: 1. No console do Lambda, abra a página Funções. 2. Escolha a função Lambda. 3. Em Visão geral da função, escolha Adicionar gatilho. 4. Na lista suspensa Configuração do acionador, escolha S3. 5. No campo Bucket, insira o nome do seu bucket de origem. 6. Na lista suspensa Tipo de evento, escolha Todos os eventos criados por objetos. 7. Marque a caixa de seleção Eu reconheço que usar o mesmo bucket do S3 para entrada e saída não é recomendado e, em seguida, escolha Adicionar. Para obter mais informações, consulte Tutorial: Como usar um trigger do Amazon S3 para chamar uma função Lambda.	Líder de migração

Tarefa	Descrição	Habilidades necessárias
Forneça permissões do IAM para a função Lambda.	As permissões do IAM são necessárias para que a função Lambda acesse o destino da transferência de arquivos e os buckets S3 do conjunto de dados de origem. Atualize a política associada à função de execução da função Lambda permitindo `s3:GetObject` e `s3:DeleteObject` autorizando o bucket S3 de destino da transferência de arquivos e `s3:PutObject` acessando o bucket S3 do conjunto de dados de origem. Para obter mais informaçõ es, consulte a seção Criar uma política de permissões no Tutorial: Usando um gatilho do Amazon S3 para invocar uma função Lambda.	Líder de migração

Defina uma tarefa de transferência de dados de mainframe

Tarefa	Descrição	Habilidades necessárias
Crie uma tarefa de transferê ncia para copiar o arquivo do mainframe para o bucket do S3.	Para criar uma tarefa de transferência de arquivos de mainframe, siga as instruções na AWS Mainframe Moderniza tion documentação.	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	Note Especifique a codificação da página de código-fonte como IBM1047 e a codificação da página de código de destino como UTF-8.	
Verifique a tarefa de transferência.	Para verificar se a transferência de dados foi bem-sucedida, siga as instruções na AWS Mainframe Modernization documentação. Confirme se o arquivo do mainframe está no bucket S3 de destino da transferência de arquivos.	Líder de migração
Verifique a função de cópia do Lambda.	Verifique se a função Lambda foi iniciada e se o arquivo foi copiado com uma extensão. csv para o bucket S3 do conjunto de dados de origem. O arquivo.csv criado pela função Lambda é o arquivo de dados de entrada para. QuickSight Por exemplo, dados, consulte o `Sample-data-member-healthcare-APG` arquivo na seção Anexos.	Líder de migração

Conecte-se QuickSight aos dados do mainframe

Tarefa	Descrição	Habilidades necessárias
Configurar QuickSight.	Para configurar QuickSight, siga as instruções na AWS documentação.	Líder de migração
Crie um conjunto de dados para QuickSight.	Para criar um conjunto de dados para QuickSight, siga as instruções na AWS documentação. O arquivo de dados de entrada é o arquivo de mainframe convertido que foi criado quando você definiu a tarefa de transferência de dados de mainframe.	Líder de migração

Obtenha insights de negócios a partir dos dados do mainframe usando o Amazon Q em QuickSight

Tarefa	Descrição	Habilidades necessárias
Configure o Amazon Q em QuickSight.	Esse recurso requer a Enterprise Edition. Para configurar o Amazon Q em QuickSight, faça o seguinte: 1. Para obter o complemento Amazon Q, siga as instruções Etapa 1: Obtenha o complemento Q na AWS documentação. 2. Para usar os recursos generativos de BI no Amazon Q, atualize as contas de seus usuários.	Líder de migração

Tarefa	Descrição	Habilidades necessárias
	Siga as instruções na AWS documentação. 3. Crie um tópico do Amazon Q usando o conjunto de dados que você criou anteriormente. Siga as instruções na AWS documentação. 4. Para configurar os metadados do tópico de forma que sejam compatíveis com a linguagem natural, siga as instruções na documentação.AWS	

Tarefa	Descrição	Habilidades necessárias
Analise os dados do mainframe e crie um painel visual.	Para analisar e visualizar seus dados em QuickSight, faça o seguinte: 1. Para criar a análise de dados do mainframe, siga as instruções na AWS documentação. Para o conjunto de dados, escolha o conjunto de dados criado na etapa anterior. 2. Na página de análise, escolha Criar visual. 3. Na janela Criar tópico para análise, escolha Atualizar tópico existente. 4. Na lista suspensa Selecionar um tópico, escolha o tópico que você criou anteriormente. 5. Escolha Vinculação de tópicos. 6. Depois de vincular o tópico, escolha Criar visual para abrir a janela Amazon Q Build a Visual. 7. Na barra de prompts, escreva suas perguntas de análise. Os exemplos de perguntas usadas para esse padrão são os seguintes:	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	• Mostrar distribuição de membros por região • Mostrar distribuição de membros por idade • Mostrar distribuição de membros por gênero • Mostrar distribuição de membros por tipo de plano • Mostrar imunização preventiva não concluída do membro Depois de inserir suas perguntas, escolha Criar. O Amazon Q in QuickSight cria os recursos visuais. 8. Para adicionar os elementos visuais ao seu painel visual, escolha ADICIONAR À ANÁLISE. Ao terminar, você poderá publicar seu painel para compartilhar com outras pessoas em sua organização. Para ver exemplos, consulte Painel visual do mainframe na seção Informações adicionais.	

Crie uma história de dados com o Amazon Q a QuickSight partir dos dados do mainframe

Tarefa	Descrição	Habilidades necessárias
Crie uma história de dados.	Crie uma história de dados para explicar os insights da análise anterior e gere uma recomendação para aumentar a imunização preventiva dos membros: 1. Para criar a história de dados, siga as instruções na AWS documentação. 2. Para o prompt da história de dados, use o seguinte: `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunizat ion. Include 4 points of supportin g data for this pattern.` Você também pode criar seu próprio prompt para gerar histórias de dados	Engenheiro de migração

Tarefa	Descrição	Habilidades necessárias
	para outros insights de negócios. 3. Escolha Adicionar elementos visuais e adicione os elementos visuais que são relevantes para a história dos dados. Para esse padrão, use as imagens que você criou anteriormente. 4. Escolha Criar. 5. Por exemplo, saída da história de dados, consulte Saída da história de dados na seção Informações adicionais.	
Veja a história de dados gerada.	Para ver a história de dados gerada, siga as instruções na AWS documentação.	Líder de migração
Edite uma história de dados gerada.	Para alterar a formatação, o layout ou os elementos visuais em uma história de dados, siga as instruções na AWS documentação.	Líder de migração
Compartilhe uma história de dados.	Para compartilhar uma história de dados, siga as instruções na AWS documentação.	Engenheiro de migração

Solução de problemas

Problema	Solução
Não foi possível descobrir os arquivos de mainframe ou os conjuntos de dados inseridos nos critérios de pesquisa de conjuntos de dados para Criar tarefa de transferência em Transferência de AWS Mainframe Moderniza tion arquivos com BMC.	1. Primeiro, verifique a conexão escolhend o Pontos finais de transferência de dados no console AWS Mainframe Moderniza tion Transferir com BMC. Se o tempo da última pulsação for maior que dois minutos, a conexão para transferência de arquivos não foi estabelecida. Se o tempo da última pulsação for inferior a 2 minutos para o agente em execução no mainframe, a conexão com o agente será bem-sucedida. Vá para a etapa 2. 2. Verifique a AWS Secrets Manager configura ção. Uma chave secreta deve ser configura da no Secrets Manager com uma chave de `userId` (I maiúsculo) com um valor de ID de usuário do mainframe e uma chave de `password` com o valor da senha do mainframe. As `userId` chaves `password` secretas fazem distinção entre maiúsculas e minúsculas e devem ser inseridas como estão.

Recursos relacionados

Para converter tipos de dados de mainframe, como PACKED-DECIMAL (COMP-3) ou BINARY (COMP ou COMP-4), em um tipo de dados compatível com, consulte os seguintes padrões: QuickSight

- Converta e descompacte dados EBCDIC em ASCII usando Python AWS
- Converta arquivos de mainframe do formato EBCDIC para o formato ASCII delimitado por caracteres no Amazon S3 usando AWS Lambda

Mais informações

S3 .py CopyLambda

O código Python a seguir foi gerado usando um prompt com o Amazon Q Developer em um IDE:

```
#Create a lambda function triggered by S3. display the S3 bucket name and key
import boto3
s3 = boto3.client('s3')
def lambda_handler(event, context):
print(event)
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
print(bucket, key)
#If key starts with object_created, skip copy, print "copy skipped". Return lambda with
 key value.
if key.startswith('object_created'):
print("copy skipped")
return {
'statusCode': 200,
'body': key
}
# Copy the file from the source bucket to the destination bucket.
 Destination_bucket_name = 'm2-filetransfer-final-opt-bkt'. Destination_file_key =
 'healthdata.csv'
copy_source = {'Bucket': bucket, 'Key': key}
s3.copy_object(Bucket='m2-filetransfer-final-opt-bkt', Key='healthdata.csv',
 CopySource=copy_source)
print("file copied")
#Delete the file from the source bucket.
s3.delete_object(Bucket=bucket, Key=key)
return {
'statusCode': 200,
'body': 'Copy Successful'
}
```

Painel visual do mainframe

O visual de dados a seguir foi criado pela Amazon Q QuickSight para a pergunta de análise `show member distribution by region`.

O visual de dados a seguir foi criado pela Amazon Q QuickSight para a pergunta`show member distribution by Region who have not completed preventive immunization, in pie chart`.

Saída da história de dados

As capturas de tela a seguir mostram seções da história de dados criada pela Amazon Q QuickSight para o prompt `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunization. Include 4 points of supporting data.`

Na introdução, a história dos dados recomenda escolher a região com mais membros para obter o maior impacto dos esforços de imunização.

A história dos dados fornece uma análise do número de membros das três principais regiões e nomeia o sudoeste como a principal região para se concentrar nos esforços de imunização.

> **Note**
>
> Cada uma das regiões Sudoeste e Nordeste tem oito membros. No entanto, o sudoeste tem mais membros que não estão totalmente vacinados, por isso tem mais potencial para se beneficiar de iniciativas para aumentar as taxas de imunização.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Integre o controlador universal Stonebranch com o AWS Mainframe Modernization

Criado por Vaidy Sankaran (AWS), Robert Lemieux (Stonebranch), Huseyin Gomleksizoglu (Stonebranch) e Pablo Alonso Prieto (AWS)

Resumo

Esse padrão explica como integrar a orquestração da workload Centro de Automação Universal do Stonebranch (UAC) com o serviço do Amazon Web Services (AWS) Mainframe Modernization. O serviço do AWS Mainframe Modernization migra e moderniza aplicações de mainframe para a Nuvem AWS. Ele oferece dois padrões: AWS Mainframe Modernization Replatform com tecnologia Micro Focus Enterprise e AWS Mainframe Modernization Automated Refactor com AWS Blu Age.

O Stonebranch UAC é uma plataforma de automação e orquestração de TI em tempo real. O UAC foi projetado para automatizar e orquestrar trabalhos, atividades e fluxos de trabalho em sistemas de TI híbridos, de on-premises até a AWS. Clientes corporativos que usam sistemas de mainframe estão migrando para infraestruturas e aplicações modernizadas centradas na nuvem. As ferramentas e os serviços profissionais da Stonebranch facilitam a migração dos agendadores e recursos de automação existentes para a Nuvem AWS.

Ao migrar ou modernizar seus programas de mainframe para a Nuvem AWS usando o Serviço do AWS Mainframe Modernization, você pode usar essa integração para automatizar o agendamento em lotes, aumentar a agilidade, melhorar a manutenção e diminuir os custos.

Esse padrão fornece instruções para integrar o agendador Stonebranch com aplicativos de mainframe migrados para o tempo de execução do serviço de modernização de mainframe da AWS Micro Focus Enterprise. Esse padrão é para arquitetos de soluções, desenvolvedores, consultores, especialistas em migração e outros que trabalham em migrações, modernizações, operações ou. DevOps

Resultados direcionados

Esse padrão se concentra em fornecer os seguintes resultados desejados:

- A capacidade de programar, automatizar e executar trabalhos em lote de mainframe executados no Serviço do AWS Mainframe Modernization (runtime do Microfocus) do Controlador Universal Stonebranch.
- Monitore os processos em lote aplicativo a partir do controlador universal Stonebranch.

- Start/Restart/Rerun/Stopprocessos em lote automática ou manualmente a partir do controlador universal Stonebranch.
- Recupere os resultados dos processos em lote do AWS Mainframe Modernization.
- Capture os CloudWatch registros da AWS dos trabalhos em lote no Stonebranch Universal Controller.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo Micro Focus Bankdemo com arquivos de linguagem de controle de tarefas (JCL) e um processo em lote implantado em um ambiente de serviço de modernização de mainframe da AWS (tempo de execução da Micro Focus)
- Conhecimento básico de como compilar e implantar um aplicativo de mainframe executado no Micro Focus Enterprise Server
- Conhecimento básico do Controlador universal Stonebranch
- Licença experimental do Stonebranch (entre em contato com a Stonebranch)
- Instâncias Windows ou Linux Amazon Elastic Compute Cloud (Amazon EC2) (por exemplo, xlarge) com um mínimo de quatro núcleos, 8 GB de memória e 2 GB de espaço em disco
- Apache Tomcat versão 8.5.x ou 9.0.x
- Ambiente de Execução Java (JRE) Oracle ou OpenJDK versão 8 ou 11
- Amazon Aurora Edição Compatível com MySQL
- Bucket do Amazon Simple Storage Service (Amazon S3) para repositório de exportação
- Amazon Elastic File System (Amazon EFS) para conexões do agente Stonebranch Universal Message Service (OMS) para alta disponibilidade (HA)
- Arquivos de instalação do controlador universal Stonebranch 7.2 Agente universal 7.2
- Modelo de agendamento de tarefas do AWS Mainframe Modernization (última versão lançado do arquivo .zip)

Limitações

- O produto e a solução foram testados e a compatibilidade foi validada somente com o OpenJDK 8 e 11.

- O modelo aws-mainframe-modernization-stonebranchde agendamento de tarefas de integração funcionará somente com o serviço AWS Mainframe Modernization.
- Esse modelo de agendamento de tarefas funcionará somente em uma edição Unix, Linux ou Windows dos agentes Stonebranch.
- Alguns serviços da AWS não estão disponíveis em todas as regiões da AWS. Para ver a disponibilidade da região, consulte os serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Arquitetura de estado final

O diagrama a seguir mostra um exemplo de ambiente AWS necessário para esse piloto.

1. O Centro de Automação Universal (UAC) do Stonebranch inclui dois componentes principais: controlador universal e agentes universais. O Stonebranch OMS é usado como um barramento de mensagens entre o controlador e os agentes individuais.
2. O banco de dados do Stonebranch UAC é usado pelo controlador universal. O banco de dados pode ser compatível com MySQL, Microsoft SQL Server, Oracle ou Aurora MySQL.
3. Serviço de modernização de mainframe da AWS — ambiente de execução da Micro Focus com o BankDemo aplicativo implantado. Os arquivos do BankDemo aplicativo serão armazenados em um bucket do S3. Este bucket também contém os arquivos JCL do mainframe.
4. O Stonebranch UAC pode executar as seguintes funções para a execução em lote:
    a. Inicie um trabalho em lotes usando o nome do arquivo JCL que existe no bucket do S3 vinculado ao Serviço do AWS Mainframe Modernization.
    b. Obtenha o status da execução do trabalho em lotes.
    c. Aguarde até que a execução do trabalho em lotes seja concluída.
    d. Busque os logs da execução do trabalho em lotes.
    e. Execute novamente os trabalhos em lotes com falha.
    f. Cancele o trabalho em lote enquanto o trabalho está em execução.
5. O Stonebranch UAC pode executar as seguintes funções para o aplicativo:
    a. Iniciar a replicação
    b. Obter status da aplicação

c. Aguarde até que o aplicativo seja iniciado ou interrompido

d. Interromper a aplicação

e. Obter logs de operação do aplicativo

Conversão de trabalhos do Stonebranch

O diagrama a seguir representa o processo de conversão de trabalhos do Stonebranch durante a jornada de modernização. Ele descreve como as programações de trabalho e as definições de tarefas são convertidas em um formato compatível que pode executar tarefas em lote do AWS Mainframe Modernization.

1. Para o processo de conversão, as definições de trabalho são exportadas do sistema de mainframe existente.
2. Os arquivos JCL podem ser carregados no bucket do S3 para o aplicativo de modernização de mainframe para que esses arquivos JCL possam ser implantados pelo serviço do AWS Mainframe Modernization.
3. A ferramenta de conversão converte as definições de trabalho exportadas em tarefas do UAC.
4. Depois que todas as definições de tarefas e programações de trabalho forem criadas, esses objetos serão importados para o Controlador Universal. As tarefas convertidas então executam os processos no Serviço do AWS Mainframe Modernization em vez de executá-los no mainframe.

Arquitetura Stonebranch UAC

O diagrama de arquitetura a seguir representa um active-active-passive modelo de controlador universal de alta disponibilidade (HA). O Stonebranch UAC é implantado em várias zonas de disponibilidade para fornecer alta disponibilidade e apoiar a recuperação de desastres (DR).

Controlador universal

Dois servidores Linux são provisionados como controladores universais. Ambos se conectam ao mesmo endpoint do banco de dados. Cada servidor abriga um aplicativo Universal Controller e o OMS. A versão mais recente do Controlador Universal é usada no momento em que é provisionada.

Os Controladores Universais são implantados no aplicativo web Tomcat como o documento ROOT e são servidos na porta 80. Essa implantação facilita a configuração do balanceador de carga de frontend.

O HTTP sobre TLS ou HTTPS está habilitado usando o certificado curinga Stonebranch (por exemplo, `https://customer.stonebranch.cloud`). Isso protege a comunicação entre o navegador e o aplicativo.

OMS

Um agente universal e o OMS (Opswise Message Service) residem em cada servidor do controlador universal. Todos os agentes universais implantados do lado do cliente são configurados para se conectarem a ambos os serviços OMS. O OMS atua como um serviço de mensagens comum entre os agentes universais e o controlador universal.

O Amazon EFS monta um diretório de spool em cada servidor. O OMS usa esse diretório de spool compartilhado para manter as informações de conexão e tarefas dos controladores e agentes. O OMS funciona em um modo de alta disponibilidade. Se o OMS ativo cair, o OMS passivo terá acesso a todos os dados e retomará as operações ativas automaticamente. Os agentes universais detectam essa alteração e se conectam automaticamente ao novo OMS ativo.

Banco de dados

O Amazon Relational Database Service (Amazon RDS) hospeda o banco de dados UAC, com o Amazon Aurora MySQL, compatível com Amazon Aurora MySQL como seu mecanismo. O Amazon RDS ajuda a gerenciar e oferecer backups programados em intervalos regulares. As duas instâncias do controlador universal se conectam ao mesmo endpoint do banco de dados.

Load balancer

Um Application Load Balancer é configurado para cada instância. O balanceador de carga direciona o tráfego para o controlador ativo a qualquer momento. Os nomes de domínio da sua instância apontam para os respectivos endpoints do balanceador de carga.

URLs

Cada uma de suas instâncias tem um URL, conforme mostrado no exemplo a seguir.

Ambiente	Instância

Produção	`customer.stonebranch.cloud`
Desenvolvimento (não produção)	`customerdev.stonebranch.cloud`
Teste (não produção)	`customertest.stonebranch.cloud`

> **Note**
>
> Os nomes das instâncias que não são de produção podem ser definidos com base nas suas necessidades.

Alta disponibilidade

Alta disponibilidade (HA) é a capacidade de um sistema operar continuamente sem falhas por um determinado período de tempo. Essas falhas incluem, mas não estão limitadas a, armazenamento, atrasos na resposta de comunicação do servidor causados por problemas de CPU ou memória e conectividade da rede.

Para atender aos requisitos de HA:

- Todas as EC2 instâncias, bancos de dados e outras configurações são espelhadas em duas zonas de disponibilidade separadas na mesma região da AWS.
- O controlador é provisionado por meio de uma Imagem de máquina da Amazon (AMI) em dois servidores Linux nas duas zonas de disponibilidade. Por exemplo, se você estiver provisionado na região europeia eu-west-1, você tem um controlador universal na zona de disponibilidade eu-west-1a e na zona de disponibilidade eu-west-1c.
- Nenhum trabalho pode ser executado diretamente nos servidores de aplicativos e nenhum dado pode ser armazenado nesses servidores.
- O Application Load Balancer executa verificações de integridade em cada controlador universal para identificar o ativo e direcionar o tráfego para ele. Caso um servidor tenha problemas, o balanceador de carga automaticamente promove o controlador universal passivo para um estado ativo. O balanceador de carga então identifica a nova instância ativa do controlador universal a partir das verificações de integridade e começa a direcionar o tráfego. O failover ocorre em quatro minutos sem perda de trabalhos, e o URL do frontend permanece o mesmo.
- O serviço de banco de dados do Aurora compatível com MySQL armazena dados do controlador universal. Para ambientes de produção, um cluster de banco de dados é criado com duas

instâncias de banco de dados em duas zonas de disponibilidade diferentes em uma única região da AWS. Ambos os controladores universais usam uma interface de Conectividade do banco de dados Java (JDBC) que aponta para um único endpoint do cluster do banco de dados. Caso uma instância de banco de dados tenha problemas, o endpoint do cluster do banco de dados aponta dinamicamente para a instância íntegra. Nenhuma intervenção manual é necessária.

Backup e limpeza

O controlador universal Stonebranch está configurado para fazer backup e limpar dados antigos seguindo a programação mostrada na tabela.

Tipo	Programação
Atividades	7 dias
Auditoria	90 dias
Histórico	60 dias

Os dados de backup anteriores às datas mostradas são exportados para o formato.xml e armazenados no sistema de arquivos. Após a conclusão do processo de backup, os dados mais antigos são removidos do banco de dados e arquivados em um bucket S3 por até um ano para instâncias de produção.

Você pode ajustar essa programação na interface do seu controlador universal. No entanto, aumentar esses prazos pode causar maior tempo de inatividade durante a manutenção.

Ferramentas

Serviços da AWS

- O AWS Mainframe Modernization é um serviço nativo de nuvem da plataforma AWS que ajuda a modernizar aplicações de mainframe para ambientes de runtime gerenciados da AWS. Ele fornece ferramentas e recursos para ajudar você a planejar e implementar a migração e a modernização.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias da Amazon. EC2
- O Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS.

- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS. Esse padrão usa Amazon Aurora Edição compatível com MySQL.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre EC2 instâncias, contêineres e endereços IP da Amazon em uma ou mais zonas de disponibilidade. Este padrão usa um Application Load Balancer.

Stonebranch

- O Universal Automation Center (UAC) é um sistema de produtos de automação de workload empresarial. Esse padrão usa os seguintes componentes do UAC:
  - O Universal Controller, um aplicativo web Java executado em um contêiner web Tomcat, é a solução corporativa de agendamento de tarefas e corretora de automação de carga de trabalho do Universal Automation Center. O Controller apresenta uma interface de usuário para criar, monitorar e configurar as informações do Controller; manipula a lógica de agendamento; processa todas as mensagens de e para os Universal Agents; e sincroniza grande parte da operação de alta disponibilidade do Universal Automation Center.
  - O Universal Agent é um agente de agendamento independente do fornecedor que colabora com o agendador de trabalhos existente em todas as principais plataformas de computação, tanto legadas quanto distribuídas. Todos os agendadores executados em z/Series, i/Series, Unix, Linux ou Windows são compatíveis.
- O Universal Agent é um agente de agendamento independente do fornecedor que colabora com o agendador de trabalhos existente em todas as principais plataformas de computação, tanto legadas quanto distribuídas. Todos os agendadores executados em z/Series, i/Series, Unix, Linux ou Windows são compatíveis.
- aws-mainframe-modernization-stonebranchIntegração com o Stonebranch O AWS Mainframe Modernization Universal Extension é o modelo de integração para executar, monitorar e executar novamente trabalhos em lote na plataforma AWS Mainframe Modernization.

Código

O código desse padrão está disponível no GitHub repositório aws-mainframe-modernization-stonebranch-integration.

Épicos

Instale o Universal Controller e o Universal Agent na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Baixe os arquivos de instalação.	Baixe a instalação dos servidores Stonebranch. Para obter os arquivos de instalação, entre em contato com a Stonebranch.	Arquiteto de nuvem
Inicie a EC2 instância.	Você precisará de cerca de 3 GB de espaço extra para as instalações do Universal Controller e do Universal Agent. Portanto, forneça pelo menos 30 GB de espaço em disco para a instância. Adicione a porta 8080 ao grupo de segurança para que ela fique acessível.	Arquiteto de nuvem

Verifique os pré-requisitos.	Antes da instalação, faça o seguinte:
	
	1. Instale o Java conforme descrito em Baixando o Java Runtime Environment.
	
	``
	$ sudo yum -y update
	$ sudo yum install
	 java-11-amazon-cor
	retto
	``
		Administrador de nuvem, administrador Linux

Tarefa	Descrição	Habilidades necessárias

	Certifique-se de usar uma das versões compatíveis do JAVA. O comando anterior deve instalar o java-11. Verifique a versão do Java e certifique-se de estar usando a versão 11 antes de continuar.
	2. Conforme descrito em Instalando o Apache Tomcat, execute os comandos a seguir.
	`$ sudo yum install tomcat tomcat-admin-webapps`
	`$ sudo systemctl enable tomcat`
	`$ sudo systemctl start tomcat`
	3. Crie um banco de dados Amazon Aurora conforme descrito em Criação e conexão com um cluster de banco de dados Aurora MySQL. Use Amazon Aurora Edição compatível com MySQL
	Escolha um nome de usuário principal e uma senha mestre. Deixe as demais configurações com os valores padrão.	

Tarefa	Descrição	Habilidades necessárias

Instale o Universal Controller.	1. Faça upload do arquivo de `universal-controller-7.2.0.0.tar` instalação na EC2 instância.
	2. Desarquive os arquivos de instalação em uma pasta `temp`.
	`$ tar -xvf universal-controller-7.2.0.0.tar`
	3. Conceda permissão de execução ao script de instalação.
	`$ chmod a+x install-controller.sh`
	4. Instale o controlador. Este exemplo usa o comando a seguir para instalar o Universal Controller em `/usr/share/tomcat`. Use o banco de dados Amazon Aurora que você criou nas etapas anteriores.
	`$ sudo ./install-controller.sh --tomcat-dir /usr/share/tomcat/ --controller-file universal-controller-7.2.0.0-build.145.war --dbuser admin --dbpass`
		Arquiteto de nuvem, administrador Linux

Tarefa	Descrição	Habilidades necessárias
	“****” --dbname uc --rdbms mysql --dburl jdbc:mysql://database-2-instance-1.cih63miincgy.us-east-1.rds.amazonaws.com:3306/ A última linha da saída do script deve ser “Instalação concluída”. 5. Navegue até o seguinte URL na EC2 instância. `http://<public_ip>:8080/uc` 6. Na tela de login, digite ops.admin na seção Nome de usuário, e mantenha o campo Senha vazio. 7. Defina uma nova senha para o usuário `ops.admin`.	

Tarefa	Descrição	Habilidades necessárias

Instale o Universal Agent.	1. Faça upload do arquivo de `sb-7.2.0.1-linux-3.10-x86_64.tar.Z` instalação na EC2 instância.
	2. Faça login na EC2 instância.
	3. Desarquive o pacote de instalação do Universal Agent.
	`$ zcat sb-7.2.0.1-linux-3.10-x86_64.tar.Z | tar xvf -`
	4. Execute o seguinte comando:
	`$ sudo ./unvinst --oms_servers 7878@localhost --oms_autostart yes --python yes`
	5. Crie um arquivo PAM.
	`$ cp /etc/pam.d/login /etc/pam.d/ucmd`
	6. Ative o início automático para o Universal Agent.
	`$ /sbin/restorecon -v /etc/rc.d/init.d/ubrokerd`
		Administrador de nuvem, administrador Linux

Tarefa	Descrição	Habilidades necessárias
Adicione o OMS ao Universal Controller.	1. Faça login no Universal Controller com o usuário `ops.admin` . 2. Escolha o menu Serviços no canto superior esquerdo da tela e, em seguida, escolha o menu Servidores OMS no Sistema 3. No campo Endereço do servidor OMS`localhost` , digite e salve. 4. Você verá o status do servidor OMS como Conectado e o Status da Sessão como Operacional.	Administrador do Universal Controller

Importe o AWS Mainframe Modernization Universal Extension e crie uma tarefa

Tarefa	Descrição	Habilidades necessárias
Importar modelo de integração.	Para essa etapa, você precisa do AWS Mainframe Modernization Universal Extension. Verifique se a versão mais recente do arquivo .zip foi baixada. 1. Faça login no Controlador Universal com o usuário `ops.admin` . 2. Navegue até Serviços, Importar modelo de integração.	Administrador do Universal Controller

Tarefa	Descrição	Habilidades necessárias
	3. Selecione o arquivo .zip do modelo de integração (`aws_mainframe_modernization_stonebranch_extension.zip`) e escolha Importar. Depois que o modelo de integração for importado, você verá as Tarefas do AWS Mainframe Modernization em Serviços disponíveis.	

Tarefa	Descrição	Habilidades necessárias
Ative credenciais resolvíveis.	1. Navegue até Serviços, Tarefas do AWS Mainframe Modernization. 2. No painel direito, preencha os campos obrigatórios: • Nome: Nova tarefa de modernização do mainframe • Agente: selecione o único agente (AGNT0001). Em Detalhes do AWS Mainframe Modernization: • Ação: Listar ambientes • Credenciais da AWS: se você tiver uma função do AWS Identity and Access Management (IAM) adicionada à EC2 instância, você pode manter esse campo vazio. Se você for usar `AWSAccessKeyID` e `AWSSecretKey` , escolha o ícone () ao lado do campo. Na janela Detalhes da credencial que se abre, insira as seguintes informações e salve. • Nome: Credenciais do AWS Mainframe Modernization	Administrador do Universal Controller

Tarefa	Descrição	Habilidades necessárias
	• Usuário de runtime: escreva a ID da chave de acesso da AWS neste campo. • Senha de runtime: escreva a chave secreta da AWS neste campo. • Endpoint: certifique-se de que o endpoint tenha a região da AWS correta. O padrão é `https://m2.us-east-1.amazonaws.com` . • Região: insira a região do serviço do AWS Mainframe Modernization. O padrão é `us-east-1` . 3. Mantenha os valores padrão nos demais campos e salve a tarefa.	

Tarefa	Descrição	Habilidades necessárias
Inicie a tarefa.	1. Na parte superior do painel direito, escolha Iniciar tarefa. 2. Na janela Confirmação, escolha Iniciar. Depois disso, o console do Universal Controller exibirá uma mensagem semelhante à seguinte mensagem. 2022-08-24 10:11:49 AM Iniciou com sucesso a tarefa universal “Nova tarefa de modernização de mainframe” com a instância de tarefa sys_id 166129149 3634146313 E38 OZJY. NC8 DB8 3. Navegue até Instância s Caso não veja a guia Instâncias, escolha a seta para a direita para rolar para a direita. 4. Abra o menu de contexto (clique com o botão direito do mouse) da instância da tarefa na lista e escolha Recuperar saída e, em seguida, Enviar em Recuperar saída 5. Na janela Recuperar saída, você verá a lista de ambientes no STDOUT.	Administrador do Universal Controller

Teste ao iniciar um trabalho em lote

Tarefa	Descrição	Habilidades necessárias
Crie uma tarefa para o trabalho em lotes.	1. Navegue até Serviços, Tarefas do AWS Mainframe Modernization. 2. No painel direito, preencha os campos obrigatórios: • Nome: Nova tarefa de modernização do mainframe • Agente: selecione o único agente (AGNT0001). Em Detalhes do AWS Mainframe Modernization: • Ação: Start Batch (ou Start Batch and Wait para executar o trabalho em lotes e aguardar até que a tarefa seja concluída na AWS) • Credenciais da AWS: se você tiver uma função do IAM adicionada à EC2 instância, você pode manter esse campo vazio. Se você for usar `AWSAccessKeyID` e `AWSSecretKey` , escolha o ícone () ao lado do campo. • Endpoint: certifique-se de que o endpoint tenha a região da AWS correta.	Administrador do Universal Controller

Tarefa	Descrição	Habilidades necessárias
	O padrão é https://m2.us-east-1.amazonaws.com. • Região: insira a região do serviço do AWS Mainframe Moderniza tion. O padrão é `us-east-1` . • Aplicativo: escolha o ícone ao lado do campo () e escolha Enviar nas Opções de Atualização do Aplicativo. Isso se conectará ao Serviço do AWS Mainframe Modernization e retornará a lista de aplicativ os. Agora é possível selecionar o aplicativo na lista suspensa. Selecione o aplicativo para o qual você deseja executar o trabalho em lote. • Nome do arquivo JCL: `RUNHELLO.jcl` • Aguardar por sucesso ou falha:se essa opção estiver selecionada, a tarefa aguardará até que o status do trabalho em lotes seja bem-sucedido ou malsucedido. • Intervalo de sondagem: essa é a quantidade	

Tarefa	Descrição	Habilidades necessárias
	de tempo entre cada sondagem. • Buscar logs de execução: se selecionada, os registros serão buscados automaticamente quando o trabalho em lotes for concluído. • Formato do log: esse é o formato dos logs a serem impressos. Pode ser em texto ou Formato JSON. 3. Mantenha os valores padrão nos demais campos e salve a tarefa.	

Tarefa	Descrição	Habilidades necessárias
Inicie a tarefa.	1. Na parte superior do painel direito, escolha Iniciar tarefa. 2. Na janela Confirmação, escolha Iniciar. Depois disso, o console do Universal Controller exibirá uma mensagem semelhante à seguinte mensagem. 2022-08-24 11:11:59 AM Iniciou com sucesso a tarefa universal “Mainframe Modernization Start Batch” com a instância de tarefa sys_id <sys id>. 3. Navegue até Instâncias Caso não veja a guia Instâncias, escolha a seta para a direita para rolar para a direita. 4. Abra o menu de contexto (clique com o botão direito do mouse) da instância da tarefa na lista e escolha Recuperar saída e, em seguida, Enviar em Recuperar saída 5. Na janela Recuperar saída, você verá a lista de ambientes no STDOUT.	Administrador do Universal Controller

Crie um fluxo de trabalho para várias tarefas

Tarefa	Descrição	Habilidades necessárias
Copie as tarefas.	1. Abra o menu de contexto (clique com o botão direito do mouse) da tarefa da qual você deseja criar cópias e escolha Copiar. 2. Na janela Copiar tarefa de modernização de mainframe da AWS, insira o seguinte novo nome para a nova tarefa: Mainframe Modernization Start Batch -. RUNAWS2 3. Copie a tarefa novamente , usando o seguinte nome: Mainframe Modernization Start Batch -. RUNAWS3 4. Copie com a tarefa novamente, usando o seguinte nome: Mainframe Modernization Start Batch -. RUNAWS4 5. Copie a tarefa pela última vez, usando o seguinte nome: Mainframe Modernization Start Batch - FOOBAR.	Administrador do Universal Controller
Tarefas de atualização.	1. Abra (clique duas vezes) a RUNAWS2 tarefa Mainframe Moderniza tion Start Batch -, altere o campo Nome do arquivo	Administrador do Universal Controller

Tarefa	Descrição	Habilidades necessárias
	JCL para `RUNAWS2.jcl` e salve. 2. Abra (clique duas vezes) a RUNAWS3 tarefa Mainframe Moderniza tion Start Batch -, altere o campo Nome do arquivo JCL para *`RUNAWS3.jcl`* e salve. 3. Abra (clique duas vezes) a RUNAWS4 tarefa Mainframe Moderniza tion Start Batch -, altere o campo Nome do arquivo JCL para *`RUNAWS4.jcl`* e salve. 4. Abra (clique duas vezes) na tarefa Mainframe Moderniza tion Start Batch - FOOBAR task, altere o campo Nome do arquivo JCL para `MISSING.jcl` e salve. Essa tarefa falhará porque o valor do nome do arquivo JCL está incorreto.	

Tarefa	Descrição	Habilidades necessárias
Crie um fluxo de trabalho.	1. Navegue até Serviços, Fluxos de trabalho. 2. No painel direito, insira o Fluxo de trabalho de modernização do mainframe no campo Nome e salve. 3. No painel à direita, escolha Editar fluxo de trabalho. 4. Na guia Editor de fluxo de trabalho, o botão Adicionar tarefa (+). 5. Na janela Localização de tarefas, escolha Pesquisar para ver todas as tarefas no Universal Controller. 6. Clique no ícone ao lado de Mainframe Moderniza tion Start Batch Task e arraste o ícone para um local vazio no Editor de fluxo de trabalho. 7. Repita a mesma ação para as outras tarefas de modernização do mainframe e posicione -as conforme mostrado na seção Informações adicionais. 8. Escolha o botão Conectar (), e conecte as tarefas Para conectar uma tarefa a outra, clique no meio de	Administrador do Universal Controller

Tarefa	Descrição	Habilidades necessárias
	uma tarefa e arraste-a até a tarefa de destino. 9. Conecte as tarefas conforme mostrado na seção Informações adicionais e salve o fluxo de trabalho. 10. Clique com o botão direito do mouse em um local vazio no Editor de fluxo de trabalho, escolha Iniciar fluxo de trabalho e escolha OK.	

Tarefa	Descrição	Habilidades necessárias
Confira o status do fluxo de trabalho.	1. No menu à esquerda, escolha a Atividade 2. No meio da janela, escolha Iniciar. Você verá a lista de instâncias de tarefas na lista. 3. Abra (clique duas vezes) Fluxo de trabalho de modernização de mainframe na lista ou abra o menu de contexto (clique com o botão direito do mouse) e escolha Comandos de tarefas do fluxo de trabalho, Exibir fluxo de trabalho. Você verá as tarefas conforme mostrado na seção Informações adicionais. Esperava-se que a segunda tarefa falhasse porque você usou um arquivo JCL ausente.	Administrador do Universal Controller

Solucione problemas de trabalhos em lotes com falha e execute novamente

Tarefa	Descrição	Habilidades necessárias
Corrija a tarefa com falha e execute novamente.	1. Abra a tarefa com falha (clique duas vezes) para ver o erro da tarefa.	Administrador do Universal Controller

Tarefa	Descrição	Habilidades necessárias
	2. Você tem duas opções para corrigir a tarefa com falha. • Corrija o nome do arquivo JCL e defina-o como `FOOBAR.jcl` . • Adicione o nome correto do arquivo JCL ao Nome do arquivo JCL (Temp). Esse campo substituirá o campo Nome do arquivo JCL. Para esse piloto, escolha a segunda opção e salve a instância da tarefa. 3. No Monitor de fluxo de trabalho, abra o menu de contexto (clique com o botão direito do mouse) da tarefa com falha e escolha Comandos, Executar novamente. 4. Depois disso, todas as tarefas serão concluídas com sucesso.	

Crie tarefas para iniciar o aplicativo e interromper o aplicativo

Tarefa	Descrição	Habilidades necessárias
Crie a ação Iniciar aplicativo.	1. Navegue até Serviços, Tarefas do AWS Mainframe Modernization.	Administrador do Universal Controller

Tarefa	Descrição	Habilidades necessárias
	2. No painel direito, preencha os campos obrigatórios: • Nome: aplicativo de início de modernização do mainframe • Agente: selecione o único agente (AGNT0001). Em Detalhes do AWS Mainframe Modernization: • Ação: Iniciar aplicativo • Credenciais da AWS: se você tiver uma função do IAM adicionada à EC2 instância, você pode manter esse campo vazio. Se você usar `AWSAccessKeyID` e `AWSSecretKey` , selecione a credencial que você criou antes. • Endpoint: certifique-se de que o endpoint tenha a região correta. O padrão é `https://m2.us-east-1.amazonaws.com` . • Região: insira a região do serviço do AWS Mainframe Moderniza tion. O padrão é `us-east-1` . • Aplicativo: escolha o ícone ao lado do campo	

Tarefa	Descrição	Habilidades necessárias
	() e escolha Enviar nas Opções de Atualização do Aplicativo. Isso se conectará ao Serviço do AWS Mainframe Modernization e retornará a lista de aplicativ os. Agora é possível selecionar o aplicativo na lista suspensa. Selecione o aplicativo para o qual você deseja executar o trabalho em lote. • Aguardar por sucesso ou falha:se essa opção estiver selecionada, a tarefa aguardará até que o status do trabalho em lotes seja bem-sucedido ou malsucedido. • Intervalo de sondagem: essa é a quantidade de tempo entre cada sondagem. • Buscar logs de execução: se selecionada, os registros serão buscados automaticamente quando o trabalho em lotes for concluído. • Formato do log: esse é o formato dos logs a serem impressos. Pode ser em texto ou Formato JSON.	

Tarefa	Descrição	Habilidades necessárias
	3. Mantenha os valores padrão nos demais campos e salve a tarefa. 4. Agora copie essa tarefa e crie uma tarefa para Interromper aplicação . Altere o nome para Mainframe Moderinization Stop Application e altere a ação para Interromper aplicação.	

Crie uma tarefa de execução de Cancelar lote

Tarefa	Descrição	Habilidades necessárias
Crie a ação Cancelar lote.	1. Navegue até Serviços, Tarefas do AWS Mainframe Modernization. 2. No painel direito, preencha os campos obrigatórios: • Nome: Mainframe Modernization Cancel Batch Execution • Agente: selecione o único agente (AGNT0001). Em Detalhes do AWS Mainframe Modernization: • Ação: Execução de cancelar lote • Credenciais da AWS: se você tiver uma função	

Tarefa	Descrição	Habilidades necessárias
	do IAM adicionada à EC2 instância, você pode manter esse campo vazio. Se você usar `AWSAccessKeyID` e `AWSSecretKey`, selecione a credencial que você criou antes. • Endpoint: certifique-se de que o endpoint tenha a região correta. O padrão é `https://m2.us-east-1.amazonaws.com`. • Região: insira a região do serviço do AWS Mainframe Modernization. O padrão é `us-east-1`. • Aplicativo: escolha o ícone ao lado do campo () e escolha Enviar nas Opções de Atualização do Aplicativo. Isso se conectará ao Serviço do AWS Mainframe Modernization e retornará a lista de aplicativos. Agora é possível selecionar o aplicativo na lista suspensa. Selecione o aplicativo para o qual você deseja executar o trabalho em lote.	

Tarefa	Descrição	Habilidades necessárias
	• Aguardar por sucesso ou falha:se essa opção estiver selecionada, a tarefa aguardará até que o status do trabalho em lotes seja bem-sucedido ou malsucedido. • Intervalo de sondagem: essa é a quantidade de tempo entre cada sondagem. • Buscar logs de execução: se selecionada, os registros serão buscados automaticamente quando o trabalho em lotes for concluído. • Formato do log: esse é o formato dos logs a serem impressos. Pode ser em texto ou Formato JSON. 3. Mantenha os valores padrão nos demais campos e salve a tarefa.	

Recursos relacionados

- Controlador universal
- Universal Agent
- Configurações do LDAP
- Login único SAML
- Ferramenta de conversão Xpress

Mais informações

Ícones no editor de fluxo de trabalho

Todas as tarefas conectadas

Status do fluxo de trabalho

Migre e replique arquivos VSAM para o Amazon RDS ou o Amazon MSK usando o Connect da Precisely

Criado por Prachi Khanna (AWS) e Boopatia GOPALSAMY (AWS)

Resumo

Esse padrão mostra como migrar e replicar arquivos do Método de acesso ao armazenamento virtual (VSAM - Virtual Storage Access Method) de um mainframe para um ambiente de destino na Nuvem AWS usando o Connect da Precisely. Os ambientes de destino abrangidos por este padrão incluem o Amazon Relational Database Service (Amazon RDS) e o Amazon Managed Streaming for Apache Kafka (Amazon MSK). O Connect usa a captura de dados de alteração (CDC - change data capture) para monitorar continuamente as atualizações dos seus arquivos VSAM de origem e, em seguida, transferir essas atualizações para um ou mais dos seus ambientes de destino da AWS. Você pode usar esse padrão para atender às suas metas de modernização de aplicativos ou análise de dados. Por exemplo, você pode usar o Connect para migrar seus arquivos do aplicativo VSAM para a Nuvem AWS com baixa latência ou migrar seus dados do VSAM para um data warehouse ou data lake da AWS para análises que possam tolerar latências de sincronização maiores do que as necessárias para a modernização do aplicativo.

Pré-requisitos e limitações

Pré-requisitos

- IBM z/OS V2R1 ou superior
- CICS Transaction Server para z/OS (CICS TS) V5.1 ou superior (captura de dados CICS/VSAM)
- IBM MQ 8.0 ou superior
- Conformidade com os requisitos de segurança do z/OS (por exemplo, autorização do APF para SQData carregar bibliotecas)
- Logs de recuperação do VSAM ativados
- (Opcional) Versão de recuperação do CICS VSAM (CICS VR - CICS VSAM Recovery Version) para capturar automaticamente os registros do CDC
- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) com uma sub-rede acessível por sua plataforma legada
- Uma licença VSAM Connect da Precisely

Limitações

- O Connect não oferece suporte à criação automática de tabelas de destino com base nos esquemas ou copybooks do VSAM de origem. Você deve definir a estrutura da tabela de destino pela primeira vez.
- Para destinos sem streaming, como o Amazon RDS, você deve especificar a fonte de conversão para o mapeamento de destino no script de configuração do Apply Engine.
- As funções de registro, monitoramento e alerta são implementadas APIs e exigem que componentes externos (como a Amazon CloudWatch) estejam totalmente operacionais.

Versões do produto

- SQData 40134 para z/OS
- SQData 4.0.43 para o Amazon Linux Amazon Machine Image (AMI) na Amazon Elastic Compute Cloud (Amazon) EC2

Arquitetura

Pilha de tecnologia de origem

- Job Control Language (JCL - Linguagem de controle de trabalho)
- Shell z/OS Unix e Interactive System Productivity Facility (ISPF - Facilidade de produtividade do sistema interativo)
- Utilitários VSAM (IDCAMS)

Pilha de tecnologias de destino

- Amazon EC2
- Amazon MSK
- Amazon RDS
- Amazon VPC

Arquitetura de destino

Migração de arquivos VSAM para o Amazon RDS

O diagrama a seguir mostra como migrar arquivos VSAM para um banco de dados relacional, como o Amazon RDS, em tempo real ou quase em tempo real usando o agente/publicador do CDC no ambiente de origem (mainframe on-premises) e o Apply Engine no ambiente de destino (Nuvem AWS).

O diagrama mostra o seguinte fluxo de trabalho em lote:

1. O Connect captura as alterações em um arquivo comparando os arquivos VSAM dos arquivos de backup para identificar as alterações e, em seguida, envia as alterações para o fluxo de registros.
2. O publicador consome dados do fluxo de log do sistema.
3. O publicador comunica as alterações de dados capturadas a um mecanismo de destino por meio de TCP/IP. O Controller Daemon autentica a comunicação entre os ambientes de origem e de destino.
4. O mecanismo de aplicação no ambiente de destino recebe as alterações do agente do Publisher e as aplica a um banco de dados relacional ou não relacional.

O diagrama mostra o seguinte fluxo de trabalho on-line:

1. O Connect captura as alterações no arquivo on-line usando uma replicação de log e, em seguida, transmite as alterações capturadas para um logstream.
2. O publicador consome dados do fluxo de log do sistema.
3. O publicador comunica as alterações de dados capturadas ao mecanismo de destino por meio de TCP/IP. O Controller Daemon autentica a comunicação entre os ambientes de origem e de destino.
4. O mecanismo de aplicação no ambiente de destino recebe as alterações do agente do Publisher e as aplica a um banco de dados relacional ou não relacional.

Migração de arquivos VSAM para o Amazon MSK

O diagrama a seguir mostra como transmitir estruturas de dados VSAM de um mainframe para o Amazon MSK no modo de alto desempenho e gerar automaticamente conversões de esquema JSON ou AVRO que se integram ao Amazon MSK.

O diagrama mostra o seguinte fluxo de trabalho em lote:

1. O Connect captura as alterações em um arquivo usando o CICS VR ou comparando arquivos VSAM de arquivos de backup para identificar alterações. As alterações capturadas são enviadas para o fluxo de registros.
2. O publicador consome dados do fluxo de log do sistema.
3. O publicador comunica as alterações de dados capturadas ao mecanismo de destino por meio de TCP/IP. O Controller Daemon autentica a comunicação entre os ambientes de origem e de destino.
4. O Replicator Engine que está operando no modo de processamento paralelo divide os dados em uma unidade de cache de trabalho.
5. Os segmentos de trabalho capturam os dados do cache.
6. Os dados são publicados nos tópicos do Amazon MSK a partir dos segmentos de trabalho.
7. Os usuários aplicam alterações do Amazon MSK a destinos como Amazon DynamoDB, Amazon Simple Storage Service (Amazon S3) ou Amazon Service usando conectores OpenSearch .

O diagrama mostra o seguinte fluxo de trabalho on-line:

1. As alterações no arquivo on-line são capturadas usando uma replicação de log. As alterações capturadas são transmitidas para o logstream.
2. O publicador consome dados do fluxo de log do sistema.
3. O publicador comunica as alterações de dados capturadas ao mecanismo de destino por meio de TCP/IP. O Controller Daemon autentica a comunicação entre os ambientes de origem e de destino.
4. O Replicator Engine que está operando no modo de processamento paralelo divide os dados em uma unidade de cache de trabalho.
5. Os segmentos de trabalho capturam os dados do cache.
6. Os dados são publicados nos tópicos do Amazon MSK a partir dos segmentos de trabalho.
7. Os usuários aplicam alterações do Amazon MSK a destinos como DynamoDB, Amazon S3 ou Service usando conectores OpenSearch .

Ferramentas

- O Amazon Managed Streaming for Apache Kafka (Amazon MSK) é um serviço totalmente gerenciado que ajuda você a criar e executar aplicações que usam o Apache Kafka para processar dados em streaming.

- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.

Épicos

Prepare o ambiente de origem (mainframe)

Tarefa	Descrição	Habilidades necessárias
Instale o Connect CDC 4.1.	1. Entre em contato com a equipe do Precisely Support para obter uma licença e pacotes de instalação. 2. Use o exemplo JCLs para instalar o Connect CDC 4.1. Para obter instruções, consulte Install Connect CDC (SQData) usando JCL na documentação do Precisely. 3. Execute o comando `SETPROG APF` para autorizar as bibliotecas de carregamento do SQDATA.V4nnn.LOADLIB.	Desenvolvedor/administrador de mainframe IBM
Configure o diretório zFS.	Para configurar um diretório zFS, siga as instruções dos diretórios de variáveis do zFS na documentação do Precisely. **Note** Controller Daemon e sistema de arquivos Capture/Publisher	Desenvolvedor/administrador de mainframe IBM

Tarefa	Descrição	Habilidades necessárias
	agent configura tions are stored in the z/OS UNIX Systems Services (conhecido como zFS). Os agentes Controller Daemon, Capture, Storage e Publisher exigem uma estrutura de diretório s zFS predefinida para armazenar um pequeno número de arquivos.	
Configure portas TCP/IP.	Para configurar portas TCP/IP, siga as instruções das portas TCP/IP na documentação do Precisely. **Note** O Daemon do controlador requer portas TCP/IP nos sistemas de origem. As portas são referenciadas pelos mecanismos nos sistemas de destino (onde os dados de alteração capturados são processados).	Desenvolvedor/administrador de mainframe IBM

Tarefa	Descrição	Habilidades necessárias
Crie um logstream do z/OS.	Para criar um logstream do z/OS, siga as instruções de Criar fluxos de registros do sistema z/OS na documentação do Preciously. **Note** O Connect usa o logstream para capturar e transmitir dados entre o ambiente de origem e o ambiente de destino durante a migração. Para ver um exemplo de JCL que cria um z/OS LogStream, consulte Criar LogStreams do sistema z/OS na documentação Precisely.	Desenvolvedor de mainframe da IBM
Identifique e autorize IDs usuários do zFS e tarefas iniciadas.	Use o RACF para conceder acesso ao sistema de arquivos OMVS zFS. Para ver um exemplo de JCL, consulte Identificar e autorizar o usuário do ZFS e a tarefa iniciada IDs na documentação do Precisely.	Desenvolvedor/administrador de mainframe IBM

Tarefa	Descrição	Habilidades necessárias
Gere as chaves públicas/privadas do z/OS e o arquivo de chave autorizado.	Execute o JCL para gerar o par de chaves. Para obter um exemplo, consulte Exemplo de par de chaves na seção Informações adicionais desse padrão. Para obter instruções, consulte Gerar chaves públicas e privadas do z/OS e o arquivo de chave autorizado na documentação do Precisely .	Desenvolvedor/administrador de mainframe IBM

Ative o CICS VSAM Log Replicate e anexe-o ao fluxo de logs.	Execute o seguinte script JCL:
	
	``
	 //STEP1 EXEC PGM=IDCAMS
	 //SYSPRINT DD SYSOUT=*
	 //SYSIN DD *
	   ALTER SQDATA.CICS.FILEA -
	   LOGSTREAMID(SQDATA.VSAMCDC.LOG1) -
	   LOGREPLICATE
	``
		Desenvolvedor/administrador de mainframe IBM

Tarefa	Descrição	Habilidades necessárias
Ative o log de recuperação de arquivos VSAM por meio de um FCT.	Modifique a Tabela de controle de arquivos (FCT - File Control Table) para refletir as seguintes alterações de parâmetros: `Configure FCT Parms CEDA ALT FILE(name) GROUP(groupname) DSNAME(data set name) RECOVERY(NONE|BACKOUTONLY|ALL) FWDRECOVLOG(NO|1-99) BACKUPTYPE(STATIC|DYNAMIC) RECOVERY PARAMETERS RECOVery : None | Backoutonly | All Fwdrecovlog : No | 1-99 BAckuptype : Static | Dynamic`	Desenvolvedor/administrador de mainframe IBM
Configure o CDCz Log para o agente do Publisher.	1. Crie o arquivo CAB do CDCz Log Publisher. 2. Criptografe os dados publicados. 3. Prepare o CDCz Log Publisher Runtime JCL.	Desenvolvedor/administrador de mainframe IBM

Tarefa	Descrição	Habilidades necessárias
Ative o Daemon do controlador.	1. Abra o painel do ISPF e execute o seguinte comando para abrir o menu Precisamente: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar o Daemon do controlador, escolha a opção 2 no menu.	Desenvolvedor/administrador de mainframe IBM
Ative o publicador.	1. Abra o painel do ISPF e execute o seguinte comando para abrir o menu Precisamente: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar o publicador, escolha a opção 3 no menu e eu para inserir.	Desenvolvedor/administrador de mainframe IBM

Tarefa	Descrição	Habilidades necessárias
Ative o fluxo de registro.	1. Abra o painel do ISPF e execute o seguinte comando para abrir o menu Precisamente: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar o fluxo de registros, escolha a opção 4 no menu e eu para inserir. Em seguida, insira o nome do fluxo de logs criado nas etapas anteriores.	Desenvolvedor/administrador de mainframe IBM

Preparar o ambiente de destino (AWS)

Tarefa	Descrição	Habilidades necessárias
Instale com precisão em uma EC2 instância.	Para instalar o Connect from Precisely no Amazon Linux AMI para Amazon EC2, siga as instruções de Install Connect CDC (SQData) no UNIX na documentação do Precisely.	AWS geral
Abra portas TCP/IP.	Para modificar o grupo de segurança para incluir as portas do Controller Daemon para acesso de entrada e saída, siga as instruções do TCP/IP na documentação do Precisely.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie diretórios de arquivos.	Para criar diretórios de arquivos, siga as instruções de Preparar o ambiente de aplicação de destino na documentação do Precisely.	AWS geral

Crie o arquivo de configuração do Apply Engine.	Crie o arquivo de configuração do Apply Engine no diretório de trabalho do Apply Engine. O exemplo de arquivo de configuração a seguir mostra o Apache Kafka como destino:
	`builtin.features=SASL_SCRAM`
	`security.protocol=SASL_SSL`
	`sasl.mechanism=SCRAM-SHA-512`
	`sasl.username=`
	`sasl.password=`
	`metadata.broker.list=`
	Note
	Para obter mais informações, consulte Segurança na documentação do Apache Kafka.
		AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie scripts para o processamento do Apply Engine.	Crie os scripts para que o Apply Engine processe os dados de origem e replique os dados de origem para o destino. Para obter mais informações, consulte Criar um script de mecanismo de aplicação na documentação do Precisely.	AWS geral
Execute os scripts.	Use os comandos `SQDPARSE` e `SQDENG` para executar o script. Para obter mais informações, consulte Analisar um script para ZoS na documentação do Precisely.	AWS geral

Valide o ambiente

Tarefa	Descrição	Habilidades necessárias
Valide a lista de arquivos VSAM e tabelas de destino para processamento de CDC.	1. Valide arquivos VSAM, incluindo logs de replicação, logs de recuperação, parâmetros FCT e o fluxo de logs. 2. Valide as tabelas do banco de dados de destino, incluindo se as tabelas foram criadas de acordo com a definição de esquema necessária, o acesso à tabela e outros critérios.	AWS geral, Mainframe

Tarefa	Descrição	Habilidades necessárias
Verifique se o SQData produto Connect CDC está vinculado.	Execute um trabalho de teste e verifique se o código de retorno desse trabalho é 0 (bem-sucedido). **Note** As mensagens de status do Connect CDC SQData Apply Engine devem mostrar mensagens de conexão ativas.	AWS geral, Mainframe

Execute e valide casos de teste (Batch)

Tarefa	Descrição	Habilidades necessárias
Execute o trabalho em lotes no mainframe.	Execute o trabalho de aplicação em lote usando um JCL modificado. Inclua etapas na JCL modificada que façam o seguinte: 1. Faça um backup dos arquivos de dados. 2. Compare o arquivo de backup com os arquivos de dados modificados, gere o arquivo delta e anote a contagem de registros delta das mensagens. 3. Envie o arquivo delta para o fluxo de log do z/OS.	AWS geral, Mainframe

Tarefa	Descrição	Habilidades necessárias
	4. Execute o JCL. Para ver um exemplo de JCL, consulte Preparar arquivo, comparar e capturar JCL na documentação do Preciousl y.	
Verifique o fluxo de logs.	Verifique o fluxo de registros para confirmar que você pode ver os dados de alteração do trabalho em lote concluído do mainframe.	AWS geral, Mainframe
Valide as contagens das alterações do delta de origem e da tabela de destino.	Para confirmar se os registros foram contabilizados, faça o seguinte: 1. Reúna a contagem delta de origem das mensagens JCL em lote. 2. Monitore o Apply Engine para ver as contagens em nível de registro do número de registros inseridos, atualizados ou excluídos no arquivo VSAM. 3. Consulte a tabela de destino para ver as contagens de registros. 4. Compare e contabili ze todas as diferentes contagens de registros.	AWS geral, Mainframe

Execute e valide casos de teste (on-line)

Tarefa	Descrição	Habilidades necessárias
Execute a transação on-line em uma região do CICS.	1. Execute a transação on-line para validar o caso de teste. 2. Valide o código de execução da transação (RC=0 – Sucesso).	Desenvolvedor de mainframe da IBM
Verifique o fluxo de logs.	Confirme se o fluxo de registros está preenchido com alterações específicas no nível do registro.	Desenvolvedor do AWS Mainframe
Valide a contagem no banco de dados de destino.	Monitore o mecanismo de aplicação para obter contagens de níveis recordes.	Precisely, Linux
Valide as contagens de registros e os registros de dados no banco de dados de destino.	Consulte o banco de dados de destino para validar as contagens de registros e os registros de dados.	AWS geral

Recursos relacionados

- VSAM z/OS (documentação do Precisely)
- Aplique o mecanismo (documentação do Precisely)
- Mecanismo replicador (documentação do Precisely)
- O fluxo de logs (documentação da IBM)

Mais informações

Exemplo do arquivo de configuração

Este é um exemplo de arquivo de configuração para um fluxo de logs em que o ambiente de origem é um mainframe e o ambiente de destino é o Amazon MSK:

```
 -- JOBNAME -- PASS THE SUBSCRIBER NAME
 -- REPORT  progress report will be produced after "n" (number) of Source records
processed.

 JOBNAME VSMTOKFK;
 --REPORT EVERY 100;
 -- Change Op has been ‘I’ for insert, ‘D’ for delete , and ‘R’ for Replace. For RDS
it is 'U' for update
 -- Character Encoding on z/OS is Code Page 1047, on Linux and UNIX it is Code Page
819 and on Windows, Code Page 1252
 OPTIONS
 CDCOP('I', 'U', 'D'),
 PSEUDO NULL = NO,
 USE AVRO COMPATIBLE NAMES,
 APPLICATION ENCODING SCHEME = 1208;

 --       SOURCE DESCRIPTIONS

 BEGIN GROUP VSAM_SRC;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       TARGET DESCRIPTIONS

 BEGIN GROUP VSAM_TGT;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       SOURCE DATASTORE (IP & Publisher name)

 DATASTORE cdc://10.81.148.4:2626/vsmcdct/VSMTOKFK
 OF VSAMCDC
 AS CDCIN
 DESCRIBED BY GROUP VSAM_SRC ACCEPT ALL;

 --       TARGET DATASTORE(s) - Kafka and topic name

 DATASTORE 'kafka:///MSKTutorialTopic/key'
 OF JSON
```

```
  AS CDCOUT
  DESCRIBED BY GROUP VSAM_TGT FOR INSERT;

  --       MAIN SECTION

  PROCESS INTO
  CDCOUT
  SELECT
  {
  SETURL(CDCOUT, 'kafka:///MSKTutorialTopic/key')
  REMAP(CDCIN, account_file, GET_RAW_RECORD(CDCIN, AFTER), GET_RAW_RECORD(CDCIN,
 BEFORE))
  REPLICATE(CDCOUT, account_file)
  }
  FROM CDCIN;
```

Exemplo de par de chaves

Este é um exemplo de como executar o JCL para gerar o par de chaves:

```
//SQDUTIL EXEC PGM=SQDUTIL //SQDPUBL DD DSN=&USER..NACL.PUBLIC, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPKEY DD DSN=&USER..NACL.PRIVATE, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPARMS DD  keygen //SYSPRINT DD SYSOUT= //SYSOUT DD SYSOUT=* //
SQDLOG DD SYSOUT=* //*SQDLOG8 DD DUMMY
```

Modernize o gerenciamento de saída do mainframe AWS usando o Rocket Enterprise Server e o LRS X PageCenter

Criado por Shubham Roy (AWS), Abraham Rondon (Micro Focus) e Guy Tucker (Levi, Ray and Shoup Inc)

Resumo

Ao modernizar seu gerenciamento de produção de mainframe, você pode obter economia de custos, reduzir a dívida técnica de manter sistemas legados e melhorar a resiliência e a agilidade por meio de tecnologias nativas em nuvem da Amazon Web DevOps Services (AWS). Esse padrão mostra como modernizar suas workloads de gerenciamento de saída de mainframe essenciais para os negócios na Nuvem AWS. O padrão usa o Rocket Enterprise Server como tempo de execução para um aplicativo de mainframe modernizado, com a Levi, Ray & Shoup, Inc. (LRS) VPSX/MFI (Micro Focus Interface) como servidor de impressão e o LRS X como servidor de arquivamento. PageCenter O LRS PageCenter X fornece soluções de gerenciamento de resultados para visualização, indexação, pesquisa, arquivamento e proteção do acesso aos resultados comerciais.

O padrão é baseado na abordagem de modernização do mainframe de redefinir a plataforma. Os aplicativos de mainframe são migrados pela AWS Mainframe Modernization na Amazon Elastic Compute Cloud (Amazon). EC2 As cargas de trabalho de gerenciamento de saída do mainframe são migradas para a Amazon EC2, e um banco de dados de mainframe, como o IBM Db2 for z/OS, é migrado para o Amazon Relational Database Service (Amazon RDS). O LRS Directory Integration Server (LRS/DIS) funciona com o AWS Directory Service for Microsoft Active Directory para autenticação e autorização do fluxo de trabalho de gerenciamento de saída.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma workload de gerenciamento de saída de mainframe.
- Conhecimento básico de como reconstruir e entregar um aplicativo de mainframe executado no Rocket Enterprise Server. Para obter mais informações, consulte a planilha de dados do Rocket Enterprise Server na documentação do Rocket Software.
- Conhecimento básico das soluções e conceitos de impressão em nuvem da LRS. Para obter mais informações, consulte Modernização de saída na documentação do LRS.

- Software e licença do Rocket Enterprise Server. Para obter mais informações, entre em contato com a Rocket Software.
- VPSX/MFI, LRS PageCenterX, LRS/Queue, and LRS/DISSoftware e licenças do LRS. Para obter mais informações, entre em contato com LRS. Você deve fornecer os nomes de host das EC2 instâncias em que os produtos LRS serão instalados.

> **Note**
>
> Para obter mais informações sobre considerações de configuração para cargas de trabalho de gerenciamento de saída de mainframe, consulte Considerações na seção Informações adicionais desse padrão.

Versões do produto

- Servidor Rocket Enterprise 10.0
- LRS VPSX/MFI
- LRS PageCenter X V1R3 ou posterior

Arquitetura

Pilha de tecnologia de origem

- Sistema operacional: IBM z/OS
- Linguagem de programação — linguagem comum orientada a negócios (COBOL), linguagem de controle de tarefas (JCL) e Sistema de Controle de Informações do Cliente (CICS)
- Banco de dados: IBM Db2 for z/OS, banco de dados IBM Information Management System (IMS) e Virtual Storage Access Method (VSAM)
- Segurança — Instalação de Controle de Acesso a Recursos (RACF), CA Top Secret para z/OS e Instalação de Controle de Acesso 2 () ACF2
- Soluções de impressão e arquivamento: produtos de saída e impressão z/OS de mainframe IBM (IBM Infoprint Server for z/OS, LRS e CA Deliver) e soluções de arquivamento (CA Deliver, ASG Mobius ou CA Bundle)

Arquitetura de origem

O diagrama a seguir mostra uma arquitetura típica do estado atual para uma workload de gerenciamento de saída de mainframe.

O diagrama mostra o seguinte fluxo de trabalho:

1. Os usuários realizam transações comerciais em um sistema de engajamento (SoE) construído em um aplicativo IBM CICS escrito em COBOL.
2. O SoE invoca o serviço de mainframe, que registra os dados da transação comercial em um banco de dados system-of-records (SoR), como o IBM Db2 for z/OS.
3. O SoR persiste os dados comerciais do SoE.
4. O agendador de trabalhos em lotes inicia um trabalho em lotes para gerar a saída de impressão.
5. O trabalho em lotes extrai dados do banco de dados. Ele formata os dados de acordo com os requisitos comerciais e, em seguida, gera resultados comerciais, como extratos de cobrança, carteiras de identidade ou extratos de empréstimos. Por fim, o trabalho em lotes encaminha a saída para o gerenciamento de saída para formatação, publicação e armazenamento da saída com base nos requisitos comerciais.
6. O gerenciamento de saída recebe a saída do trabalho em lotes. O gerenciamento de saída indexa, organiza e publica a saída em um destino específico no sistema de gerenciamento de saída, como as soluções LRS PageCenter X (conforme demonstrado nesse padrão) ou o CA View.
7. Os usuários podem visualizar, pesquisar e recuperar a saída.

Pilha de tecnologias de destino

- Sistema operacional — Windows Server em execução na Amazon EC2
- Computação — Amazon EC2
- Armazenamento — Amazon Elastic Block Store (Amazon EBS) e FSx Amazon para Windows File Server
- Linguagem de programação: COBOL, JCL e CICS
- Banco de dados: Amazon RDS
- Segurança: AWS Managed Microsoft AD

- Impressão e arquivamento — solução de impressão LRS (VPSX) e arquivamento (PageCenterX) na AWS
- Ambiente de execução do mainframe — Rocket Enterprise Server

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para uma workload de gerenciamento de saída de mainframe que é implantada na Nuvem AWS.

O diagrama mostra o seguinte fluxo de trabalho:

1. O agendador de trabalhos em lotes inicia um trabalho em lotes para criar resultados, como extratos de cobrança, cartões de identificação ou extratos de empréstimos.
2. O trabalho em lote do mainframe (reformulado para a Amazon EC2) usa o tempo de execução do Rocket Enterprise Server para extrair dados do banco de dados do aplicativo, aplicar lógica de negócios aos dados e formatar os dados. Em seguida, ele envia os dados para um destino de saída usando o módulo de saída da impressora Rocket Software (documentação da OpenText Micro Focus).
3. O banco de dados do aplicativo (um SoR executado no Amazon RDS) persiste os dados para a saída de impressão.
4. O agente de VPSX/MFI printing solution is deployed on Amazon EC2, and its operational data is stored in Amazon EBS. LRS VPSX/MFI uses the TCP/IP-based LRS/Queue transmissão LRS para coletar dados de saída por meio da API de saída de impressão JES da Rocket Software.

   O LRS VPSX/MFI faz o pré-processamento de dados, como a tradução de EBCDIC para ASCII. Ele também executa tarefas mais complexas, incluindo a conversão de fluxos de dados exclusivos do mainframe, como IBM Advanced Function Presentation (AFP) e Xerox Line Conditioned Data Stream (LCDS), em fluxos de dados de visualização e impressão mais comuns, como Printer Command Language (PCL) e PDF.

   Durante a janela de manutenção do LRS PageCenter X, o LRS VPSX/MFI persists the output queue and serves as backup for the output queue. LRS VPSX/MFI connects and sends output to LRS PageCenterX by using the LRS/Queue protocol. LRS/Queue realiza uma troca de prontidão e conclusão dos trabalhos para ajudar a garantir que a transferência de dados ocorra.

   Observações:

Para obter mais informações sobre dados de impressão transmitidos do Rocket Software Print Exit para mecanismos de lote de mainframe LRS/Queue and LRS VPSX/MFI suportados, consulte Captura de dados de impressão na seção Informações adicionais.

O LRS VPSX/MFI pode realizar verificações de integridade no nível da frota de impressoras. Para obter mais informações, consulte Verificações de integridade da frota de impressoras na seção Informações adicionais desse padrão.

5. A solução de gerenciamento de saída LRS PageCenter X é implantada na Amazon EC2 e seus dados operacionais são armazenados no Amazon FSx for Windows File Server. O LRS PageCenter X fornece um sistema central de gerenciamento de relatórios de todos os arquivos importados para o LRS PageCenter X junto com todos os usuários capazes de acessar os arquivos. Os usuários podem visualizar o conteúdo específico do arquivo ou realizar pesquisas em vários arquivos para verificar os critérios correspondentes.

   O servidor de aplicativos LRS/NetX component is a multi-threaded web application server that provides a common runtime environment for the LRS PageCenterX application and other LRS applications. The LRS/Web Connect component is installed on your web server and provides a connector from the web server to the LRS/NetX web.
6. O LRS PageCenter X fornece armazenamento para objetos do sistema de arquivos. Os dados operacionais do LRS PageCenter X são armazenados no Amazon FSx for Windows File Server.
7. A autenticação e autorização do gerenciamento de saída são realizadas pelo AWS Managed Microsoft AD com LRS/DIS.

> **Note**
>
> A solução de destino normalmente não exige alterações no aplicativo para acomodar linguagens de formatação de mainframe, como IBM AFP ou Xerox LCDS.

Arquitetura de infraestrutura da AWS

O diagrama a seguir mostra uma arquitetura de infraestrutura da AWS altamente disponível e segura para uma workload de gerenciamento de saída de mainframe.

O diagrama mostra o seguinte fluxo de trabalho:

1. O agendador de lotes inicia o processo em lote e é implantado na Amazon EC2 em várias zonas de disponibilidade para alta disponibilidade (HA).

> **Note**
>
> Esse padrão não abrange a implementação do agendador de lotes. Para obter mais informações sobre implementação, consulte a documentação do fornecedor de software para o agendador.

2. O trabalho em lote do mainframe (escrito em uma linguagem de programação como JCL ou COBOL) usa a lógica comercial principal para processar e gerar resultados impressos, como extratos de cobrança, cartões de identificação e extratos de empréstimos. O trabalho em lote é implantado na Amazon EC2 em duas zonas de disponibilidade para HA. Ele usa a API de saída de impressão da Rocket Software para rotear a saída de impressão para o LRS VPSX/MFI para pré-processamento de dados.
3. O servidor de impressão LRS VPSX/MFI é implantado na Amazon em duas zonas de disponibilidade para HA (par redundante ativo EC2 em espera). Ele usa o Amazon EBS como um armazenamento de dados operacional. O Network Load Balancer executa uma verificação de integridade nas instâncias VPSX/MFI do LRS. EC2 Se uma instância ativa não estiver íntegra, o balanceador de carga encaminha o tráfego para instâncias standby a quente na outra zona de disponibilidade. As solicitações de impressão persistem no LRS Job Queue localmente em cada uma das instâncias. EC2 Em caso de falha, uma instância com falha deve ser reiniciada antes que os serviços do LRS possam retomar o processamento da solicitação de impressão.

> **Note**
>
> O LRS VPSX/MFI também pode realizar verificações de saúde no nível da frota de impressoras. Para obter mais informações, consulte Verificações de integridade da frota de impressoras na seção Informações adicionais desse padrão.

4. O gerenciamento de saída do LRS PageCenter X é implantado na Amazon EC2 em duas zonas de disponibilidade para HA (par redundante ativo em espera). Ele usa o Amazon FSx for Windows File Server como um armazenamento de dados operacional. Se uma instância ativa não estiver íntegra, o balanceador de carga executará uma verificação de integridade nas instâncias do LRS PageCenter X e encaminhará o tráfego para EC2 instâncias em espera na outra zona de disponibilidade.

5. Um Network Load Balancer fornece um nome DNS para integrar o servidor LRS VPSX/MFI com o LRS X. PageCenter

> **Note**
>
> O LRS PageCenter X oferece suporte a um balanceador de carga de camada 4.

6. O LRS PageCenter X usa o Amazon FSx for Windows File Server como um armazenamento de dados operacional implantado em duas zonas de disponibilidade para HA. O LRS PageCenter X compreende somente os arquivos que estão no compartilhamento de arquivos, não em um banco de dados externo.
7. O AWS Managed Microsoft AD é usado com o LRS/DIS para realizar a autenticação e autorização do fluxo de trabalho de gerenciamento de saída. Para obter mais informações, consulte Autenticação e autorização de saída de impressão na seção Informações adicionais.

Ferramentas

Serviços da AWS

- O AWS Directory Service para Microsoft Active Directory permite que cargas de trabalho com reconhecimento de diretório e recursos da AWS usem o Microsoft Active Directory na Nuvem AWS.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (Amazon). EC2
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre EC2 instâncias, contêineres e endereços IP da Amazon em uma ou mais zonas de disponibilidade. Esse padrão usa um Network Load Balancer.
- FSxA Amazon fornece sistemas de arquivos que suportam protocolos de conectividade padrão do setor e oferecem alta disponibilidade e replicação em todas as regiões da AWS. Esse padrão usa o Amazon FSx para Windows File Server.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.

Outras ferramentas

- O software LRS PageCenter X fornece uma solução escalável de gerenciamento de conteúdo de documentos e relatórios que ajuda os usuários a obter o máximo valor das informações por meio de indexação automatizada, criptografia e recursos avançados de pesquisa.
- O LRS VPSX/MFI (Micro Focus Interface), desenvolvido em conjunto pela LRS e pela Rocket Software, captura a saída de um spool JES da Rocket Software e a entrega de forma confiável a um destino de impressão especificado.
- LRS/Queue is a transmission agent that's TCP/IP based. LRS VPSX/MFI uses LRS/Queuepara coletar ou capturar dados de impressão por meio da interface de programação JES Print Exit da Rocket Software.
- O LRS Directory Integration Server (LRS/DIS) é usado para autenticação e autorização durante o fluxo de trabalho de impressão.
- O Rocket Enterprise Server é um ambiente de implantação de aplicativos para aplicativos de mainframe. Ele fornece o ambiente de execução para aplicativos de mainframe que são migrados ou criados usando qualquer versão do Rocket Enterprise Developer.

Épicos

Configure o tempo de execução do Rocket e implante um aplicativo em lote de mainframe

Tarefa	Descrição	Habilidades necessárias
Configure o runtime e implante um aplicativo de demonstração.	Para configurar o Rocket Enterprise Server na Amazon EC2 e implantar o aplicativo de BankDemo demonstração da Rocket Software, siga as instruções no guia do usuário do AWS Mainframe Modernization. O BankDemo aplicativo é um aplicativo em lote de mainframe que cria e, em	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	seguida, inicia a saída de impressão.	

Configurar um servidor de impressão LRS na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Crie uma instância EC2 do Amazon Windows.	Para iniciar uma instância EC2 do Amazon Windows, siga as instruções em Iniciar uma EC2 instância da Amazon na EC2 documentação da Amazon. Use o mesmo nome de host que você usou para sua licença de produto LRS. Sua instância deve atender aos seguintes requisitos de hardware e software para LRS VPSX/MFI: • CPU: Dual Core • MEMÓRIA RAM: 16 GB • Unidade: 500 GB • EC2 Instância mínima — `m5.xlarge` • SISTEMA OPERACIONAL: Windows • Software: Internet Informati on Service (IIS) ou Apache	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Note Os requisitos anteriores de hardware e software são destinados a uma pequena frota de impressoras (cerca de 500-1000). Para obter todos os requisitos, consulte seus contatos do LRS e da AWS. 1. Ao criar sua instância do Windows, confirme se o EC2 nome do host é o mesmo usado para a licença do produto LRS. 2. Conecte-se à sua EC2 instância seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 3. No menu Iniciar do Windows, abra Gerenciador do Servidor. 4. No Gerenciador do Servidor, escolha Painel, Início Rápido, Adicionar funções e recursos e, em seguida, escolha Funções do servidor.	

Tarefa	Descrição	Habilidades necessárias
	5. Em Funções de servidor, escolha WebServer (IIS) e, em seguida, escolha Desenvolvimento de aplicativos. 6. Em Desenvolvimento de aplicativos, marque a caixa de seleção CGI. 7. Para instalar o CGI, siga as instruções no assistent e para Adicionar funções e recursos do Windows Server Manager. 8. Abra a porta 5500 no firewall do Windows da EC2 instância para comunicação LRS/Queue.	

Tarefa	Descrição	Habilidades necessárias
Instale o LRS VPSX/MFI na instância. EC2	1. Conecte-se à sua EC2 instância. 2. Abra o link para a página de download do produto a partir da mensagem de e-mail do LRS que você deve ter recebido. **Note** Os produtos LRS são distribuídos por transferência eletrônica de arquivos (TEF). 3. Baixe o LRS VPSX/MFI e descompacte o arquivo (pasta padrão: `c:\LRS`). 4. Para instalar o LRS VPSX/MFI, inicie o LRS Product Installer a partir da pasta descompactada. 5. No menu Seleciona r recursos, selecione Servidor VPSX® e escolha Avançar para iniciar o processo de instalaçã o. Você receberá uma mensagem de sucesso quando a instalação for concluída.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Instale o LRS/Queue.	1. Conecte-se à sua EC2 instância do Rocket Enterprise Server. 2. Abra o link para a página de download do produto LRS a partir da mensagem de e-mail do LRS que você deve ter recebido, baixe o LRS/Queue e, em seguida, descompacte o arquivo. 3. Navegue até o local onde você baixou os arquivos e, em seguida, inicie o LRS Product Installer para instalar o LRS/Queue. 4. Siga as instruções no instalador do produto LRS para concluir o processo de instalação.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Instale o LRS/DIS.	O LRS/DIS product often is included in LRS VPSX installation. However, if LRS/DIS não foi instalado junto com o LRS VPSX, use as seguintes etapas para instalá-lo: 1. Conecte-se à sua instância LRS EC2 VPSX/MFI. 2. Abra o link para a página de download do produto LRS a partir da mensagem de e-mail do LRS que você deve ter recebido, baixe o LRS/DIS e, em seguida, descompacte o arquivo. 3. Navegue até o local em que você fez o download dos arquivos e, em seguida, inicie o LRS Product Installer. 4. No LRS Product Installer, expanda LRS Misc Tools, selecione LRS DIS e escolha Avançar. 5. Siga o restante das instruções no instalador do produto LRS para concluir o processo de instalação.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de destino.	Crie um grupo de destino seguindo as instruções em Criar um grupo de destino para o Network Load Balancer. Ao criar o grupo de destino, registre a instância LRS EC2 VPSX/MFI como destino: 1. Na página Especificar detalhes do grupo, em Escolher um Tipo de destino, escolha Instâncias. 2. Para Protocol, escolha TCP. 3. Em Porta, escolha 5500. 4. Na página Registrar destinos, na seção Instâncias disponíveis, selecione a instância LRS EC2 VPSX/MFI.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar um Network Load Balancer.	Para criar o Network Load Balancer, siga as instruções na documentação do Elastic Load Balancing. Seu Network Load Balancer roteia o tráfego do Rocket Enterprise Server para a instância LRS VPSX/MFI. EC2 Ao criar o Network Load Balancer, escolha os seguintes valores na página Receptores e roteamento: 1. Para Protocolo, escolha TCP. 2. Em Porta, escolha 5500. 3. Em Ação padrão, escolha Encaminhar para o grupo de destino que você criou anteriormente.	Arquiteto de nuvem

Integre o Rocket Enterprise Server com LRS/Queue and LRS VPSX/MFI

Tarefa	Descrição	Habilidades necessárias
Configure o Rocket Enterprise Server para integração LRS/Queue.	1. Conecte-se à sua EC2 instância do Rocket Enterprise Server seguindo as instruções na EC2 documentação da Amazon. 2. No menu Iniciar do Windows, abra a interface	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	de administração do Rocket Enterprise Server. 3. Na barra de menu, escolha NATIVO. 4. No painel de navegação , escolha Servidor de Diretórios e, em seguida, escolha BANKDEMO para sua região do Enterprise Server. 5. Em Geral, no painel de navegação esquerdo, role para baixo até a seção Adicional para configurar as variáveis de ambiente (`LRSQ_ADDRESS` , `LRSQ_PORT` e `LRSQ_COMMAND`) para apontar para o LRSQ. • Para LRSQ_ADDRESS, insira o endereço IP ou o nome DNS do Network Load Balancer que você criou anteriormente. • Para LRSQ_PORT, insira VPSX LRSQ Listener Port (5500). • Para LRSQ_COMMAND, insira a localização do caminho do executável do LRSQ.	

Tarefa	Descrição	Habilidades necessárias
	Note Atualmente, o LRS suporta um limite máximo de 50 caracteres para nomes DNS. Se seu nome DNS tiver mais de 50 caracteres, você poderá usar o endereço IP do Network Load Balancer como alternativa.	

Tarefa	Descrição	Habilidades necessárias
Configure o Rocket Enterpris e Server para integração LRS VPSX/MFI.	1. Copie a `VPSX_MFI_R2` pasta do instalador LRS VPSX/MFI para o local do Rocket Enterprise Server em. `C\BANKDEMO\print` 2. Conecte-se à sua EC2 instância do Rocket Enterprise Server seguindo as instruções na EC2 documentação da Amazon. 3. No menu Iniciar do Windows, abra a interface de administração do Rocket Enterprise Server. 4. Na barra de menus, selecione NATIVE. 5. No painel de navegação , escolha Servidor do diretório e BANKDEMO. 6. Em BANKDEMO, escolha JES. 7. Em JES Program Path, adicione o `DLL(VPSX_MFI_R2)` caminho de `C\BANKDEMO\print` .	Arquiteto de nuvem

Configurar a fila de impressão e os usuários de impressão

Tarefa	Descrição	Habilidades necessárias
Associe o módulo de saída de impressão do software Rocket ao processo de execução do	1. Conecte-se à sua EC2 instância do Rocket Enterprise Server seguindo	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
servidor da impressora em lote Rocket Enterprise Server.	as instruções na EC2 documentação da Amazon. 2. No menu Iniciar do Windows, abra a interface de usuário do Rocket Focus Enterprise Server Administration. 3. Na barra de menus, selecione NATIVE. 4. No painel de navegação, escolha Servidor do diretório e BANKDEMO. 5. Em BANKDEMO, escolha JES e role para baixo até Impressoras. 6. Em Impressoras, associe o módulo de saída de impressão da Rocket Software (para LRSPRTE6 lote) à impressora em lote Rocket Enterprise Server Server Server Server Server (SEP). Isso permite o roteamento da saída de impressão para LRS VPSX/MFI. Para obter mais informações sobre configuração, consulte Usando a saída na documentação da OpenText Micro Focus.	

Tarefa	Descrição	Habilidades necessárias
Crie uma fila de saída de impressão no LRS VPSX/MFI e integre-a ao LRS X. PageCenter	1. Conecte-se à sua instância LRS EC2 VPSX/MFI. 2. No menu Iniciar do Windows, abra a interface da web do VPSX. 3. No painel de navegação, escolha Impressoras. 4. Escolha Adicionar e Adicionar impressora. 5. Na página Configuração da impressora, em Nome da impressora, insira Local. 6. Para ID VPSX, insira. VPS1 7. Para CommType, selecione TCPIP/LRSQ. 8. Em Host/IP Address, insira o endereço IP do Network Load Balancer na frente das instâncias do LRS X. PageCenter EC2 9. Em Porta remota, insira 5800. 10. Em Fila remota, insira o nome da pasta de documentos do LRS PageCenter X onde a saída será armazenada. 11. Escolha Adicionar.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um usuário de impressão no LRS VPSX/MFI.	1. Conecte-se à sua instância LRS EC2 VPSX/MFI. 2. No menu Iniciar do Windows, abra a interface da web do VPSX. 3. No painel de navegação , escolha Segurança e depois Usuários. 4. Na coluna Nome de usuário, escolha admin e, em seguida, escolha Copiar. 5. Na janela Manutenção do perfil do usuário, em Nome do usuário, insira um nome de usuário (por exemplo, PrintUser). 6. Em Descrição, insira uma breve descrição (por exemplo, Usuário para impressão de teste). 7. Selecione Atualizar. Isso cria um usuário de impressão (por exemplo, PrintUser). 8. No painel de navegação, em Usuário, escolha o novo usuário que você criou. 9. No menu Comando, escolha Segurança. 10. Na página Regras de segurança, escolha todas as opções aplicáveis de	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	segurança da impressora e segurança do trabalho e, em seguida, escolha Salvar. 11. Para adicionar seu novo usuário de impressão ao grupo Administrador, no painel de navegação, escolha Segurança e, em seguida, Configurar. 12. Na janela Configuração de segurança, adicione seu novo usuário de impressão à coluna Administrador.	

Configurar um servidor LRS PageCenter X na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Crie uma instância EC2 do Amazon Windows.	Execute uma instância EC2 do Amazon Windows seguindo as instruções da Etapa 1: Inicie uma instância na EC2 documentação da Amazon. Use o mesmo nome de host que você usou para sua licença de produto LRS. Sua instância deve atender aos seguintes requisitos de hardware e software para o LRS PageCenter X: • CPU: Dual Core	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	• MEMÓRIA RAM: 16 GB • Unidade: 500 GB • EC2 Instância mínima — `m5.xlarge` • SISTEMA OPERACIONAL: Windows • Software: IIS ou Apache **Note** Os requisitos anteriores de hardware e software são destinados a uma pequena frota de impressoras (cerca de 500 a 1000). Para obter todos os requisitos, consulte seus contatos do LRS e da AWS. 1. Ao criar sua instância do Windows, confirme se o EC2 nome do host é o mesmo usado para a licença do produto LRS. 2. Conecte-se à sua EC2 instância seguindo as instruções na EC2 documentação da Amazon.	

Tarefa	Descrição	Habilidades necessárias
	3. No menu Iniciar do Windows, abra Gerenciador do Servidor. 4. No Gerenciador do Servidor, escolha Painel, Início Rápido, Adicionar funções e recursos e, em seguida, Funções do servidor. 5. Em Funções de servidor, escolha WebServer (IIS) e, em seguida, escolha Desenvolvimento de aplicativos. 6. Em Desenvolvimento de aplicativos, marque a caixa de seleção CGI. 7. Para instalar o CGI, siga as instruções no assistent e para Adicionar funções e recursos do Windows Server Manager. 8. Abra a porta 5800 para o TCP/IP traffic in the Windows firewall of the EC2 instance. LRS VPSX uses the TCPIP/LRSQ protocolo de entrada na porta 5800 para se comunicar com o LRS X. PageCenter	

Tarefa	Descrição	Habilidades necessárias
Instale o LRS PageCenter X na EC2 instância.	1. Conecte-se à sua EC2 instância. 2. Abra o link para a página de download do produto a partir da mensagem de e-mail do LRS que você deve ter recebido. **Note** Os produtos LRS são distribuídos por transferência eletrônica de arquivos (TEF). 3. Baixe o LRS PageCenter X e descompacte o arquivo (pasta padrão:`c:\LRS`). 4. Para instalar o LRS PageCenter X, inicie o LRS Product Installer a partir da pasta descompactada. 5. No menu Seleciona r recursos, selecione PageCenterX e escolha Avançar para iniciar o processo de instalaçã o. Você receberá uma mensagem de sucesso quando a instalação for concluída.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Instale o LRS/DIS.	O LRS/DIS product often is included in LRS VPSX installation. However, if LRS/DIS não foi instalado junto com o LRS VPSX, use as seguintes etapas para instalá-lo: 1. Conecte-se à sua EC2 instância do LRS PageCenter X. 2. Abra o link para a página de download do produto LRS a partir do e-mail do LRS que você deve ter recebido, baixe o LRS/DIS e, em seguida, descompacte o arquivo. 3. Navegue até o local em que você fez o download dos arquivos e, em seguida, inicie o LRS Product Installer. 4. No LRS Product Installer, expanda LRS Misc Tools, selecione LRS DIS e escolha Avançar. 5. Siga o restante das instruções no instalador do produto LRS para concluir o processo de instalação.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de destino.	Crie um grupo de destino seguindo as instruções em Criar um grupo de destino para o Network Load Balancer. Ao criar o grupo de destino, registre a EC2 instância do LRS PageCenter X como destino: 1. Na página Especificar detalhes do grupo, em Escolher um Tipo de destino, escolha Instâncias. 2. Para Protocol, escolha TCP. 3. Em Porta, escolha 5800. 4. Na página Registrar destinos, na seção Instâncias disponíveis, selecione a EC2 instância LRS PageCenter X.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar um Network Load Balancer.	Para criar o Network Load Balancer, siga as instruções na documentação do Elastic Load Balancing. Seu Network Load Balancer roteia o tráfego do LRS VPSX/MFI para a instância do LRS X. PageCenter EC2 Ao criar o Network Load Balancer, escolha os seguintes valores na página Receptores e roteamento: 1. Para Protocolo, escolha TCP. 2. Em Porta, escolha 5800. 3. Em Ação padrão, escolha Encaminhar para o grupo de destino que você criou anteriormente.	Arquiteto de nuvem

Configurar recursos de gerenciamento de saída no LRS X PageCenter

Tarefa	Descrição	Habilidades necessárias
Ative a função Importar no LRS X. PageCenter	Você pode usar a função LRS PageCenter X Import para reconhecer as saídas que chegam ao LRS PageCenter X por critérios como Job name ou Form ID. Em seguida, você pode rotear as saídas	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	para pastas específicas no PageCenter LRS X. Para habilitar a função de importação, faça o seguinte: 1. Conecte-se à sua EC2 instância do LRS PageCenter X seguindo as instruções na EC2 documentação da Amazon. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de pastas, escolha Admin. 4. Na página Configura ção, escolha Avançado, Parâmetro de importação. 5. Na seção Parâmetro de importação, marque a caixa de seleção Importação avançada. 6. Para confirmar as alteraçõe s, escolha Atualizar.	

Tarefa	Descrição	Habilidades necessárias
Configure a política de retenção de documentos.	O LRS PageCenter X usa uma política de retenção de documentos para decidir por quanto tempo manter um documento no PageCenter LRS X. Para configurar a política de retenção de documentos, faça o seguinte: 1. Conecte-se à sua EC2 instância do LRS PageCenter X. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de pastas, escolha Admin. 4. Na página Administrador, escolha Arquivar lista de grupos/administrador geral e, em seguida, escolha Política de retenção. 5. Na seção Política de retenção, escolha Adicionar para criar uma política de retenção. 6. Na página Informaçõ es sobre a política de retenção, insira o Nome da política de retenção, a Descrição e o período de Retenção do documento.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	7. Para salvar as alterações e criar a política, escolha Ok.	

Tarefa	Descrição	Habilidades necessárias
Crie uma regra para rotear o documento de saída para uma pasta específica no LRS PageCenter X.	No LRS PageCenter X, o Destino determina o caminho da pasta para onde a saída será enviada quando esse destino for chamado pela Definição de Relatório. Neste exemplo, crie uma pasta com base na pasta ID do formulário na definição do relatório e salve a saída nessa pasta. 1. Conecte-se à sua EC2 instância do LRS PageCenter X. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de pastas, escolha Administrador, Importação avançada, Destino. 4. Na seção Destino, escolha Adicionar para abrir o formulário Manutenção do destino. 5. Noformulário Manutenção de destino, insira os seguintes valores: • Nome do destino: formulário • Descrição: descrição do destino, como Estrutura de pastas baseada em formulário	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	• Tipo de destino: pasta • Parâmetros da pasta — Caminho da pasta de importação (o caminho da pasta que será criado no PageCenter X quando o documento chegar; por exemplo, o caminho **`/Test/&FORM/&IMPORTDATE/&IMPORTTIME`** criará uma pasta base, uma **`Test`** subpasta com base no nome Form-ID, uma subpasta com base na data de importação e **`STD`**, em seguida, uma subpasta com base na hora da importação) • Nome do documento: nome dinâmico atribuído a um documento quando ele é armazenado na pasta. 6. Na lista suspensa, escolha uma política de retenção. Por exemplo, escolha Ano1 para reter o documento por 1 ano. 7. Para salvar as alterações, escolha Ok.	

Tarefa	Descrição	Habilidades necessárias
Criar uma definição de relatório.	1. Conecte-se à sua EC2 instância do LRS PageCenter X. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de pastas, escolha Administrador, Importação avançada, Definição de relatório e, em seguida, escolha Adicionar. 4. Na página Manutenção da definição de relatório, na guia Geral, insira o Nome da definição de relatório. 5. Na guia Geral, em Campos, você pode especificar critérios de seleção, como Nome do trabalho, Formulário, Classe e Autor. Por exemplo, você pode inserir um Nome do trabalho de MFIDEMO. O valor do Nome do Trabalho será o nome do trabalho em lotes que gerará a saída de impressão. 6. Na guia Destino, em Destino disponível, escolha o destino criado anteriorm ente (Formulário). 7. Escolha Adicionar para adicionar o destino do	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Formulário como Destino atribuído. **Note** Este exemplo inclui uma definição de relatório em que uma saída gerada pelo MFIDEMO e roteada para o LRS PageCenter X é salva na estrutura de pastas definida na definição de destino.	

Configurar autenticação e autorização para gerenciamento de saída

Tarefa	Descrição	Habilidades necessárias
Crie um domínio AWS Managed Microsoft AD com usuários e grupos.	1. Para criar um diretório no AWS Managed Microsoft AD, siga as instruções em Crie seu diretório AWS Managed Microsoft AD. 2. Para implantar uma EC2 instância (gerencia dor do Active Directory) e instalar ferrament as do Active Directory para gerenciar seu AWS Managed Microsoft AD, siga as instruções na Etapa	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	3: Implantar uma EC2 instância para gerenciar seu AWS Managed Microsoft AD. 3. Para se conectar à sua EC2 instância, siga as instruções na EC2 documentação da Amazon. **Note** Ao se conectar à EC2 instância, na janela Segurança do Windows, insira as credenciais de administrador do diretório que você criou na etapa 1. 4. No menu Iniciar do Windows, em Ferramentas administrativas do Windows, escolha Usuários e computadores do Active Directory. 5. Para criar um usuário de impressão no domínio do Active Directory, siga as instruções em Criar um usuário.	

Tarefa	Descrição	Habilidades necessárias
Associe as EC2 instâncias a um domínio do AWS Managed Microsoft AD.	Associe as instâncias LRS VPSX/MFI e LRS PageCenter X EC2 ao seu domínio AWS Managed Microsoft AD automaticamente (documentação do AWS Knowledge Center) ou manualmente (documentação do AWS Directory Service).	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure e integre o LRS/DIS com o AWS Managed Microsoft AD para a instância do PageCenter LRS X. EC2	1. Conecte-se à sua EC2 instância do LRS PageCenter X. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de pastas, escolha Admin. 4. Na página Configuração, na seção Parâmetros de segurança, em Tipo de segurança, selecione LRS/DIS. 5. Insira suas preferências para o restante das opções na seção Parâmetros de segurança. 6. No menu Iniciar do Windows, abra a pasta PageCenterX, escolha Iniciar do servidor e escolha Parar do servidor. 7. Faça login no LRS PageCenter X com seu nome de usuário e senha do Active Directory.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure um grupo de importação para importar a saída do LRS VPSX para o LRS X. PageCenter	1. Conecte-se à sua EC2 instância do LRS PageCenter X. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de pastas, escolha Administrador, Administrador de segurança , Grupos. 4. Na seção Grupos, escolha Adicionar para abrir o formulário de Preferência de grupo. 5. No formulário Preferênc ia de grupo, insira valores para Nome do grupo e Descrição. 6. Expanda Opções gerais e marque a caixa de seleção Importar. 7. Para salvar as alterações, escolha Ok.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Adicione um regra de segurança ao grupo de importação.	1. Abra o menu de contexto (clique com o botão direito do mouse) em Importar grupo. 2. Escolha Avançado e, em seguida, Segurança. 3. Na seção Segurança , escolha Importar e marque a caixa de seleção Subpasta. 4. Para salvar as alterações, escolha Aplicar.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um usuário no LRS PageCenter X para realizar a importação de saída do LRS VPSX/MFI.	Quando você cria um usuário no LRS PageCenter X para realizar a importação de saída, o nome de usuário deve ser o mesmo que o ID VPSX da fila de saída de impressão no LRS VPSX/MFI. Neste exemplo, o ID do VPSX é. VPS1 1. Conecte-se à sua EC2 instância do LRS PageCenter X. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de pastas, escolha Administrador, Administrador de segurança , Usuário. 4. Escolha Adicionar para abrir o formulário de Manutenção do perfil do usuário. 5. Em Manutenção do perfil do usuário, em Nome do usuário, insira VPS1.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Adicione o usuário do LRS PageCenter X Import ao grupo Somente importação.	Para fornecer a permissão necessária para a importação de documentos do LRS VPSX para o LRS PageCenter X, faça o seguinte: 1. Conecte-se à sua EC2 instância do LRS PageCenter X. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de pastas, escolha Administrador, Administrador de segurança , Grupos. 4. Na seção Grupos, abra o menu de contexto (clique com o botão direito do mouse) do grupo Somente importar e escolha Avançado, Segurança. 5. Na página Registros de segurança da pasta (ImportOnly), escolha a guia Usuário. 6. Na guia Usuário, em Nome, selecione usuário na VPS1lista suspensa e escolha Aplicar.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure a LRS/DIS with AWS Managed Microsoft AD for the LRS VPSX/MFI EC2 instância.	1. Conecte-se à sua instância LRS EC2 VPSX/MFI. 2. No menu Iniciar do Windows, abra a Interface Web do VPSX. 3. No painel de navegação , escolha Segurança e depois Configurar. 4. Na página Configuração de Segurança, na seção Parâmetros de Segurança , em Tipo de segurança , selecione LRS/DIS (Externo). 5. Insira suas preferências para o restante das opções na seção Parâmetros de segurança. 6. No menu Iniciar do Windows, abra a pasta Gerenciamento de Saída do LRS, escolha Iniciar do Servidor e, em seguida, escolha Parar do Servidor. 7. Faça login no LRS VPSX/MFI com seu nome de usuário e senha do Active Directory.	Arquiteto de nuvem

Configure o Amazon FSx para Windows File Server como o armazenamento de dados operacional para o LRS X PageCenter

Tarefa	Descrição	Habilidades necessárias
Crie um sistema de arquivos para o LRS X. PageCenter	Para usar o Amazon FSx para Windows File Server como um armazenamento de dados operacional para o LRS PageCenter X em um ambiente Multi-AZ, siga as instruções na Etapa 1: Crie seu sistema de arquivos.	Arquiteto de nuvem
Mapeie o compartilhamento de arquivos para a EC2 instância do LRS PageCenter X.	Para mapear o compartil hamento de arquivos criado na etapa anterior para a EC2 instância do LRS PageCente r X, siga as instruções na Etapa 2: Mapear seu compartil hamento de arquivos para uma EC2 instância executand o o Windows Server.	Arquiteto de nuvem
Mapeie o Diretório de Controle e o Diretório de Pastas Mestras do LRS PageCenter X para a unidade de compartil hamento FSx de rede da Amazon.	1. Conecte-se à sua EC2 instância do LRS PageCenter X seguindo as instruções na EC2 documentação da Amazon. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No Explorador de Pastas, escolha Administrador, Configuração. 4. Na página Configuração, escolha Diretórios e, em	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	seguida, escolha Diretório de Controle. 5. Em Diretórios de controle, insira `\\FSx file share DNS name\share\cntl` . 6. Em Diretório de pastas mestras, insira `\\FSx file share DNS name\share\mstr` .	

Teste um fluxo de trabalho de gerenciamento de saída

Tarefa	Descrição	Habilidades necessárias
Inicie uma solicitação de impressão em lote a partir do aplicativo Rocket Software BankDemo .	1. Abra o emulador de terminal 3270 na sua instância do Rocket Enterprise Server. EC2 2. Conecte-se ao BankDemo aplicativo executando o comando `connect 127.0.0.1:9278` . 3. Na interface da linha de BankDemo comando, em ID do usuário, insira B0001. Em Senha, insira uma chave que não esteja em branco. 4. Para a opção Solicitar demonstrativo(s) impresso(s), insira X na linha em branco.	Engenheiro de testes

Tarefa	Descrição	Habilidades necessárias
	5. Na seção Enviar declaraçã o por, em Correspondência, digite Y e pressione F10.	

Tarefa	Descrição	Habilidades necessárias
Verifique a saída de impressão no LRS X. PageCenter	1. Conecte-se à sua EC2 instância do LRS PageCenter X seguindo as instruções na EC2 documentação da Amazon. 2. No menu Iniciar do Windows, abra a interface da web do PCX. 3. No painel de navegação, abra a pasta Teste, abra a pasta STD e, em seguida, abra a pasta com a data de execução do trabalho, como `08-03-2023` (MM-DD-AAAA). **Note** Essa é a mesma estrutura de pastas definida na história Crie uma regra para rotear o documento de saída para uma pasta específica no LRS PageCenter X. 4. Abra o arquivo `formtest-STD.txt` . Agora você pode ver a saída impressa de um extrato de conta com colunas para o Número da conta., Descrição, Data,	Engenheiro de testes

Tarefa	Descrição	Habilidades necessárias
	Valor e Saldo. Para ver um exemplo, consulte o anexo `batch_print_output` desse padrão.	

Recursos relacionados

- LRS
- Fluxo de dados de apresentação de funções avançadas (documentação da IBM)
- Fluxo de dados condicionado por linha (LCDS) (documentação do Compart)
- Capacitando workloads de mainframe corporativo na AWS com a Micro Focus (publicação no blog)
- Modernize suas workloads de impressão on-line de mainframe na AWS (Recomendações da AWS)
- Modernize suas workloads de impressão em lote de mainframe na AWS (Recomendações da AWS)

Mais informações

Considerações

Durante sua jornada de modernização, você pode considerar uma grande variedade de configurações para processos on-line e em lote de mainframe e a saída que eles geram. A plataforma de mainframe foi personalizada por cada cliente e fornecedor que a utiliza com requisitos específicos que afetam diretamente a impressão. Por exemplo, sua plataforma atual pode incorporar o fluxo de dados IBM AFP ou o Xerox LCDS ao fluxo de trabalho atual. Além disso, os caracteres de controle do carro do mainframe e as palavras de comando do canal podem afetar a aparência da página impressa e podem precisar de tratamento especial. Como parte do processo de planejamento da modernização, recomendamos que você avalie e compreenda as configurações em seu ambiente de impressão específico.

Captura de dados de impressão

O Rocket Software Print Exit passa as informações necessárias para que o LRS VPSX/MFI processe efetivamente o arquivo spool. As informações consistem em campos passados nos blocos de controle relevantes, como:

- JOBNAME (NOME DA FUNÇÃO)
- PROPRIETÁRIO (ID DO USUÁRIO)
- DESTINATION (DESTINO)
- FORMULÁRIO
- FILENAME (NOME DO ARQUIVO)
- WRITER (GRAVADOR)

O LRS VPSX/MFI suporta os seguintes mecanismos de lote de mainframe para capturar dados do Rocket Enterprise Server:

- print/spool processing using standard z/OS JCL SYSOUT DD/OUTPUTDeclarações BATCH COBOL.
- Instruções BATCH COBOL print/spool processing using standard z/OS JCL CA-SPOOL SUBSYS DD.
- IMS/COBOL print/spoolprocessamento usando a interface CBLTDLI. Para obter uma lista completa dos métodos suportados e exemplos de programação, consulte a documentação do LRS incluída na licença do produto.

Verificações de integridade da frota de impressoras

O LRS VPSX/MFI (LRS LoadX) pode realizar verificações de integridade detalhadas, incluindo gerenciamento de dispositivos e otimização operacional. O gerenciamento de dispositivos pode detectar falhas em um dispositivo de impressora e encaminhar a solicitação de impressão para uma impressora saudável. Para obter mais informações sobre verificações de integridade detalhadas para frotas de impressoras, consulte a documentação do LRS incluída na licença do produto.

Autorização e autenticação de impressão

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or a Lightweight Directory Access Protocol (LDAP) server. In addition to basic print authorization, LRS/DIStambém pode aplicar controles de segurança de impressão em nível granular nos seguintes casos de uso:

- Gerencie quem pode navegar pelo trabalho da impressora.
- Gerencie o nível de navegação dos trabalhos de outros usuários.

- Gerencie tarefas operacionais—por exemplo, segurança em nível de comando, como suspender ou liberar, eliminar, modificar, copiar e redirecionar. A segurança pode ser configurada pela ID do usuário ou pelo grupo, semelhante a um grupo de segurança do Active Directory ou um grupo LDAP.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Modernize o aplicativo de CardDemo mainframe usando AWS Transform

Criado por Santosh Kumar Singh (AWS) e Cheryl du Preez (AWS)

Resumo

AWS Transformfoi projetado para acelerar a modernização dos aplicativos de mainframe. Ele usa IA generativa para agilizar o processo de modernização do mainframe. Ele automatiza tarefas complexas, como: análise de código legado, documentação de mainframe, extração de regras de negócios, decomposição de aplicativos monolíticos em domínio comercial e refatoração de código. Ele acelera os projetos de modernização automatizando tarefas complexas, como análise de aplicativos e planejamento da sequência de migração. Ao decompor aplicativos monolíticos, sequencia de AWS Transform forma inteligente a transformação do aplicativo de mainframe, o que ajuda você a transformar as funções de negócios em paralelo. AWS Transform pode acelerar a tomada de decisões e aprimorar a agilidade operacional e a eficiência da migração.

Esse padrão oferece step-by-step instruções para ajudá-lo a testar os recursos de modernização do mainframe AWS Transform usando CardDemo, que é um exemplo de aplicativo de mainframe de código aberto.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- AWS IAM Identity Center, habilitado
- Permissões que permitem que os administradores habilitem AWS Transform
- Permissões que permitem aos administradores aceitar solicitações de conexão do Amazon Simple Storage Service (Amazon S3) para o aplicativo web AWS Transform

Limitações

- AWS Transform está disponível apenas em alguns Regiões da AWS. Para obter uma lista completa das regiões suportadas, consulte Regiões suportadas para AWS Transform.
- AWS Transform suporta análise de código, geração de documentos, extração de regras de negócios, decomposição e refatoração da Common Business-Oriented Language (COBOL) para Java. Para obter mais informações, consulte Capacidades e principais recursos e Tipos de arquivos compatíveis para transformação de aplicativos de mainframe.

- Há uma cota de serviço para recursos de transformação de mainframe em. AWS Transform Para mais informações, consulte Cotas para o AWS Transform.
- Para colaborar em um espaço de trabalho compartilhado, todos os usuários devem ser usuários registrados da mesma instância associada à sua instância do aplicativo AWS Transform web. AWS IAM Identity Center
- O bucket do Amazon S3 AWS Transform deve estar na mesma região Conta da AWS .

Arquitetura

O diagrama a seguir mostra a arquitetura que você configurou nesse padrão.

O diagrama mostra o seguinte fluxo de trabalho:

1. AWS Transform usa um conector para acessar o aplicativo de CardDemo mainframe, que é armazenado em um bucket do Amazon S3.
2. AWS Transform usa AWS IAM Identity Center para gerenciar o acesso e a autenticação do usuário. O sistema implementa várias camadas de controles de segurança para autenticação, autorização, criptografia e gerenciamento de acesso para ajudar a proteger códigos e artefatos durante o processamento. Os usuários interagem com o AWS Transform agente por meio de uma interface de bate-papo. Você pode fornecer instruções ao agente de IA para tarefas específicas em inglês. Para obter mais informações, consulte Human in the loop (HITL) na AWS Transform documentação.
3. O agente de IA interpreta as instruções do usuário, cria um plano de trabalho, divide o trabalho em tarefas executáveis e o executa de forma autônoma. Os usuários podem revisar e aprovar a transformação. As tarefas de transformação incluem o seguinte:
   - Análise de código — AWS Transform analisa o código em cada arquivo para obter detalhes como nome do arquivo, tipo de arquivo, linhas de código e seus caminhos. O agente analisa o código-fonte, executa classificações, cria mapeamentos de dependências e identifica quaisquer artefatos ausentes. Ele também identifica componentes duplicados.
   - Geração de documentos — AWS Transform gera documentação para o aplicativo de mainframe. Ao analisar o código, ele pode criar automaticamente uma documentação detalhada dos programas de aplicativos, incluindo descrições da lógica de negócios, fluxos, integrações e dependências presentes em seus sistemas legados.

- Extração da lógica de negócios — AWS Transform analisa os programas COBOL para documentar sua lógica de negócios principal, para ajudá-lo a entender a lógica comercial fundamental.
- Decomposição de código — AWS Transform decompõe o código em domínios que respondem pelas dependências entre programas e componentes. O agrupamento de arquivos e programas relacionados no mesmo domínio melhora a organização e ajuda a preservar a estrutura lógica do aplicativo ao dividi-lo em componentes menores.
- Planejamento da onda de migração — Com base nos domínios que você criou durante a fase de decomposição, AWS Transform gera um plano de onda de migração com a ordem de modernização recomendada.
- Refatoração de código — AWS Transform refatora o código em todos os arquivos de domínio ou em arquivos de domínio selecionados em código Java. O objetivo dessa etapa é preservar a lógica comercial crítica do aplicativo e, ao mesmo tempo, refatorá-la em um aplicativo Java modernizado e otimizado para a nuvem.

4. AWS Transform armazena o código refatorado, os documentos gerados, os artefatos associados e as bibliotecas de tempo de execução em seu bucket do Amazon S3. Você pode fazer o seguinte:
   - Acesse a pasta de tempo de execução em seu bucket do Amazon S3.
   - Crie e implante o aplicativo seguindo a seção Criar e implantar seu aplicativo modernizado após a refatoração na documentação. AWS Transform
   - Por meio da interface de bate-papo, solicite e baixe uma amostra AWS CloudFormation ou modelo do Hashicorp Terraform. AWS Cloud Development Kit (AWS CDK) Esses modelos podem ajudá-lo a implantar os AWS recursos necessários para dar suporte ao aplicativo refatorado.
   - Use o Reforge para melhorar a qualidade do código refatorado usando modelos de linguagem grandes (). LLMs O mecanismo de refatoração preserva a equivalência funcional do COBOL enquanto o transforma em código Java. O Reforge é uma etapa opcional que está disponível após a transformação. Essa etapa é usada LLMs para reestruturar o código para que se pareça muito com o Java nativo, o que pode melhorar a legibilidade e a capacidade de manutenção. O Reforge também adiciona comentários legíveis para ajudar você a entender o código e implementa padrões de codificação modernos e melhores práticas.

Ferramentas

Serviços da AWS

- AWS Transformusa IA agente para ajudá-lo a acelerar a modernização de cargas de trabalho legadas, como.NET, mainframe e cargas de trabalho. VMware
- AWS IAM Identity Centerajuda você a gerenciar centralmente o acesso de login único (SSO) aos seus Contas da AWS aplicativos e à nuvem.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Repositório de código

Você pode usar o aplicativo de AWS CardDemomainframe de código aberto como um aplicativo de exemplo para começar a modernizar o mainframe.

Práticas recomendadas

- Comece pequeno — comece com um código pequeno e menos complexo (15.000 a 20.000 linhas de código) para entender como AWS Transform analisa e transforma aplicativos de mainframe.
- Combine com a experiência humana — use AWS Transform como acelerador enquanto aplica a experiência humana para obter os melhores resultados.
- Revise e teste minuciosamente — Sempre revise cuidadosamente o código transformado e execute testes abrangentes para validar a equivalência funcional após a transformação.
- Forneça feedback — Para fornecer feedback e sugestões de melhoria, use o botão Enviar feedback no AWS Management Console ou crie um caso com AWS Support. Para obter mais informações, consulte Criar um caso de suporte. Sua opinião é valiosa para aprimoramentos de serviços e desenvolvimento futuro.

Épicos

Preparar o aplicativo de mainframe

Tarefa	Descrição	Habilidades necessárias
Crie um bucket.	Crie um bucket do Amazon S3 na mesma Conta da AWS região em que AWS Transform está habilitad	AWS geral

Tarefa	Descrição	Habilidades necessárias
	o. Você usa esse bucket para armazenar o código do aplicativo de mainframe e AWS Transform usa esse bucket para armazenar os documentos gerados, o código refatorado e outros arquivos associados à transform ação. Para obter instruçõe s, consulte Criação de um bucket na documentação do Amazon S3.	

Tarefa	Descrição	Habilidades necessárias
Prepare a amostra do aplicativo de mainframe.	1. Digite o comando a seguir para clonar o CardDemorepositório na sua estação de trabalho local: `git clone https://github.com/aws-samples/aws-mainframe-modernization-carddemo.git` 2. Crie uma nova pasta chamada`carddemo`. 3. Copie a `app` pasta, que contém o código-fonte do mainframe, do repositório clonado para a pasta. `carddemo` 4. Comprima a `cardemo` pasta em um arquivo ZIP. 5. Faça o upload do arquivo ZIP para o bucket do Amazon S3 que você criou. Para obter instruções, consulte Fazer uploads de objetos na documentação do Amazon S3.	Desenvolvedor de aplicativos, DevOps engenheiro

Configurar o IAM Identity Center e AWS Transform

Tarefa	Descrição	Habilidades necessárias
Adicione usuários ao IAM Identity Center.	Adicione seus usuários em potencial ao IAM Identity Center. Siga as instruções em Adicionar usuários no IAM Identity Center na AWS Transform documentação.	Administrador da AWS
Habilite AWS Transform e adicione usuários.	1. Habilitar AWS Transform. Siga as instruções em Ativar AWS Transform. 2. Adicionar usuários AWS Transform a. Siga as instruções em Adicionar usuários AWS Transform a.	Administrador da AWS
Configure o acesso do usuário ao aplicativo AWS Transform web.	Cada usuário deve aceitar o convite para acessar o aplicativo AWS Transform web. Siga as instruções em Aceitar o convite na AWS Transform documentação.	Desenvolvedor do aplicativo, proprietário do aplicativo
Faça login no aplicativo da AWS Transform web.	Siga as instruções em Fazer login em AWS Transform.	Desenvolvedor do aplicativo, proprietário do aplicativo
Configure um espaço de trabalho.	Configure um espaço de trabalho onde os usuários possam colaborar no aplicativo AWS Transform web. Siga as instruções em Configurando seu espaço de trabalho na AWS Transform documentação.	Administrador da AWS

Transforme o aplicativo de mainframe

Tarefa	Descrição	Habilidades necessárias
Crie um trabalho de transform ação.	Crie um trabalho de transform ação para modernizar o aplicativo de CardDemo mainframe. Para obter instruções, consulte Criar e iniciar um trabalho na AWS Transform documentação. Quando você for solicitad o a definir os objetivos na interface de AWS Transform bate-papo, escolha Executar modernização do mainframe (IBM z/OS para AWS) e, em seguida, escolha Analisar código, Gerar documentação técnica, Lógica de negócios, Decompor código, Planejar sequência de migração e Transformar código em Java.	Desenvolvedor do aplicativo, proprietário do aplicativo
Configure o conector.	Estabeleça um conector para o bucket do Amazon S3 que contém o aplicativo de CardDemo mainframe. Esse conector permite AWS Transform acessar recursos no bucket e executar funções de transformação consecuti vas. Para obter instruçõe s, consulte Configurar um conector na AWS Transform documentação.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Execute a análise do código.	1. Na página Especificar localização do ativo, insira o caminho do bucket do Amazon S3 para o arquivo `carddemo` ZIP que você carregou. 2. Escolha Aprovar e enviar para AWS Transform. Ele começa a analisar o código. 3. Monitore o status na guia Registro de trabalho. 4. Quando a análise estiver concluída, em Analisar código no painel de navegação esquerdo, escolha Exibir resultados da análise de código. 5. (Opcional) Escolha Baixar para baixar a lista completa de ativos, o código-fonte ausente e o arquivo de dependência. Para obter mais informações, consulte Análise de código na AWS Transform documenta ção.	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Gere documentação técnica.	1. No painel de navegação esquerdo, em Gerar documentação técnica, escolha Selecionar arquivos e definir configurações. 2. Expanda COBOL ou JCL e selecione um ou vários arquivos. 3. Escolha o nível de detalhes da documentação: • Resumo — Fornece uma visão geral de alto nível de cada arquivo no escopo. Além disso, fornece um resumo de uma linha de cada arquivo. • Especificação funcional detalhada — fornece detalhes abrangentes de cada arquivo no escopo de transformação do aplicativo de mainframe. Alguns detalhes incluem lógica e fluxo, regras de negócios identificadas, fluxo de dados, dependências, processamento de entrada e saída e vários detalhes da transação. 4. Escolha Enviar para AWS Transform.	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	5. Monitore o progresso na guia Registro de trabalho. **Note** O tempo de geração de documentos varia de minutos a horas, dependendo do número de arquivos e linhas de código. 6. Ao concluir, escolha Revisar resultados da documentação. 7. Acesse o documento gerado por meio do aplicativo web ou baixe-o. A documentação gerada também é armazenada no bucket do Amazon S3. 8. Explore a documentação gerada fazendo perguntas específicas na interface de bate-papo. Por exemplo, você pode dizer “Diga-me os recursos do CBACT01C” . Para obter mais informações, consulte Gerar documentação técnica na AWS Transform documentação.	

Tarefa	Descrição	Habilidades necessárias
Extraia a lógica de negócios.	1. No painel de navegação esquerdo, expanda Extrair lógica comercial e escolha Selecionar arquivos para extração da lógica comercial. 2. Expanda COBOL ou JCL e selecione um ou vários arquivos. 3. Escolha Enviar para AWS Transform. 4. Monitore o progresso na guia Registro de trabalho. **Note** O tempo de extração da lógica de negócios varia de minutos a horas, dependendo do número de arquivos e linhas de código. 5. Quando a extração estiver concluída, escolha Revisar os resultados da extração da lógica comercial. 6. Selecione um arquivo COBOL ou JCL e escolha Exibir. 7. Altere o escopo no diagrama de fluxo e nas regras funcionais para	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	revisar os diferentes níveis dos fluxogramas, incluindo o código de suporte. 8. (Opcional) Analise a lógica de negócios gerada, que é armazenada no formato JSON em seu bucket do Amazon S3. Para obter mais informaçõ es, consulte Extrair lógica de negócios na AWS Transform documentação.	

Tarefa	Descrição	Habilidades necessárias
Decomponha o código.	1. No painel de navegação esquerdo, expanda Decompor código e escolha Decompor em domínios. 2. Na lista Ações, escolha Criar domínio. 3. Insira um nome para o novo domínio, como `Bill payment`. 4. (Opcional) Forneça uma descrição. 5. Na barra de pesquisa Localizar arquivos `CB00`, pesquise e selecione o arquivo. 6. Escolha Marcar como semente. 7. Verifique se o sinalizador inicial muda de Não para Sim. 8. Escolha Criar. 9. Escolha Salvar. 10. Escolha Decompor. 11. Revise a saída da decomposição escolhendo o nome do domínio. 12. Quando a decomposição estiver concluída, escolha Enviar para AWS Transform.	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es sobre decomposição e sementes, consulte Decomposição na AWS Transform documentação.	
Planeje as ondas de migração.	Planeje as ondas de migração para o CardDemo aplicativ o. Siga as instruções em Planejamento de ondas de migração na AWS Transform documentação para revisar e editar o plano de ondas.	Desenvolvedor do aplicativo, proprietário do aplicativo
Refatore o código.	1. Refatore o aplicativo de CardDemo mainframe em código Java em todos os arquivos de domínio ou em arquivos de domínio selecionados. Siga as instruções no código Refactor na AWS Transform documentação. 2. Depois que o processo de refatoração estiver concluído, crie e implante o aplicativo Java moderniza do. Siga as instruções em Crie e implante seu aplicativ o modernizado após a refatoração na documenta ção. AWS Transform	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
(Opcional) Use o Reforge para melhorar o código Java.	1. Crie um novo trabalho e, em seguida, insira um objetivo de`Reforge the code`. 2. Insira o de um projeto que foi modernizado por meio AWS Transform de. Esse projeto deve estar em seu bucket do Amazon S3. 3. Insira a lista de classes Java que especifica quais classes de serviço devem ser reforjadas. 4. Analise a saída gerada no bucket do Amazon S3. Para obter mais informaçõ es, consulte Reforge na AWS Transform documentação.	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Simplifique a implantação.	AWS Transform pode fornecer modelos de infraestrutura como código (IaC) para CloudFormation AWS CDK, ou Terraform. Esses modelos ajudam você a implantar componentes principai s, incluindo recursos de computação, banco de dados, armazenamento e segurança. 1. Na interface de AWS Transform bate-papo , solicite os modelos inserindo`Share the mainframe refactor <service> templates` , onde `<service>` está um dos serviços IaC suportado s. 2. Implante o modelo usando seu serviço preferido. Por exemplo, consulte os seguintes recursos: • Crie uma pilha a partir do CloudFormation console (CloudFormation documentação) • Implantar AWS CDK aplicativos (AWS CDK documentação) • Construir infraestrutura (documentação do Terraform)	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es, consulte Recursos de implantação na AWS Transform documentação.	

Solução de problemas

Problema	Solução
Você não consegue visualizar o código-fonte ou o documento gerado no aplicativo AWS Transform web.	Adicione uma política à permissão do CORS para que o bucket do Amazon S3 AWS Transform permita como origem. Para obter mais informações, consulte as permissõe s CORS do bucket S3 na AWS Transform documentação.

Recursos relacionados

AWS documentação

- Transformação de aplicativos de mainframe (AWS Transform documentação)

Outros AWS recursos

- Acelere sua jornada de modernização do mainframe usando agentes de IA com AWS Transform (AWS postagem no blog)
- AWS Transform FAQs
- AWS IAM Identity Center FAQs

Vídeos e tutoriais

- Introdução ao Amazon Q Developer: Transform (AWS Skill Builder)

- AWS re:Invent 2024 — Modernize aplicativos de mainframe com mais rapidez usando o Amazon Q Developer () YouTube
- AWS re:Invent 2024 - Automatizando a migração e a modernização para acelerar a transformação () YouTube
- AWS re:Invent 2024 - A Toyota impulsiona a inovação e melhora a eficiência operacional com a geração AI () YouTube

> **Note**
>
> AWS Transform era conhecido anteriormente como Amazon Q Developer transform for mainframe.

Modernize as cargas de trabalho de impressão em lote do mainframe AWS usando o Rocket Enterprise Server e o LRS VPSX/MFI

Criado por Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) e Kevin Yung (AWS)

Resumo

Esse padrão mostra como modernizar suas cargas de trabalho de impressão em lote de mainframe essenciais para os negócios na nuvem da Amazon Web Services (AWS) usando o Rocket Enterprise Server como um tempo de execução para um aplicativo de mainframe modernizado e o LRS VPSX/MFI (Micro Focus Interface) como servidor de impressão. O padrão é baseado na abordagem de modernização do mainframe de redefinir a plataforma. Nessa abordagem, você migra seus trabalhos em lote de mainframe para o Amazon Elastic Compute Cloud (Amazon EC2) e migra seu banco de dados de mainframe, como o IBM for z/OS, DB2 para o Amazon Relational Database Service (Amazon RDS). A autenticação e autorização para o fluxo de trabalho de impressão modernizado são realizadas pelo AWS Directory Service for Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD. O LRS Directory Information Server (LRS/DIS) é integrado ao AWS Managed Microsoft AD. Ao modernizar suas cargas de trabalho de impressão em lote, você pode reduzir os custos de infraestrutura de TI, mitigar a dívida técnica de manter sistemas legados, remover silos de dados, aumentar a agilidade e a eficiência com um DevOps modelo e aproveitar os recursos sob demanda e a automação na nuvem da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma workload de gerenciamento de impressão ou saída de mainframe
- Conhecimento básico de como reconstruir e entregar um aplicativo de mainframe executado no Rocket Enterprise Server (para obter mais informações, consulte a planilha de dados do Rocket Enterprise Server na documentação do Rocket.)
- Conhecimento básico das soluções e conceitos de impressão em nuvem da LRS
- Software e licença do Rocket Enterprise Server (para obter mais informações, entre em contato com o departamento de vendas da Rocket.)
- VPSX/MFI, LRS/Queue, and LRS/DISSoftware e licenças do LRS (para obter mais informações, entre em contato com a equipe de vendas do LRS.)

> **Note**
>
> Para obter mais informações sobre considerações de configuração para cargas de trabalho de impressão em lote de mainframe, consulte Considerações na seção Informações adicionais desse padrão.

Versões do produto

- Rocket Enterprise Server 6.0 (atualização do produto 7)
- LRS VPSX/MFI V1R3 ou superior

Arquitetura

Pilha de tecnologia de origem

- Sistema operacional: IBM z/OS
- Linguagem de programação — Common Business-Oriented Language (COBOL), linguagem de controle de tarefas (JCL) e Customer Information Control System (CICS)
- Banco de dados — IBM DB2 for z/OS e Virtual Storage Access Method (VSAM)
- Segurança — Resource Access Control Facility (RACF), CA Top Secret for z/OS e Access Control Facility 2 () ACF2
- Gerenciamento de impressão e saída: produtos de impressão z/OS de mainframe IBM (IBM Tivoli Output Manager for z/OS, LRS e CA View)

Pilha de tecnologias de destino

- Sistema operacional — Microsoft Windows Server em execução na Amazon EC2
- Computação — Amazon EC2
- Linguagem de programação: COBOL, JCL e CICS
- Banco de dados: Amazon RDS
- Segurança: AWS Managed Microsoft AD
- Gerenciamento de impressão e produção: solução de impressão LRS na AWS
- Ambiente de execução do mainframe — Rocket Enterprise Server

Arquitetura de origem

O diagrama a seguir mostra uma arquitetura típica do estado atual para uma workload de impressão em lote de mainframe:

O diagrama mostra o seguinte fluxo de trabalho:

1. Os usuários realizam transações comerciais em um sistema de engajamento (SoE) construído em um aplicativo IBM CICS escrito em COBOL.
2. O SoE invoca o serviço de mainframe, que registra os dados da transação comercial em um banco de dados system-of-records (SoR), como o IBM for z/OS. DB2
3. O SoR persiste os dados comerciais do SoE.
4. O agendador de trabalhos em lotes inicia um trabalho em lotes para gerar a saída de impressão.
5. O trabalho em lotes extrai dados do banco de dados, formata os dados de acordo com os requisitos comerciais e, em seguida, gera resultados comerciais, como extratos de cobrança, cartões de identificação ou extratos de empréstimos. Por fim, o trabalho em lotes direciona a saída para o gerenciamento da saída de impressão para processamento e entrega da saída, com base nos requisitos comerciais.
6. O gerenciamento da saída de impressão recebe a saída de impressão do trabalho em lote e, em seguida, entrega essa saída para um destino específico, como e-mail, um compartilhamento de arquivos que usa FTP seguro, uma impressora física que usa soluções de impressão LRS (conforme demonstrado nesse padrão) ou IBM Tivoli.

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para uma workload de impressão em lote de mainframe que é implantada na nuvem AWS:

O diagrama mostra o seguinte fluxo de trabalho:

1. O programador de trabalhos em lotes inicia um trabalho em lotes para criar resultados de impressão, como extratos de cobrança, cartões de identificação ou extratos de empréstimos.
2. O trabalho em lote do mainframe (reformatado para a Amazon EC2) usa o tempo de execução do Rocket Enterprise Server para extrair dados do banco de dados do aplicativo, aplicar lógica

comercial aos dados, formatar os dados e, em seguida, enviar os dados para um destino de impressão usando o Rocket Software Print Exit (documentação da Micro Focus).

3. O banco de dados do aplicativo (um SoR executado no Amazon RDS) persiste os dados para a saída de impressão.
4. O agente de VPSX/MFI printing solution is deployed on Amazon EC2 and its operational data is stored in Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI uses the TCP/IP-based LRS/Queue transmissão do LRS coleta dados de impressão por meio da API JES Print Exit da Rocket Software e entrega os dados a um destino de impressora especificado.

> **Note**
>
> A solução de destino normalmente não exige alterações no aplicativo para acomodar linguagens de formatação de mainframe, como IBM Advanced Function Presentation (AFP) ou Xerox Line Condition Data Stream (LCDS). Para obter mais informações sobre o uso da Rocket Software para migração e modernização de aplicativos de mainframe na AWS, consulte a postagem do blog Empowering Enterprise Mainframe Workloads on AWS with Micro Focus.

Arquitetura de infraestrutura da AWS

O diagrama a seguir mostra uma arquitetura de infraestrutura da AWS altamente disponível e segura para uma workload de impressão em lote de mainframe:

O diagrama mostra o seguinte fluxo de trabalho:

1. O agendador de lotes inicia o processo em lote e é implantado na Amazon EC2 em várias zonas de disponibilidade para alta disponibilidade (HA).

   > **Note**
   >
   > Esse padrão não abrange a implementação do agendador de lotes. Para obter mais informações sobre implementação, consulte a documentação do fornecedor de software para o agendador.

2. O trabalho em lote do mainframe (escrito em uma linguagem de programação como JCL ou COBOL) usa a lógica comercial principal para processar e gerar resultados impressos, como

extratos de cobrança, cartões de identificação e extratos de empréstimos. O trabalho é implantado na Amazon em duas EC2 zonas de disponibilidade para HA e usa o Rocket Software Print Exit para rotear a saída de impressão para o LRS VPSX/MFI para impressão do usuário final.

3. VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect or capture print data from the Rocket Software JES Print Exit programming interface. Print Exit passes the necessary information to enable LRS VPSX/MFI to effectively process the spool file and dynamically build LRS/QueueComandos do LRS. Os comandos são então executados usando uma função embutida padrão da Rocket Software.

> **Note**
>
> Para obter mais informações sobre dados de impressão passados do Rocket Software Print Exit para mecanismos de lote de mainframe LRS/Queue and LRS VPSX/MFI suportados, consulte Captura de dados de impressão na seção Informações adicionais desse padrão.

4.
> **Note**
>
> Um Network Load Balancer fornece um nome DNS para integrar o Rocket Enterprise Server ao LRS VPSX/MFI. : LRS VPSX/MFI supports a Layer 4 load balancer. The Network Load Balancer also does a basic health check on LRS VPSX/MFI e roteia o tráfego para os alvos registrados que estão íntegros.

5.
> **Note**
>
> O servidor de impressão LRS VPSX/MFI é implantado na Amazon em duas EC2 zonas de disponibilidade para HA e usa o Amazon EBS como um armazenamento de dados operacional. O LRS também VPSX/MFI supports both the active-active and active-passive service modes. This architecture uses multiple AZs in an active-passive pair as an active and hot standby. The Network Load Balancer performs a health check on LRS VPSX/MFI EC2 instances and routes traffic to hot standby instances in the other AZ if an active instance is in an unhealthy state. The print requests are persisted in the LRS Job Queue locally in each of the EC2 instances. In the event of recovery, a failed instance has to be restarted for the LRS services to resume processing the print request. : LRS VPSX/MFI pode realizar verificações de saúde no nível da frota de impressoras. Para obter

mais informações, consulte Verificações de integridade da frota de impressoras na seção Informações adicionais desse padrão.

6. O AWS Managed Microsoft AD se integra ao LRS/DIS para realizar a autenticação e autorização do fluxo de trabalho de impressão. Para obter mais informações, consulte Autenticação e autorização de impressão na seção Informações adicionais desse padrão.
7. O LRS VPSX/MFI usa o Amazon EBS para armazenamento em bloco. Você pode fazer backup de dados do Amazon EBS de EC2 instâncias ativas para o Amazon S3 point-in-time como snapshots e restaurá-los em volumes do EBS em espera ativa. Para automatizar a criação, retenção e exclusão de snapshots de volume do Amazon EBS, você pode usar o Amazon Data Lifecycle Manager para definir a frequência dos snapshots automatizados e restaurá-los com base em seus requisitos de RTO/RPO.

Ferramentas

Serviços da AWS

- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias. EC2 Os volumes do EBS se comportam como dispositivos de bloco brutos e não formatados. É possível montar esses volumes como dispositivos em suas instâncias.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você pode usar EC2 a Amazon para lançar quantos servidores virtuais precisar e pode expandir ou aumentar a escala.
- O Amazon Relational Database Service (Amazon RDS) é um serviço web que facilita a configuração, a operação e a escalabilidade de um banco de dados relacional na nuvem da AWS. Ele fornece capacidade econômica e redimensionável para um banco de dados relacional e gerencia tarefas comuns de administração de banco de dados.
- O AWS Directory Service for Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD, permite que suas cargas de trabalho e recursos da AWS com reconhecimento de diretório usem o Microsoft Active Directory na nuvem da AWS.

Outras ferramentas

- O LRS VPSX/MFI (Micro Focus Interface), desenvolvido em conjunto pela LRS e pela Rocket Software, captura a saída de um spool JES do Rocket Enterprise Server e a entrega de forma confiável a um destino de impressão especificado.

- O LRS Directory Information Server (LRS/DIS) é usado para autenticação e autorização durante o fluxo de trabalho de impressão.
- TCP/IP-based LRS/Queue transmission agent is used by LRS VPSX/MFIpara coletar ou capturar dados de impressão por meio da interface de programação JES Print Exit da Rocket Software.
- O Rocket Enterprise Server é um ambiente de implantação de aplicativos para aplicativos de mainframe. Ele fornece o ambiente de execução para aplicativos de mainframe que são migrados ou criados usando qualquer versão do Rocket Software Enterprise Developer.

Épicos

Configure o Rocket Enterprise Server na Amazon EC2 e implante um aplicativo em lote de mainframe

Tarefa	Descrição	Habilidades necessárias
Configure o Rocket Enterprise Server e implante um aplicativo de demonstração.	Configure o Rocket Enterprise Server na Amazon e EC2, em seguida, implante o aplicativo de BankDemo demonstração do Rocket Software na Amazon. EC2 O BankDemo aplicativo é um aplicativo em lote de mainframe que cria e, em seguida, inicia a saída de impressão.	Arquiteto de nuvem

Configurar um servidor de impressão LRS na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Obtenha uma licença de produto LRS para impressão.	Para obter uma licença de produto LRS para o LRSVPSX/MFI, LRS/Queue, and LRS/DIS, entre em	Crie um lead

Tarefa	Descrição	Habilidades necessárias
	contato com a equipe de gerenciamento de saída do LRS. Você deve fornecer os nomes de host das EC2 instâncias em que os produtos LRS serão instalados.	

Tarefa	Descrição	Habilidades necessárias
Crie uma instância EC2 do Amazon Windows para instalar o LRS VPSX/MFI.	Execute uma instância EC2 do Amazon Windows seguindo as instruções em Iniciar uma EC2 instância da Amazon na EC2 documentação da Amazon. Sua instância deve atender aos seguintes requisitos de hardware e software para LRS VPSX/MFI: • CPU: Dual Core • MEMÓRIA RAM: 16 GB • Unidade: 500 GB • EC2 Instância mínima — m5.xlarge • SISTEMA OPERACIONAL: Windows/Linux • Software: Internet Information Service (IIS) ou Apache **Note** Os requisitos anteriores de hardware e software são destinados a uma pequena frota de impressoras (cerca de 500 a 1000). Para obter todos os requisitos, consulte seus contatos do LRS e da AWS.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Ao criar sua instância do Windows, faça o seguinte: 1. Confirme se o nome do EC2 host é o mesmo usado para a licença do produto LRS. 2. Ative o CGI na Amazon EC2 preenchendo o seguinte: a. Conecte-se à sua EC2 instância seguindo as instruções de	

Tarefa	Descrição	Habilidades necessárias
Instale o LRS VPSX/MFI na instância. EC2	1. Conecte-se à sua EC2 instância seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 2. **Note** Abra o link para a página de download do produto no e-mail do LRS que você deve receber. : Os produtos LRS são distribuídos por transferência eletrônica de arquivos (TEF). 3. Baixe o LRS VPSX/MFI e descompacte o arquivo (pasta padrão: `c:\LRS`). 4. Inicie o LRS Product Installer a partir da pasta descompactada para instalar o LRS VPSX/MFI. 5. No menu Seleciona r recursos, selecione Servidor VPSX® (V1R3.022) e escolha Avançar para iniciar o processo de instalação. Você receberá uma mensagem de sucesso	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	quando a instalação for concluída.	
Instale o LRS/Queue.	1. Conecte-se à sua EC2 instância do Rocket Enterprise Server seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 2. Abra o link para a página de download do produto LRS a partir do e-mail do LRS que você deve receber, baixe o LRS/Queue e, em seguida, descompacte o arquivo. 3. Vá até o local onde você baixou os arquivos e, em seguida, inicie o instalador do produto LRS para instalar o LRS/Queue.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Instale o LRS/DIS.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. Abra o link para a página de download do produto LRS a partir do e-mail do LRS que você deve receber, baixe o LRS/DIS e, em seguida, descompacte o arquivo. 3. Vá para o local em que você fez o download dos arquivos e inicie o LRS Product Installer. 4. No LRS Product Installer, expanda LRS Misc Tools, selecione LRS DIS e escolha Avançar. 5. Siga o restante das instruções no instalador do produto LRS para concluir o processo de instalação.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um grupo-alvo e registre o LRS EC2 VPSX/MFI como alvo.	Crie um grupo de destino seguindo as instruções de Criar um grupo de destino para seu Network Load Balancer na documentação do Elastic Load Balancing. Ao criar o grupo de destino, faça o seguinte: 1. Na página Especificar detalhes do grupo, em Escolher um Tipo de destino, escolha Instâncias. 2. Para Protocol, escolha TCP. 3. Em Porta, escolha 5500. 4. Na página Registrar destinos, na seção Instâncias disponíveis, selecione as instâncias LRS EC2 VPSX/MFI.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar um Network Load Balancer.	Siga as instruções de Criar um Network Load Balancer na documentação do Elastic Load Balancing. Seu Network Load Balancer roteia o tráfego do Rocket Enterprise Server para o LRS VPSX/MFI. EC2 Ao criar o Network Load Balancer, faça o seguinte na página Receptores e roteamento: 1. Para Protocolo, escolha TCP. 2. Em Porta, escolha 5500. 3. Em Ação padrão, escolha Encaminhar para o grupo de destino que você criou anteriormente.	Arquiteto de nuvem

Integre o Rocket Enterprise Server com o LRS VPSX/MFI and LRS/Queue

Tarefa	Descrição	Habilidades necessárias
Configure o Rocket Enterprise Server para integração LRS/Queue.	1. Conecte-se à sua EC2 instância do Rocket Enterprise Server seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 2. No menu Iniciar do Windows, abra a interface	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	de administração do Rocket Enterprise Server. 3. Na barra de menu, escolha NATIVO. 4. No painel de navegação , escolha Servidor do diretório e BANKDEMO. 5. Em Geral, no painel de navegação esquerdo, role para baixo até a seção Adicional para configurar as variáveis de ambiente (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) para apontar para LRSQ. 6. Para LRSQ_ADDRESS, insira o endereço IP ou o nome DNS do Network Load Balancer que você criou anteriormente. 7. Para LRSQ_PORT, insira VPSX LRSQ Listener Port (5500). 8. Para LRSQ_COMMAND, insira a localização do caminho do executável do LRSQ. **Note** Atualmente, o LRS suporta um limite	

Tarefa	Descrição	Habilidades necessárias
	máximo de 50 caracteres para nomes DNS, mas isso está sujeito a alterações no futuro. Se seu nome DNS for maior que 50, você poderá usar o endereço IP do Network Load Balancer como alternativa.	

Tarefa	Descrição	Habilidades necessárias
Configure o Rocket Enterprise Server para integração LRS VPSX/MFI.	1. Copie a `VPSX_MFI_R2` pasta do instalador LRS VPSX/MFI para o local do Rocket Enterprise Server em. `C\BANKDEMO\print` 2. Conecte-se à sua EC2 instância do Rocket Enterprise Server seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 3. No menu Iniciar do Windows, abra a interface de administração do Rocket Enterprise Server. 4. Na barra de menu, escolha NATIVO. 5. No painel de navegação , escolha Servidor do diretório e BANKDEMO. 6. Em BANKDEMO, escolha JES. 7. Em JES Program Path, adicione o caminho `DLL(VPSX_MFI_R2)` do local `C\BANKDEMO\print`.	Arquiteto de nuvem

Configure impressoras e usuários de impressão no Rocket Enterprise Server e no LRS VPSX/MFI

Tarefa	Descrição	Habilidades necessárias
Associe o módulo de saída de impressão do software Rocket ao processo de execução do servidor da impressora em lote Rocket Enterprise Server.	1. Conecte-se à sua EC2 instância do Rocket Enterprise Server seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 2. No menu Iniciar do Windows, abra a interface de administração do Rocket Enterprise Server. 3. Na barra de menu, escolha NATIVO. 4. No painel de navegação , escolha Servidor do diretório e BANKDEMO. 5. Em BANKDEMO, escolha JES e role para baixo até Impressoras. 6. Em Impressoras, associe o módulo de saída de impressão da Rocket Software (para LRSPRTE6 lote) ao processo de execução do servidor (SEP) da impressora em lote Rocket Enterprise Server. Isso permite o roteamento da saída de impressão para LRS VPSX/MFI.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	7. Faça login na IU do Enterprise Server Administration. Para obter mais informações sobre configuração, consulte Usando a saída na documentação da Micro Focus.	

Tarefa	Descrição	Habilidades necessárias
Adicione uma impressora no LRS VPSX/MFI.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. Abra a interface da web do VPSX no menu Iniciar do Windows. 3. No painel de navegação, escolha Impressoras. 4. Escolha Adicionar e Adicionar impressora. 5. Na página Configuração da impressora, em Nome da impressora, insira Local. 6. Para ID VPSX, insira. VPS1 7. Para CommType, selecione TCPIP/LRSQ. 8. Em Host/Endereço IP, insira o endereço IP da impressora física que você deseja adicionar. 9. Em Dispositivo, insira o nome do seu dispositivo. 10. Escolha Driver do Windows ou Driver Linux/Mac. 11. Escolha Adicionar.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um usuário de impressão no LRS VPSX/MFI.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. Abra a interface da web do VPSX no menu Iniciar do Windows. 3. No painel de navegação , escolha Segurança e depois Usuários. 4. Na coluna Nome de usuário, escolha admin e, em seguida, escolha Copiar. 5. Na janela Manutenção do perfil do usuário, em Nome do usuário, insira um nome de usuário (por exemplo, PrintUser). 6. Em Descrição, insira uma breve descrição (por exemplo, Usuário para impressão de teste). 7. Selecione Atualizar. Isso cria um usuário de impressão (por exemplo, PrintUser). 8. No painel de navegação, em Usuário, escolha o novo usuário que você criou.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	9. No menu Comando, escolha Segurança. 10. Na página Regras de segurança, escolha todas as opções aplicáveis de segurança da impressora e segurança do trabalho e, em seguida, escolha Salvar. 11. Para adicionar seu novo usuário de impressão ao grupo Administrador, acesse o painel de navegação, escolha Segurança e, em seguida, escolha Configurar. 12. Na janela Configuração de segurança, adicione seu novo usuário de impressão à coluna Administrador.	

Configurar autorização e autenticação de impressão

Tarefa	Descrição	Habilidades necessárias
Crie um domínio AWS Managed Microsoft AD com usuários e grupos.	1. Crie um Active Directory no AWS Managed Microsoft AD seguindo as instruções de Criar seu diretório AWS Managed Microsoft AD na documentação do AWS Directory Service.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	2. Implante uma EC2 instância (gerenciador do Active Directory) e instale as ferramentas do Active Directory para gerenciar seu AWS Managed Microsoft AD seguindo as instruções da Etapa 3: Implantar uma EC2 instância para gerenciar seu AWS Managed Microsoft AD na documentação do AWS Directory Service. 3. **Note** Conecte-se à sua EC2 instância seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. : ao se conectar à EC2 instância, insira suas credenciais de administrador (para o diretório que você criou na etapa um) na janela Segurança do Windows.	

Tarefa	Descrição	Habilidades necessárias
	4. No menu Iniciar do Windows, em Ferrament as administrativas do Windows, escolha Usuários e computadores do Active Directory. 5. Crie um usuário de impressão no domínio do Active Directory seguindo as etapas em Criar um usuário na documentação do AWS Directory Service.	
Associe o LRS VPSX/MFI a EC2 um domínio Microsoft AD gerenciado pela AWS.	Associe o LRS VPSX/MFI ao EC2 seu domínio AWS Managed Microsoft AD automaticamente (document ação do AWS Knowledge Center) ou manualmente (documentação do AWS Directory Service).	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure e integre o LRS/DIS com AWS Managed Microsoft AD.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. No menuIniciar do Windows, abra a interface da web do VPSX. 3. No painel de navegação , escolha Segurança e depois Configurar. 4. Na página Configuração de Segurança, na seção Parâmetros de Segurança , em Tipo de Segurança, selecione Interno. 5. Insira suas preferências para o restante das opções na seção Parâmetros de segurança. 6. Abra a pasta LRS Output Management no menu Iniciar do Microsoft Windows, escolha Iniciar do Servidor e, em seguida, escolha Parar do Servidor. 7. Faça login no LRS VPSX/ MFI com seu nome de usuário e senha do Active Directory.	Arquiteto de nuvem

Teste um fluxo de trabalho de impressão

Tarefa	Descrição	Habilidades necessárias
Inicie uma solicitação de impressão em lote a partir do aplicativo Rocket Software BankDemo .	1. Abra o emulador de terminal 3270 em sua instância do Rocket Enterprise Server. EC2 2. Conecte-se ao BankDemo aplicativo executando o seguinte comando: `connect 127.0.0.1 :9278` 3. Na interface da linha de BankDemo comando, em ID do usuário, insira B0001. Em Senha, insira uma chave que não esteja em branco. 4. Para a opção Solicitar demonstrativo(s) impresso(s), insira X na linha em branco. 5. Na seção Enviar declaraçã o por, em Correspondência, digite Y e pressione F10.	Engenheiro de testes
Verifique a saída de impressão no LRS VPSX/MFI.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. No menu Iniciar do Windows, abra a interface da web do VPSX.	Engenheiro de testes

Tarefa	Descrição	Habilidades necessárias
	3. No painel de navegação, selecione Impressoras e, em seguida, selecione Fila de saída. 4. Na coluna ID do spool, escolha a ID do spool para a solicitação na fila da impressora. 5. Na guia Ações, na coluna COMANDO, escolha Procurar. Agora você pode ver a saída impressa de um extrato de conta com colunas para o Número da conta., Descrição , Data, Valor e Saldo. Para ver um exemplo, consulte o anexo batch_print_output desse padrão.	

Recursos relacionados

- Modernização da saída do LRS (documentação do LRS)
- ANSI e controles de transporte de máquinas (documentação da IBM)
- Palavras de comando do canal (documentação da IBM)
- Capacitando workloads de mainframe corporativo na AWS com a Micro Focus (blog da rede de parceiros da AWS)
- Crie um PAC do Micro Focus Enterprise Server com o Amazon EC2 Auto Scaling e o Systems Manager (documentação do AWS Prescriptive Guidance)
- Fluxo de dados de apresentação de funções avançadas (AFP) (documentação da IBM)
- Fluxo de dados condicionado por linha (LCDS) (documentação do Compart)

Mais informações

Considerações

Durante sua jornada de modernização, você pode considerar uma grande variedade de configurações tanto para os processos em lote do mainframe quanto para a saída que eles geram. A plataforma de mainframe foi personalizada por cada cliente e fornecedor que a utiliza com requisitos específicos que afetam diretamente a impressão. Por exemplo, sua plataforma atual pode incorporar o IBM Advanced Function Presentation (AFP) ou o Xerox Line Condition Data Stream (LCDS) ao fluxo de trabalho atual. Além disso, os caracteres de controle do carro do mainframe e as palavras de comando do canal podem afetar a aparência da página impressa e podem precisar de tratamento especial. Como parte do processo de planejamento da modernização, recomendamos que você avalie e compreenda as configurações em seu ambiente de impressão específico.

Captura de dados de impressão

O Rocket Software Print Exit passa as informações necessárias para permitir que o LRS VPSX/MFI processe com eficácia o arquivo spool. As informações consistem em campos passados nos blocos de controle relevantes, como:

- JOBNAME (NOME DA FUNÇÃO)
- PROPRIETÁRIO (ID DO USUÁRIO)
- DESTINATION (DESTINO)
- FORMULÁRIO
- FILENAME (NOME DO ARQUIVO)
- WRITER (GRAVADOR)

O LRS VPSX/MFI suporta os seguintes mecanismos de lote de mainframe para capturar dados do Rocket Enterprise Server.

- Declarações BATCH COBOL print/spool processing using standard z/OS JCL SYSOUT DD/ OUTPUT
- Instruções BATCH COBOL print/spool processing using standard z/OS JCL CA-SPOOL SUBSYS DD
- IMS/COBOL print/spoolprocessamento usando a interface CBLTDLI (para obter uma lista completa dos métodos suportados e exemplos de programação, consulte a documentação do LRS incluída na licença do produto.)

Verificações de integridade da frota de impressoras

O LRS VPSX/MFI (LRS LoadX) pode realizar verificações de integridade detalhadas, incluindo gerenciamento de dispositivos e otimização operacional. O gerenciamento de dispositivos pode detectar falhas em um dispositivo de impressora e encaminhar a solicitação de impressão para uma impressora saudável. Para obter mais informações sobre verificações de integridade detalhadas para frotas de impressoras, consulte a documentação do LRS que está incluída na sua licença de produto.

Autorização e autenticação de impressão

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or an LDAP server. In addition to basic print authorization, LRS/DIStambém pode aplicar controles de segurança de impressão em nível granular nos seguintes casos de uso:

- Gerencie quem pode navegar pelo trabalho da impressora.
- Gerencie o nível de navegação dos trabalhos de outros usuários.
- Gerencie tarefas operacionais. Por exemplo, segurança em nível de comando, como suspender/liberar, limpar, modificar, copiar e redirecionar. A segurança pode ser configurada pelo ID do usuário ou pelo grupo (semelhante ao grupo AD ou grupo LDAP).

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Modernização do mainframe: DevOps iniciada AWS com o Rocket Software Enterprise Suite

Criado por Kevin Yung (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Desafios do cliente

Organizações que executam aplicativos principais em hardware de mainframe geralmente enfrentam alguns desafios quando o hardware precisa ser expandido para atender às demandas das inovações digitais. Esses desafios incluem as seguintes restrições.

- Os ambientes de desenvolvimento e teste de mainframe não conseguem escalar devido à inflexibilidade dos componentes de hardware do mainframe e ao alto custo da mudança.
- O desenvolvimento de mainframe está enfrentando escassez de habilidades, porque os novos desenvolvedores não estão familiarizados e não estão interessados nas ferramentas tradicionais de desenvolvimento de mainframe. Tecnologias modernas, como contêineres, pipelines integration/continuous delivery (CI/CD (contínuos) e estruturas de teste modernas não estão disponíveis no desenvolvimento de mainframe.

Resultados do padrão

Para enfrentar esses desafios, a Amazon Web Services (AWS) e a Rocket Software Micro Focus, uma parceira AWS Partner Network (APN), colaboraram para criar esse padrão. A solução foi projetada para ajudar você a alcançar os seguintes resultados.

- Produtividade aprimorada do desenvolvedor Os desenvolvedores podem receber novas instâncias de desenvolvimento de mainframe em minutos.
- Uso do Nuvem AWS para criar novos ambientes de teste de mainframe com capacidade praticamente ilimitada.
- Provisionamento rápido da nova infraestrutura de CI/CD de mainframe. O provisionamento AWS pode ser concluído em uma hora usando e. AWS CloudFormation AWS Systems Manager

- Uso nativo de AWS DevOps ferramentas para desenvolvimento de mainframe, incluindo, AWS CodeBuild, AWS CodeCommit AWS CodePipeline AWS CodeDeploy, e Amazon Elastic Container Registry (Amazon ECR).
- Transforme o desenvolvimento tradicional em cascata em desenvolvimento ágil em projetos de mainframe.

Resumo das tecnologias

Nesse padrão, a pilha de destino contém os seguintes componentes.

Componentes lógicos	Soluções de implementação	Descrição
Repositórios de código-fonte	AccuRev Servidor Rocket Software CodeCommit, Amazon ECR	Gerenciamento de código-fonte — A solução usa dois tipos de código-fonte: • Código-fonte do mainframe, por exemplo, COBOL e JCL. • AWS modelos de infraestrutura e scripts de automação Ambos os tipos de código-fonte precisam de controle de versão, mas são gerenciados de forma diferente SCMs. O código-fonte implantado no mainframe ou nos servidores corporativos da Rocket Software é gerenciado no Rocket Software Micro Focus Server. AccuRev AWS modelos e scripts de automação são gerenciados em CodeCommit. O Amazon

		ECR é usado para os repositór ios de imagem do Docker.
Instâncias de desenvolvedores corporativos	Amazon Elastic Compute Cloud (Amazon EC2), desenvolvedor corporativo da Rocket Software para Eclipse	Os desenvolvedores de mainframe podem desenvolv er código na Amazon EC2 usando o Rocket Software Enterprise Developer for Eclipse. Isso elimina a necessidade de depender do hardware do mainframe para escrever e testar o código.
Gerenciamento de licenças do Rocket Software Enterprise Suite	License Manager do Rocket Software Enterprise Suite	Para gerenciamento e governança centralizados de licenças do Rocket Software Enterprise Suite, a solução usa o Rocket Software Enterprise Suite License Manager para hospedar a licença necessária.
Pipelines de CI/CD	CodePipeline,, CodeBuild CodeDeploy, Rocket Software Enterprise Developer em um contêiner, Rocket Software Enterprise Test Server em um contêiner, Rocket Software Micro Focus Enterprise Server	As equipes de desenvolv imento de mainframe precisam de pipelines de CI/CD para realizar compilação de código, testes de integração e testes de regressão. Em AWS, CodePipeline e CodeBuild pode trabalhar com o Rocket Software Enterprise Developer e o Enterprise Test Server em um contêiner nativamente.

Pré-requisitos e limitações

Pré-requisitos

Nome	Descrição
py3270	py3270 é uma interface Python para x3270, um emulador de terminal IBM 3270. Ele fornece uma API para um subprocesso x3270 ou s3270.
x3270	O x3270 é um emulador de terminal IBM 3270 para o X Window System e Windows. Isso pode ser usado pelo desenvolvedor para teste de unidade localmente.
Robot-Framework-Mainframe-3270-Biblioteca	O Mainframe3270 é uma biblioteca para Robot Framework baseada no projeto py3270.
Rocket Software Verastream	O Rocket Software Verastream é uma plataforma de integração que permite testar ativos de mainframe da mesma forma que aplicativos móveis, aplicativos web e serviços web SOA são testados.
Instalador e licença do Rocket Software Unified Functional Testing (UFT)	O Rocket Software Unified Functional Testing é um software que fornece automação de testes funcionais e de regressão para aplicativos e ambientes de software.
Instalador e licença do Rocket Software Enterprise Server	O Enterprise Server fornece o ambiente de runtime para aplicativos de mainframe.
Instalador e licença do Rocket Software Enterprise Test Server	O Rocket Software Enterprise Test Server é um ambiente de teste de aplicativos de mainframe da IBM.
AccuRev Instalador e licença do Rocket Software para servidor e instalador e licença da Rocket Software Micro Focus AccuRev para sistemas operacionais Windows e Linux	AccuRev fornece gerenciamento de código-fonte (SCM). O AccuRev sistema foi projetado para ser usado por uma equipe de pessoas que estão desenvolvendo um conjunto de arquivos.

Instalador, patch e licença do Rocket Software Enterprise Developer para Eclipse	O Enterprise Developer fornece ao desenvolvedor de mainframe uma plataforma para desenvolver e manter os principais aplicativos on-line e em lote do mainframe.

Limitações

- A criação de uma imagem do Windows Docker não é suportada no CodeBuild. Esse problema relatado precisa do suporte das equipes Windows Kernel/HCS e Docker. A solução alternativa é criar um runbook de criação de imagem do Docker usando o Systems Manager. Esse padrão usa a solução alternativa para criar imagens do Rocket Software Enterprise Developer for Eclipse e da Rocket Software Micro Focus Enterprise Test Server Container.
- A conectividade de nuvem privada virtual (VPC) ainda não CodeBuild é suportada no Windows, portanto, o padrão não usa o Rocket Software License Manager para gerenciar licenças nos contêineres OpenText Rocket Software Enterprise Developer e Rocket Software Enterprise Test Server.

Versões do produto

- Rocket Software Enterprise Developer 5.5 ou posterior
- Rocket Software Enterprise Test Server 5.5 ou posterior
- Rocket Software Enterprise Server 5.5 ou posterior
- Rocket Software AccuRev 7.x ou posterior
- Imagem base do Windows Docker para Rocket Software Enterprise Developer e Enterprise Test Server: microsoft/dotnet-framework-4.7.2-runtime
- Imagem base do Linux Docker para AccuRev cliente: amazonlinux:2

Arquitetura

Ambiente de mainframe

No desenvolvimento convencional de mainframe, os desenvolvedores precisam usar hardware de mainframe para desenvolver e testar programas. Eles enfrentam limitações de capacidade, por exemplo, milhões de instruções restritas por segundo (MIPS) para o ambiente de dev/teste, e precisam confiar nas ferramentas disponíveis nos computadores mainframe.

Em muitas organizações, o desenvolvimento de mainframe segue a metodologia de desenvolvimento em cascata, com equipes confiando em ciclos longos para lançar mudanças. Esses ciclos de lançamento geralmente são mais longos do que o desenvolvimento de produtos digitais.

O diagrama a seguir mostra vários projetos de mainframe compartilhando hardware de mainframe para seu desenvolvimento. No hardware de mainframe, é caro escalar um ambiente de desenvolvimento e teste para mais projetos.

Arquitetura do AWS

Esse padrão estende o desenvolvimento do mainframe para o. Nuvem AWS Primeiro, ele usa o AccuRev SCM para hospedar o código-fonte do mainframe. AWS Em seguida, ele disponibiliza o Enterprise Developer e o Enterprise Test Server para criar e testar o código do mainframe. AWS

As seções a seguir descrevem os três componentes principais do padrão.

1. SCM

Em AWS, o padrão é usado AccuRev para criar um conjunto de espaços de trabalho e controle de versão do SCM para o código-fonte do mainframe. Sua arquitetura baseada em fluxo permite o desenvolvimento paralelo de mainframe para várias equipes. Para mesclar uma alteração, AccuRev usa o conceito de promoção. Para adicionar essa alteração a outros espaços de trabalho, AccuRev use o conceito de atualização.

No nível do projeto, cada equipe pode criar um ou mais fluxos AccuRev para monitorar as mudanças no nível do projeto. Eles são chamados de fluxos de projeto. Esses fluxos de projeto são herdados do mesmo fluxo principal. O fluxo principal é usado para mesclar as alterações de diferentes fluxos do projeto.

Cada fluxo de projeto pode promover código para AccuRev, e um gatilho de publicação de promoção é configurado para iniciar o pipeline de AWS CI/CD. A compilação bem-sucedida de uma alteração na reprodução do projeto pode ser promovida para seu fluxo principal para mais testes de regressão.

Normalmente, o fluxo principal é chamado de fluxo de integração do sistema. Quando há uma promoção de uma reprodução do projeto para um fluxo de integração de sistema, um gatilho de pós-promoção inicia outro pipeline de CI/CD para executar testes de regressão.

Além do código de mainframe, esse padrão inclui AWS CloudFormation modelos, documentos do Systems Manager Automation e scripts. Seguindo as infrastructure-as-code melhores práticas, eles são controlados por versão em. CodeCommit

Se você precisar sincronizar o código do mainframe com um ambiente de mainframe para implantação, a Rocket Software fornece a solução Enterprise Sync, que sincroniza o código do SCM com o AccuRev SCM do mainframe.

2. Ambientes de teste e desenvolvimento

Em uma grande organização, escalar mais de cem ou até mais de mil desenvolvedores de mainframe é um desafio. Para resolver essa restrição, o padrão usa instâncias EC2 do Amazon Windows para desenvolvimento. Nas instâncias, as ferramentas Enterprise Developer for Eclipse estão instaladas. O desenvolvedor pode realizar todos os testes e depuração do código do mainframe localmente na instância.

AWS Systems Manager Os documentos State Manager e Automation são usados para automatizar o provisionamento da instância do desenvolvedor. O tempo médio para criar uma instância de desenvolvedor é de 15 minutos. O software e as configurações a seguir estão preparados:

- AccuRev Cliente Windows para verificar e confirmar o código-fonte AccuRev
- Ferramenta Enterprise Developers for Eclipse, para escrever, testar e depurar código de mainframe localmente
- Estruturas de teste de código aberto Estrutura de teste de desenvolvimento orientado a comportamento (BDD) Python Behave, py3270 e o emulador x3270 para criar scripts para testar aplicativos
- Uma ferramenta de desenvolvedor do Docker para criar a imagem do Enterprise Test Server Docker e testar o aplicativo no contêiner do Enterprise Test Server Docker

No ciclo de desenvolvimento, os desenvolvedores usam a EC2 instância para desenvolver e testar o código do mainframe localmente. Quando as alterações locais são testadas com sucesso, os desenvolvedores promovem a alteração no AccuRev servidor.

3. Pipelines de CI/CD

No padrão, os pipelines de CI/CD são usados para testes de integração e testes de regressão antes da implantação no ambiente de produção.

Conforme explicado na seção SCM, AccuRev usa dois tipos de fluxos: um fluxo de projeto e um fluxo de integração. Cada fluxo é conectado a pipelines de CI/CD. Para realizar a integração entre o AccuRev servidor e AWS CodePipeline, o padrão usa o script de AccuRev pós-promoção para criar um evento para iniciar o CI/CD.

Por exemplo, quando um desenvolvedor promove uma alteração em um stream de projeto em AccuRev, ele inicia um script de pós-promoção para ser executado no AccuRev Server. Em seguida, o script carrega os metadados da alteração em um bucket do Amazon Simple Storage Service (Amazon S3) para criar um evento do Amazon S3. Esse evento iniciará um pipeline CodePipeline configurado para ser executado.

O mesmo mecanismo de iniciação de eventos é usado para o fluxo de integração e seus pipelines associados.

No pipeline de CI/CD, CodePipeline use CodeBuild com o contêiner do cliente AccuRev Linux para verificar o código mais recente dos AccuRev fluxos. Em seguida, o pipeline começa CodeBuild a usar o contêiner Enterprise Developer Windows para compilar o código-fonte e a usar o contêiner Enterprise Test Server Windows CodeBuild para testar aplicativos de mainframe.

O CI/CD pipelines are built using CloudFormation templates, and the blueprint will be used for new projects. By using the templates, it takes less than an hour for a project to create a new CI/CD gasoduto chegou AWS.

Para escalar sua capacidade de teste de mainframe AWS, o padrão cria a suíte de DevOps testes da Rocket Software, o Verastream e o servidor UFT. Ao usar as DevOps ferramentas modernas, você pode executar quantos testes precisar. AWS

Um exemplo de ambiente de desenvolvimento de mainframe com o Rocket Software ativado AWS é mostrado no diagrama a seguir.

Pilha de tecnologias de destino

Esta seção fornece uma visão mais detalhada da arquitetura de cada componente no padrão.

1. Repositório de código-fonte — SCM AccuRev

AccuRev O SCM está configurado para gerenciar as versões do código-fonte do mainframe. Para alta disponibilidade, AccuRev suporta os modos primário e de réplica. Os operadores podem fazer o failover para a réplica ao realizar a manutenção no nó primário.

Para acelerar a resposta do pipeline de CI/CD, o padrão usa o Amazon CloudWatch Events para detectar alterações no código-fonte e iniciar o início do pipeline.

1. O pipeline está configurado para usar uma fonte do Amazon S3.
2. Uma regra de CloudWatch eventos é configurada para capturar eventos do S3 de um bucket do S3 de origem.
3. A regra de CloudWatch eventos define uma meta para o pipeline.
4. AccuRev O SCM está configurado para executar um script de pós-promoção localmente após a conclusão da promoção.
5. AccuRev O SCM gera um arquivo XML que contém os metadados da promoção, e o script carrega o arquivo XML no bucket S3 de origem.
6. Após o upload, o bucket S3 de origem envia eventos que correspondam à regra de CloudWatch Eventos, e a regra de CloudWatch Eventos inicia a execução do pipeline.

Quando o pipeline é executado, ele inicia um CodeBuild projeto para usar um contêiner de cliente AccuRev Linux para verificar o código de mainframe mais recente de um fluxo associado AccuRev .

O diagrama a seguir mostra uma configuração de AccuRev servidor.

2. Modelo de desenvolvedor corporativo

O padrão usa EC2 modelos da Amazon para simplificar a criação da instância do desenvolvedor. Ao usar o State Manager, ele pode aplicar configurações de software e licença às EC2 instâncias de forma consistente.

O EC2 modelo da Amazon se baseia em suas configurações de contexto de VPC e configurações de instância padrão e segue os requisitos de marcação corporativa. Ao usar um modelo, uma equipe pode criar suas próprias novas instâncias de desenvolvimento.

Quando uma instância de desenvolvedor é iniciada, associando-se a tags, o Systems Manager usa o State Manager para aplicar a automação. A automação inclui as seguintes etapas gerais.

1. Instale o software Enterprise Developer e instale os patches.
2. Instale o AccuRev cliente para Windows.
3. Instale o script pré-configurado para que os desenvolvedores participem do AccuRev stream. Inicialize os workspaces do Eclipse.

4. Instale ferramentas de desenvolvimento, incluindo x3270, py3270 e Docker.
5. Defina as configurações de licença para apontar para um balanceador de carga do License Manager.

O diagrama a seguir mostra uma instância de desenvolvedor corporativo criada pelo EC2 modelo da Amazon, com software e configuração aplicados à instância pelo State Manager. As instâncias de desenvolvedores corporativos se conectam AWS License Manager para ativar suas licenças.

3. Pipelines de CI/CD

Conforme explicado na seção de AWS arquitetura, no padrão, existem CI/CD pipelines and system integration pipelines. Each mainframe project team creates a pipeline or multiple CI/CD pipelines for building the programs that they are developing in a project. These project CI/CD pipelines em nível de projeto que verificam o código-fonte de um fluxo associado. AccuRev

Em uma equipe de projeto, os desenvolvedores promovem seu código no AccuRev fluxo associado. Em seguida, a promoção inicia o pipeline do projeto para criar o código e executar testes de integração.

Cada pipeline de CI/CD de projeto usa CodeBuild projetos com a imagem Amazon ECR da ferramenta Enterprise Developer e a ferramenta Enterprise Test Server Amazon ECR image.

CodePipeline e CodeBuild são usados para criar os pipelines de CI/CD. Porque CodeBuild , sem taxas ou compromissos iniciais, você paga apenas pelo que usa. CodePipeline Em comparação com o hardware de mainframe, a AWS solução reduz consideravelmente o lead time de provisionamento de hardware e diminui o custo do seu ambiente de testes.

No desenvolvimento moderno, várias metodologias de teste são usadas. Por exemplo, desenvolvimento orientado a testes (TDD), BDD e Robot Framework. Com esse padrão, os desenvolvedores podem usar essas ferramentas modernas para testes de mainframe. Por exemplo, usando x3270, py3270 e a ferramenta de teste Behave python, você pode definir o comportamento de um aplicativo on-line. Você também pode usar a estrutura de robôs build mainframe 3270 nesses pipelines de CI/CD.

O diagrama a seguir mostra o pipeline de CI/CD do fluxo de equipe.

O diagrama a seguir mostra o relatório de teste de CI/CD do projeto produzido pelo CodePipeline Mainframe3270 Robot Framework.

O diagrama a seguir mostra o relatório de teste de CI/CD do projeto produzido por CodePipeline in Py3270 e Behave BDD.

Depois que os testes em nível de projeto são aprovados com sucesso, o código testado é promovido manualmente para o fluxo de integração no AccuRev SCM. Você pode automatizar essa etapa depois que as equipes confiarem na cobertura de testes do pipeline de projetos.

Quando o código é promovido, o pipeline de CI/CD de integração do sistema verifica o código mesclado e executa testes de regressão. O código mesclado é promovido a partir de todos os fluxos paralelos do projeto.

Dependendo da precisão do ambiente de teste, os clientes podem ter mais pipelines de CI/CD de integração do sistema em um ambiente diferente, por exemplo, UAT, pré-produção.

No padrão, as ferramentas usadas no pipeline de integração do sistema são Enterprise Test Server, UFT Server e Verastream. Todas essas ferramentas podem ser implantadas no contêiner Docker e usadas com. CodeBuild

Depois de testar com sucesso os programas de mainframe, o artefato é armazenado, com controle de versão, em um bucket S3.

O diagrama a seguir mostra um pipeline de CI/CD de integração de sistema.

Depois que o artefato for testado com sucesso nos pipelines de CI/CD de integração do sistema, ele poderá ser promovido para implantação em produção.

Se você precisar implantar o código-fonte de volta no mainframe, a Rocket Software oferece a solução Enterprise Sync para sincronizar o código-fonte de AccuRev volta ao Mainframe Endeavour.

O diagrama a seguir mostra um pipeline de produção de CI/CD implantando o artefato em servidores corporativos. Neste exemplo, CodeDeploy orquestra a implantação do artefato de mainframe testado no Enterprise Server.

Além do passo a passo da arquitetura do pipeline de CI/CD, consulte a postagem do AWS DevOps blog Automatize milhares de testes de mainframe AWS com o Micro Focus Enterprise Suite para obter mais informações sobre como testar aplicativos de mainframe em e. CodeBuild CodePipeline (A Micro Focus agora é Rocket Software.) Consulte a postagem do blog para obter as melhores práticas e detalhes sobre como fazer testes de mainframe em AWS.

Ferramentas

AWS ferramentas de automação

- AWS CloudFormation
- CloudWatch Eventos da Amazon
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline
- Amazon ECR
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

Ferramentas da Rocket Software

- Desenvolvedor Rocket Enterprise para Eclipse
- Servidor de teste Rocket Enterprise
- Rocket Enterprise Server (implantação de produção)
- Software Rocket AccuRev
- License Manager do Rocket Software Enterprise Suite
- Integrador de hospedagem Verastream da Rocket Software
- Software Rocket UFT One

Outras ferramentas

- x3270

- py3270
- Robot-Framework-Mainframe-3270-Biblioteca

Épicos

Crie a infraestrutura do AccuRev SCM

Tarefa	Descrição	Habilidades necessárias
Implante um servidor AccuRev SCM primário usando CloudFormation.		AWS CloudFormation
Crie o usuário AccuRev administrador.	Faça login no AccuRev SCM Server e execute o comando CLI para criar um usuário administrador.	AccuRev Administrador do servidor SCM
Crie AccuRev streams.	Crie AccuRev fluxos que herdam dos fluxos superiores em sequência: produção, integração de sistemas, fluxos de equipe.	AccuRev Administrador do SCM
Crie as contas de AccuRev login do desenvolvedor.	Use os comandos da CLI do AccuRev SCM para AccuRev criar contas de login de usuários para desenvolvedores de mainframe.	AccuRev Administrador do SCM

Crie o modelo de EC2 lançamento da Amazon para desenvolvedores corporativos

Tarefa	Descrição	Habilidades necessárias
Implante o modelo de EC2 lançamento da Amazon usando CloudFormation.	Use CloudFormation para implantar um modelo de EC2 lançamento da Amazon	AWS CloudFormation

Tarefa	Descrição	Habilidades necessárias
	para instâncias do Enterpris e Developer. O modelo inclui um documento do Systems Manager Automation para a instância do Rocket Enterprise Developer.	
Crie a instância Enterprise Developer a partir do EC2 modelo da Amazon.		Login do console da AWS e habilidades para desenvolv edores de mainframe

Crie a imagem Docker da ferramenta Enterprise Developer

Tarefa	Descrição	Habilidades necessárias
Crie a imagem Docker da ferramenta Enterprise Developer.	Use o comando Docker e a ferramenta Dockerfile para desenvolvedores corporati vos para criar a imagem do Docker.	Docker
Crie o repositório Docker no Amazon ECR.	No console do Amazon ECR, crie o repositório para a imagem do Enterprise Developer Docker.	Amazon ECR
Envie a imagem Docker da ferramenta Enterprise Developer para o Amazon ECR.	Execute o comando Docker push para enviar a imagem do Docker da ferramenta Enterprise Developer e salvá-la no repositório Docker no Amazon ECR.	Docker

Crie a imagem do Enterprise Test Server Docker

Tarefa	Descrição	Habilidades necessárias
Crie a imagem do Enterprise Test Server Docker.	Use o comando Docker e o Dockerfile do Enterprise Test Server para criar a imagem do Docker.	Docker
Crie o repositório Docker no Amazon ECR.	No console do Amazon ECR, crie o repositório Amazon ECR para a imagem Docker do Enterprise Test Server.	Amazon ECR
Envie a imagem do Enterpris e Test Server Docker para o Amazon ECR.	Execute o comando Docker push para enviar e salvar a imagem do Docker do Enterprise Test Server no Amazon ECR.	Docker

Crie o pipeline de CI/CD do fluxo da equipe

Tarefa	Descrição	Habilidades necessárias
Crie o CodeCommit repositór io.	No CodeCommit console, crie um repositório baseado em Git para infraestrutura e código. CloudFormation	AWS CodeCommit
Faça o upload do CloudForm ation modelo e do código de automação no CodeCommit repositório.	Execute o comando push do Git para carregar o CloudForm ation modelo e o código de automação no repositório.	Git
Implante o pipeline de CI/CD do stream de equipe usando. CloudFormation	Use o CloudFormation modelo preparado para implantar um	AWS CloudFormation

Tarefa	Descrição	Habilidades necessárias
	pipeline de CI/CD de fluxo de equipe.	

Crie o pipeline de CI/CD de integração do sistema

Tarefa	Descrição	Habilidades necessárias
Crie a imagem do UFT Docker.	Use o comando Docker e o Dockerfile do UFT para criar a imagem do Docker.	Docker
Crie o repositório Docker no Amazon ECR para a imagem do UFT.	No console do Amazon ECR, crie o repositório Docker para a imagem do UFT.	Amazon ECR
Envie a imagem do UFT Docker para o Amazon ECR.	Execute o comando Docker push para enviar e salvar a imagem do Docker do Enterprise Test Server no Amazon ECR.	Docker
Crie a imagem Verastream Docker.	Use o comando Docker e o Verastream Dockerfile para criar a imagem do Docker.	Docker
Crie o repositório Docker no Amazon ECR para a imagem Verastream.	No console do Amazon ECR, crie o repositório Docker para a imagem Verastream.	Amazon ECR
Implante o pipeline de CI/CD de integração do sistema usando. CloudFormation	Use o CloudFormation modelo preparado para implantar um pipeline de CI/CD de integraçã o do sistema.	AWS CloudFormation

Crie um pipeline de CI/CD de implantação de produção

Tarefa	Descrição	Habilidades necessárias
Implante o Enterprise Server usando o AWS Quick Start.	Para implantar o Enterprise Server usando CloudFormation, inicie o Enterprise Server no AWS Quick Start.	AWS CloudFormation
Implante um pipeline de CI/CD de implantação de produção.	No CloudFormation console, use o CloudFormation modelo para implantar um pipeline de CI/CD de implantação de produção.	AWS CloudFormation

Recursos relacionados

Referências

- AWS DevOps Blog - Automatize milhares de testes de mainframe AWS com o Micro Focus Enterprise Suite (a Micro Focus agora é Rocket Software).
- repositório py3270/py3270 GitHub
- Repositório de bibliotecas GitHub altran-pt-gdc/robot-framework-mainframe-3270
- Bem-vindo ao Behave!
- Blog de parceiros da APN - Tag: Micro Focus (a Micro Focus agora é Rocket Software.)
- Executar uma instância a partir de um modelo de execução

AWS Marketplace

- Software Rocket UFT One

AWS Início rápido

- Servidor Rocket Enterprise em AWS

Modernize as workloads de impressão on-line de mainframe na AWS usando o Micro Focus Enterprise Server e o LRS VPSX/MFI

Criado por Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) e Kevin Yung (AWS)

Resumo

Esse padrão mostra como modernizar suas workloads de impressão on-line de mainframe essenciais para os negócios na nuvem da Amazon Web Services (AWS) usando o Micro Focus Enterprise Server como um runtime para um aplicativo de mainframe modernizado e o LRS VPSX/MFI (Micro Focus Interface) como servidor de impressão. O padrão é baseado na abordagem de modernização do mainframe de redefinir a plataforma. Nessa abordagem, você migra seu aplicativo on-line de mainframe para o Amazon Elastic Compute Cloud (Amazon EC2) e migra seu banco de dados de mainframe, como o IBM for z/OS, DB2 para o Amazon Relational Database Service (Amazon RDS). A autenticação e autorização para o fluxo de trabalho de impressão modernizado são realizadas pelo AWS Directory Service for Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD. O LRS Directory Information Server (LRS/DIS) é integrado ao AWS Managed Microsoft AD para autenticação e autorização do fluxo de trabalho de impressão. Ao modernizar suas cargas de trabalho de impressão on-line, você pode reduzir os custos de infraestrutura de TI, mitigar a dívida técnica de manter sistemas legados, remover silos de dados, aumentar a agilidade e a eficiência com um DevOps modelo e aproveitar os recursos sob demanda e a automação na nuvem da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma workload de gerenciamento de impressão ou saída on-line de mainframe
- Conhecimento básico de como reconstruir e fornecer um aplicativo de mainframe executado no Micro Focus Enterprise Server (para obter mais informações, consulte a planilha de dados do Enterprise Server na documentação da Micro Focus.)
- Conhecimento básico das soluções e conceitos de impressão em nuvem do LRS (para obter mais informações, consulte Modernização de saída na documentação do LRS).
- Software e licença do Micro Focus Enterprise Server (para obter mais informações, entre em contato com a equipe de vendas da Micro Focus.)

- VPSX/MFI, LRS/Queue, and LRS/DISSoftware e licenças do LRS (para obter mais informações, entre em contato com a equipe de vendas do LRS.)

> **Note**
>
> Para obter mais informações sobre considerações de configuração para cargas de trabalho de impressão on-line de mainframe, consulte Considerações na seção Informações adicionais desse padrão.

Versões do produto

- Micro Focus Enterprise Server 8.0 ou posterior
- LRS VPSX/MFI V1R3 ou superior

Arquitetura

Pilha de tecnologia de origem

- Sistema operacional: IBM z/OS
- Linguagem de programação: Common Business-Oriented Language (COBOL) e Customer Information Control System (CICS)
- Banco de dados — IBM DB2 para z/OS IBM Information Management System (IMS) e Virtual Storage Access Method (VSAM)
- Segurança — Instalação de Controle de Acesso a Recursos (RACF), CA Top Secret para z/OS e Instalação de Controle de Acesso 2 () ACF2
- Gerenciamento de impressão e saída: produtos de impressão z/OS de mainframe IBM (IBM Infoprint Server para z/OS, LRS e CA View)

Pilha de tecnologias de destino

- Sistema operacional — Microsoft Windows Server em execução na Amazon EC2
- Computação — Amazon EC2
- Linguagem de programação: COBOL e CICS
- Banco de dados: Amazon RDS

- Segurança: AWS Managed Microsoft AD
- Gerenciamento de impressão e produção: solução de impressão LRS na AWS
- Ambiente runtime de mainframe: Micro Focus Enterprise Server

Arquitetura de origem

O diagrama a seguir mostra uma arquitetura típica do estado atual para uma carga de trabalho de impressão on-line de mainframe.

O diagrama mostra o seguinte fluxo de trabalho:

1. Os usuários realizam transações comerciais em um sistema de engajamento (SoE) construído em um aplicativo IBM CICS escrito em COBOL.
2. O SoE invoca o serviço de mainframe, que registra os dados da transação comercial em um banco de dados system-of-records (SoR), como o IBM for z/OS. DB2
3. O SoR persiste os dados comerciais do SoE.
4. Um usuário inicia uma solicitação para gerar a saída de impressão do CICS SoE, que inicia um aplicativo de transação de impressão para processar a solicitação de impressão.
5. O aplicativo de transação de impressão (como um programa CICS e COBOL) extrai dados do banco de dados, formata os dados de acordo com os requisitos comerciais e gera resultados comerciais (dados de impressão), como extratos de cobrança, cartões de identificação ou extratos de empréstimos. Em seguida, o aplicativo envia uma solicitação de impressão usando o Método de Acesso às Telecomunicações Virtuais (VTAM). Um servidor de impressão z/OS (como o IBM Infoprint Server) usa NetSpool ou um componente VTAM similar para interceptar as solicitações de impressão e, em seguida, cria conjuntos de dados de saída de impressão no spool do JES usando os parâmetros de saída do JES. Os parâmetros de saída do JES especificam as informações de roteamento que o servidor de impressão usa para transmitir a saída para uma impressora de rede específica. O termo VTAM se refere ao z/OS Communications Server e ao elemento de serviços System Network Architecture (SNA) do z/OS.
6. O componente de transmissão de saída de impressão transmite os conjuntos de dados de impressão de saída do spool JES para impressoras remotas ou servidores de impressão, como LRS (conforme demonstrado nesse padrão), IBM Infoprint Server ou destinos de e-mail.

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura para uma workload de impressão on-line de mainframe que é implantada na nuvem AWS:

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário inicia uma solicitação de impressão a partir de uma interface de usuário on-line (CICS) para criar resultados impressos, como extratos de cobrança, cartões de identificação ou extratos de empréstimos.
2. O aplicativo on-line de mainframe (reformulado para Amazon EC2) usa o tempo de execução do Micro Focus Enterprise Server para extrair dados do banco de dados do aplicativo, aplicar lógica comercial aos dados, formatar os dados e, em seguida, enviar os dados para um destino de impressão usando o Micro Focus CICS Print Exit (DFHUPRNT).
3. O banco de dados do aplicativo (um SoR executado no Amazon RDS) persiste os dados para a saída de impressão.
4. O nome da VPSX/MFI printing solution is deployed on Amazon EC2, and its operational data is stored in Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect print data through the Micro Focus CICS Print Exit API (DFHUPRNT) and deliver the data to a specified printer destination. The original TERMID (TERM) that's used in the modernized CICS application is used as the VPSX/MFI fila LRS.

> **Note**
>
> A solução de destino normalmente não exige alterações no aplicativo para acomodar linguagens de formatação de mainframe, como IBM Advanced Function Presentation (AFP) ou Xerox Line Condition Data Stream (LCDS). Para obter mais informações sobre o uso da Micro Focus para migração e modernização de aplicativos de mainframe na AWS, consulte Capacitando workloads de mainframe corporativas na AWS com a Micro Focus na documentação da AWS.

Arquitetura de infraestrutura da AWS

O diagrama a seguir mostra uma arquitetura de infraestrutura da AWS altamente disponível e segura para uma workload de impressão on-line de mainframe:

O diagrama mostra o seguinte fluxo de trabalho:

1. O aplicativo on-line do mainframe (escrito em uma linguagem de programação como CICS ou COBOL) usa a lógica comercial principal para processar e gerar resultados impressos, como extratos de cobrança, cartões de identificação e extratos de empréstimos. O aplicativo on-line é implantado na Amazon EC2 em duas zonas de disponibilidade (AZ) para alta disponibilidade (HA) e usa o Micro Focus CICS Print Exit para rotear a saída de impressão para o LRS VPSX/MFI para impressão do usuário final.
2. VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect or capture print data from the Micro Focus online Print Exit programming interface. Online Print Exit passes the necessary information to enable LRS VPSX/MFI to effectively process the print file and dynamically build LRS/QueueComandos do LRS.

   > **Note**
   >
   > Para obter mais informações sobre vários métodos de programação de aplicativos CICS para impressão e como eles são suportados no servidor Micro Focus Enterprise e no LRS VPSX/MFI, consulte Captura de dados de impressão na seção Informações adicionais desse padrão.

3.
   > **Note**
   >
   > Um Network Load Balancer fornece um nome DNS para integrar o Micro Focus Enterprise Server ao LRS VPSX/MFI. : LRS VPSX/MFI supports a Layer 4 load balancer. The Network Load Balancer also does a basic health check on LRS VPSX/MFI e direciona o tráfego para os destinos registrados que estão íntegros.

4. O servidor de impressão LRS VPSX/MFI é implantado na Amazon em duas EC2 zonas de disponibilidade para HA e usa o Amazon EBS como um armazenamento de dados operacional. VPSX/MFI supports both the active-active and active-passive service modes. This architecture uses multiple Availability Zones in an active-passive pair as an active and hot standby. The Network Load Balancer performs a health check on LRS VPSX/MFI EC2 Instâncias do LRS e encaminha o tráfego para instâncias em espera ativa em outra zona de disponibilidade se uma instância ativa estiver em um estado não íntegro. As solicitações de impressão persistem no LRS Job Queue localmente em cada uma das instâncias. EC2 Em caso de recuperação, uma instância com falha precisa ser reiniciada para que os serviços do LRS retomem o processamento da solicitação de impressão.

> **Note**
>
> O LRS VPSX/MFI também pode realizar verificações de saúde no nível da frota de impressoras. Para obter mais informações, consulte Verificações de integridade da frota de impressoras na seção Informações adicionais desse padrão.

5. O AWS Managed Microsoft AD se integra ao LRS/DIS para realizar a autenticação e autorização do fluxo de trabalho de impressão. Para obter mais informações, consulte Autenticação e autorização de impressão na seção Informações adicionais desse padrão.
6. O LRS VPSX/MFI usa o Amazon EBS para armazenamento em bloco. Você pode fazer backup de dados do Amazon EBS de EC2 instâncias ativas para o Amazon S3 point-in-time como snapshots e restaurá-los em volumes do EBS em espera ativa. Para automatizar a criação, retenção e exclusão de snapshots de volume do Amazon EBS, você pode usar o Amazon Data Lifecycle Manager para definir a frequência dos snapshots automatizados e restaurá-los com base em seus requisitos de RTO/RPO.

Ferramentas

Serviços da AWS

- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias da Amazon. EC2 Os volumes do EBS se comportam como dispositivos de bloco brutos e não formatados. É possível montar esses volumes como dispositivos em suas instâncias.
- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- O AWS Directory Service for Microsoft Active Directory (AD), também conhecido como AWS Managed Microsoft Active Directory, permite que suas workloads e recursos da AWS com reconhecimento de diretório usem o Active Directory gerenciado na AWS.

Outras ferramentas

- O LRS VPSX/MFI (Interface do Micro Focus Interface), desenvolvido em conjunto pela LRS e pela Micro Focus, captura a saída de um spool JES do Micro Focus Enterprise Server e a entrega de forma confiável a um destino de impressão especificado.
- O LRS Directory Information Server (LRS/DIS) é usado para autenticação e autorização durante o fluxo de trabalho de impressão.
- LRS/Queue is a TCP/IP-based LRS/Queue transmission agent, used by LRS VPSX/MFI, para coletar ou capturar dados de impressão por meio da interface de programação online Print Exit da Micro Focus.
- O Micro Focus Enterprise Server é um ambiente de implantação de aplicativos para aplicativos de mainframe Ele fornece o ambiente de execução para aplicativos de mainframe que são migrados ou criados usando qualquer versão do Micro Focus Enterprise Developer.

Épicos

Configure o Micro Focus Enterprise Server na Amazon EC2 e implante um aplicativo on-line de mainframe

Tarefa	Descrição	Habilidades necessárias
Configure o Micro Focus Enterprise Server e implante um aplicativo on-line de demonstração.	Configure o Micro Focus Enterprise Server na Amazon e EC2, em seguida, implante o aplicativo Micro Focus Account Demo (ACCT Demo) na Amazon EC2 seguindo as instruções do Tutorial: CICS Support na documentação da Micro Focus. O aplicativo ACCT Demo é um aplicativo on-line de mainframe (CICS) que cria e inicia a saída de impressão.	Arquiteto de nuvem

Configurar um servidor de impressão LRS na Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Obtenha uma licença de produto LRS para impressão.	Para obter uma licença de produto LRS para o LRSVPSX/MFI, LRS/Queue , and LRS/DIS, entre em contato com a equipe de gerenciamento de saída do LRS. Você deve fornecer os nomes de host das EC2 instâncias em que os produtos LRS serão instalados.	Crie um lead
Crie uma instância EC2 do Amazon Windows para instalar o LRS VPSX/MFI.	Execute uma instância EC2 do Amazon Windows seguindo as instruções da Etapa 1: Inicie uma instância na EC2 documentação da Amazon. Sua instância deve atender aos seguintes requisitos de hardware e software para LRS VPSX/MFI: • CPU: Dual Core • MEMÓRIA RAM: 16 GB • Unidade: 500 GB • EC2 Instância mínima — m5.xlarge • SISTEMA OPERACIONAL: Windows/Linux • Software: Internet Informati on Service (IIS) ou Apache	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Note Os requisitos anteriores de hardware e software são destinados a uma pequena frota de impressoras (cerca de 500 a 1000). Para obter todos os requisitos, consulte seus contatos do LRS e da AWS. Ao criar sua instância do Windows, faça o seguinte: 1. Confirme se o nome do EC2 host é o mesmo usado para a licença do produto LRS. 2. Ative o CGI na Amazon EC2 preenchendo o seguinte: a. Conecte-se à sua EC2 instância seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. b. No menu Iniciar do Windows, localize e	

Tarefa	Descrição	Habilidades necessárias
	abra o Gerenciador do Servidor. c. No Server Manager, escolha Dashboard (Painel), Quick Start (Início rápido), Add roles and features (Adicionar funções e recursos). Em seguida, escolha Funções do servidor. d. Em Funções de servidor, escolha WebServer (IIS) e, em seguida, escolha Desenvolvimento de aplicativos. e. Em Desenvolvimento de aplicativos, marque a caixa de seleção CGI. f. Siga as instruções no assistente para Adicionar funções e recursos do Gerenciador do Windows Server para instalar o CGI. g. Abra a porta 5500 no firewall do Windows da EC2 instância para comunicação LRS/Queue.	

Tarefa	Descrição	Habilidades necessárias
Instale o LRS VPSX/MFI na instância. EC2	1. Conecte-se à sua EC2 instância seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 2. **Note** Abra o link para a página de download do produto no e-mail do LRS que você deve receber. : Os produtos LRS são distribuídos por transferência eletrônica de arquivos (TEF). 3. Baixe o LRS VPSX/MFI e descompacte o arquivo (pasta padrão: `c:\LRS`). 4. Inicie o LRS Product Installer a partir da pasta descompactada para instalar o LRS VPSX/MFI. 5. No menu Seleciona r recursos, selecione Servidor VPSX® (V1R3.022) e escolha Avançar para iniciar o processo de instalação. Você receberá uma mensagem de sucesso	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	quando a instalação for concluída.	
Instale o LRS/Queue.	1. Conecte-se à sua EC2 instância do Micro Focus Enterprise Server seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 2. Abra o link para a página de download do produto LRS a partir do e-mail do LRS que você deve receber, baixe o LRS/Queue e, em seguida, descompacte o arquivo. 3. Vá até o local onde você baixou os arquivos e, em seguida, inicie o instalador do produto LRS para instalar o LRS/Queue.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Instale o LRS/DIS.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. Abra o link para a página de download do produto LRS a partir do e-mail do LRS que você deve receber, baixe o LRS/DIS e, em seguida, descompacte o arquivo. 3. Vá para o local em que você fez o download dos arquivos e inicie o LRS Product Installer. 4. No LRS Product Installer, expanda LRS Misc Tools, selecione LRS DIS e escolha Avançar. 5. Siga o restante das instruções no instalador do produto LRS para concluir o processo de instalação.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie um grupo-alvo e registre o LRS EC2 VPSX/MFI como alvo.	Crie um grupo de destino seguindo as instruções de Criar um grupo de destino para seu Network Load Balancer na documentação do Elastic Load Balancing. Ao criar o grupo de destino, faça o seguinte: 1. Na página Especificar detalhes do grupo, em Escolher um Tipo de destino, escolha Instâncias. 2. Para Protocol, escolha TCP. 3. Em Porta, escolha 5500. 4. Na página Registrar destinos, na seção Instâncias disponíveis, selecione as instâncias LRS EC2 VPSX/MFI.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Criar um Network Load Balancer.	Siga as instruções de Criar um Network Load Balancer na documentação do Elastic Load Balancing. Seu Network Load Balancer direciona o tráfego do Micro Focus Enterprise Server para o LRS VPSX/MFI. EC2 Ao criar o Network Load Balancer, faça o seguinte na página Receptores e roteamento: 1. Para Protocolo, escolha TCP. 2. Em Porta, escolha 5500. 3. Em Ação padrão, escolha Encaminhar para o grupo de destino que você criou anteriormente.	Arquiteto de nuvem

Integre o Micro Focus Enterprise Server com o LRS VPSX/MFI and LRS/Queue

Tarefa	Descrição	Habilidades necessárias
Configure o Micro Focus Enterprise Server para integração LRS/Queue.	1. Conecte-se à sua EC2 instância do Micro Focus Enterprise Server seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	2. No menu Iniciar do Windows, abra a interface de usuário do Micro Focus Enterprise Server Administration. 3. Na barra de menu, escolha NATIVO. 4. No painel de navegação, escolha Servidor de Diretórios e, em seguida, escolha BANKDEMO ou sua região do Enterprise Server. 5. Em Geral, no painel de navegação esquerdo, role para baixo até a seção Adicional para configurar as variáveis de ambiente (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) para apontar para LRSQ. 6. Para LRSQ_ADDRESS, insira o endereço IP ou o nome DNS do Network Load Balancer que você criou anteriormente. 7. Para LRSQ_PORT, insira VPSX LRSQ Listener Port (5500). 8. Para LRSQ_COMMAND, insira a localização do caminho do executável do LRSQ.	

Tarefa	Descrição	Habilidades necessárias
	9. **Note** Atualmente, o LRS suporta um limite máximo de 50 caracteres para nomes DNS, mas isso está sujeito a alterações no futuro. Se seu nome DNS for maior que 50, você poderá usar o endereço IP do Network Load Balancer como alternativa.	

Tarefa	Descrição	Habilidades necessárias
Disponibilize o CICS Print Exit (DFHUPRNT) para a inicialização do Micro Focus Enterprise Server.	1. Conecte-se à sua EC2 instância do Micro Focus Enterprise Server seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. 2. **Note** Copie o CICS Print Exit (DFHUPRNT) da pasta executável LRS VPSX/MFI (nomeada) para o local da instância do Micro Focus Enterprise Server. `VPSX_MFI_R2` EC2 Para sistemas de 32 bits, a localização é `C:\Program Files (x86)\Micro Focus\Enterprise Server\bin` . Para sistemas de 64 bits, a localização é `C:\Program Files (x86)\Micro Focus\Enterprise Server\bin64` .: o DFHUPRNT_	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`64.dll` arquivo deve ser renomeado para `DFHUPRNT.dll` quando copiado. Verifique se o Micro Focus Enterprise Server detectou a saída de impressão do CICS (DFHUPRNT) 1. Pare e inicie o Micro Focus Enterprise Server. 2. No painel de administração do Micro Focus Enterprise Server, abra Monitor, Logs, Logs do console. 3. Verifique os logs do console para ver a seguinte mensagem: “O usuário da impressora 3270 saiu do DFHUPRNT instalado com sucesso”.	

Tarefa	Descrição	Habilidades necessárias
Defina a ID do terminal da impressora CICS (TERMIDs) como Micro Focus Enterprise Server.	Habilite a impressão 3270 no Micro Focus Enterprise Server 1. No painel de administração do Micro Focus Enterpris e Server, abra CICS, Recursos, Por grupo. 2. No painel de navegação esquerdo, escolha SIT (Tabela de Inicialização do Sistema) e, em seguida, escolha BNKCICV. 3. Na seção Geral, role para baixo até 3270 e marque a caixa de seleção Impressão 3270. Defina o terminal da impressor a CICS no Micro Focus Enterprise Server 1. No painel de administração do Micro Focus Enterpris e Server, abra CICS, Recursos, Por tipo. 2. No painel de navegação à esquerda, selecione Termo e, em seguida, selecione Novo. O formulári o Criar recurso de terminal é aberto. 3. Em Nome, insira o nome da fila de impressão do LRS. (Observação: esse	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	padrão usa “P275" como ID do terminal da impressora CICS e fila de impressão LRS VPSX.) 4. Em Grupo, insira BANKTERM. 5. Em Instalação automática – Modelo, digite NÃO. 6. Em Identificadores de terminal - Tipo de terminal, insira DFHPRT32. 7. Em Nome da rede, insira VTAMP275. 8. Para Uso do terminal, marque a caixa de seleção Em serviço. 9. Role até a parte superior da página e escolha Salvar. 10. Escolha Instalar. Uma mensagem pop-up exibe uma mensagem de instalação bem-sucedida.	

Configure impressoras e usuários de impressão no Micro Focus Enterprise Server e no LRS VPSX/MFI

Tarefa	Descrição	Habilidades necessárias
Crie uma fila de impressão no LRS VPSX.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	instância na documentação da Amazon. EC2 2. Abra a interface da web do VPSX no menu Iniciar do Windows. 3. No painel de navegação, escolha Impressoras. 4. Escolha Adicionar e Adicionar impressora. 5. Na página de Configuração da impressora, em Nome da impressora, digite P275. 6. Para ID VPSX, insira. VPS1 7. Para CommType, selecione TCPIP/LRSQ. 8. Em Host/Endereço IP, insira o endereço IP da impressora física que você deseja adicionar. 9. Em Dispositivo, insira o nome do seu dispositivo. 10. Escolha Driver do Windows ou Driver Linux/Mac. 11. Escolha Adicionar. **Note** A fila de impressão deve ser equivalente à impressão TERMIDs	

Tarefa	Descrição	Habilidades necessárias
	criada no Micro Focus Enterprise Server.	

Tarefa	Descrição	Habilidades necessárias
Crie um usuário de impressão no LRS VPSX/MFI.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. Abra a interface da web do VPSX no menu Iniciar do Windows. 3. No painel de navegação , escolha Segurança e depois Usuários. 4. Na coluna Nome de usuário, escolha admin e, em seguida, escolha Copiar. 5. Na janela Manutenção do perfil do usuário, em Nome do usuário, insira um nome de usuário (por exemplo, PrintUser). 6. Em Descrição, insira uma breve descrição (por exemplo, Usuário para impressão de teste). 7. Selecione Atualizar. Isso cria um usuário de impressão (por exemplo, PrintUser). 8. No painel de navegação, em Usuário, escolha o novo usuário que você criou.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	9. No menu Comando, escolha Segurança. 10. Na página Regras de segurança, escolha todas as opções aplicáveis de segurança da impressora e segurança do trabalho e, em seguida, escolha Salvar. 11. Para adicionar seu novo usuário de impressão ao grupo Administrador, acesse o painel de navegação, escolha Segurança e, em seguida, escolha Configurar. 12. Na janela Configuração de segurança, adicione seu novo usuário de impressão à coluna Administrador.	

Configurar autorização e autenticação de impressão

Tarefa	Descrição	Habilidades necessárias
Crie um domínio AWS Managed Microsoft AD com usuários e grupos.	1. Crie um Active Directory no AWS Managed Microsoft AD seguindo as instruções de Criar seu diretório AWS Managed Microsoft AD na documentação do AWS Directory Service.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	2. Implante uma EC2 instância (gerenciador do Active Directory) e instale as ferramentas do Active Directory para gerenciar seu AWS Managed Microsoft AD seguindo as instruções da Etapa 3: Implantar uma EC2 instância para gerenciar seu AWS Managed Microsoft AD na documentação do AWS Directory Service. 3. **Note** Conecte-se à sua EC2 instância seguindo as instruções da Etapa 2: Conecte-se à sua instância na EC2 documentação da Amazon. : ao se conectar à EC2 instância, insira suas credenciais de administrador (para o diretório que você criou na etapa um) na janela Segurança do Windows.	

Tarefa	Descrição	Habilidades necessárias
	4. No menu Iniciar do Windows, em Ferrament as administrativas do Windows, escolha Usuários e computadores do Active Directory. 5. Crie um usuário de impressão no domínio do Active Directory seguindo as etapas em Criar um usuário na documentação do AWS Directory Service.	
Associe o LRS VPSX/MFI a EC2 um domínio Microsoft AD gerenciado pela AWS.	Associe o LRS VPSX/MFI ao EC2 seu domínio AWS Managed Microsoft AD automaticamente (document ação do AWS Knowledge Center) ou manualmente (documentação do AWS Directory Service).	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure e integre o LRS/DIS com AWS Managed Microsoft AD.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. No menuIniciar do Windows, abra a interface da web do VPSX. 3. No painel de navegação , escolha Segurança e depois Configurar. 4. Na página Configuração de Segurança, na seção Parâmetros de Segurança , em Tipo de Segurança, selecione Interno. 5. Insira suas preferências para o restante das opções na seção Parâmetros de segurança. 6. Abra a pasta LRS Output Management no menu Iniciar do Microsoft Windows, escolha Iniciar do Servidor e, em seguida, escolha Parar do Servidor. 7. Faça login no LRS VPSX/ MFI com seu nome de usuário e senha do Active Directory.	Arquiteto de nuvem

Teste um fluxo de trabalho de impressão on-line

Tarefa	Descrição	Habilidades necessárias
Inicie uma solicitação de impressão on-line a partir da aplicação Micro Focus ACCT de demonstração.	1. **Note** Abra o emulador de terminal TN3270 na sua EC2 instância do Micro Focus Enterprise Server. (: Esse padrão usa emuladores de terminal 3270.) 2. Conecte-se ao emulador de terminal TN327 0 (Rumba). Para o Endereço do nome do host, use 127.0.0.1. Para a Porta Telnet, use 9270. 3. Depois de se conectar à tela 3270, pressione CTL +SHIFT+Z para limpar a tela. 4. Para iniciar o aplicativo ACCT Demo, em uma tela limpa, digite ACCT. Isso irá abrir a tela principal do aplicativo ACCT Demo online (CICS). Nota: a tela principal inclui opções de menu, como Arquivo da conta, Pesquisar por nome,	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	inserir, Tipo de solicitação, Conta e Impressora. 5. Para enviar uma solicitação de impressão do aplicativo ACCT Demo online (CICS), digite P no campo tipo de solicitação, 11111 no campo conta e P275 no campo impressora. Certifique-se de definir o valor no campo impressora como o valor da ID do terminal da impressora CICS. 6. Pressione Enter. A mensagem “Solicitação de impressão agendada” é exibida na parte inferior da tela. Isso confirma que uma solicitação de impressão on-line foi gerada a partir do aplicativo ACCT Demo e enviada ao LRS VPS/MFI para processamento de impressão.	

Tarefa	Descrição	Habilidades necessárias
Verifique a saída de impressão no LRS VPSX/MFI.	1. Conecte-se à sua EC2 instância LRS VPSX/MFI seguindo as instruções da Etapa 2: Conecte-se à sua instância na documentação da Amazon. EC2 2. No menu Iniciar do Windows, abra a interface da web do VPSX. 3. No painel de navegação, selecione Impressoras e, em seguida, selecione Fila de saída. Encontre a fila de impressão P275 que você criou para impressão on-line anteriormente. 4. Para a fila de impressão (P275), na coluna ID do spool, escolha a ID do spool para a solicitação na fila da impressora. 5. Na guia Ações, na coluna COMANDO, escolha Procurar. Agora você pode ver a saída impressa de um extrato de conta com colunas para Número da Conta, SOBRENOME, PRIMEIRO, ENDEREÇO, TELEFONE, Nº. Cartões emitidos, Data de emissão, Valor e Saldo.	Engenheiro de testes

Tarefa	Descrição	Habilidades necessárias
	Para ver um exemplo, consulte o anexo online_print_output desse padrão.	

Recursos relacionados

- Modernização da saída do LRS (documentação do LRS)
- Conceitos de rede VTAM (documentação da IBM)
- Resumo dos tipos de unidades lógicas (LU) (documentação da IBM)
- ANSI e controles de transporte de máquinas (documentação da IBM)
- Capacitando workloads de mainframe corporativo na AWS com a Micro Focus (blog da rede de parceiros da AWS)
- Crie um PAC do Micro Focus Enterprise Server com o Amazon EC2 Auto Scaling e o Systems Manager (documentação do AWS Prescriptive Guidance)
- Fluxo de dados de apresentação de funções avançadas (AFP) (documentação da IBM)
- Fluxo de dados condicionado por linha (LCDS) (documentação do Compart)

Mais informações

Considerações

Durante sua jornada de modernização, você pode considerar uma grande variedade de configurações para os processos on-line do mainframe e a saída que eles geram. A plataforma de mainframe foi personalizada por cada cliente e fornecedor que a utiliza com requisitos específicos que afetam diretamente a impressão. Por exemplo, sua plataforma atual pode incorporar o IBM Advanced Function Presentation (AFP) ou o Xerox Line Condition Data Stream (LCDS) ao fluxo de trabalho atual. Além disso, os caracteres de controle do carro do mainframe e as palavras de comando do canal podem afetar a aparência da página impressa e podem precisar de tratamento especial. Como parte do processo de planejamento da modernização, recomendamos que você avalie e compreenda as configurações em seu ambiente de impressão específico.

Captura de dados de impressão

Esta seção resume os métodos de programação de aplicativos CICS que você pode usar em um ambiente de mainframe IBM para impressão. Servidor de VPSX/MFI components provide techniques to allow the same application programs to create data in the same way. The following table describes how each application programming method is supported in a modernized CICS application running in AWS and Micro Focus Enterprise Server with an LRS VPSX/MFI impressão LRS.

Método	Descrição	Suporte para o método em um ambiente modernizado
EXEC CICS ENVIA TEXTO... ou EXEC CICS ENVIAR MAPA..	Esses métodos CICS e VTAM são responsáveis por criar e fornecer fluxos de dados de impressão 3270/SCS para LUTYPE0 e dispositi vos de impressão. LUTYPE1 LUTYPE3	Uma interface de programa de aplicativo (API) do Micro Focus online Print Exit (DFHUPRNT) permite que os dados de impressão sejam processados por fluxos de dados de VPSX/MFI when 3270/SCS impressão criados usando qualquer um desses métodos.
EXEC CICS ENVIA TEXTO... ou EXEC CICS ENVIAR MAPA.. (com software de mainframe IBM de terceiros)	Os métodos CICS e VTAM são responsáveis por criar e fornecer fluxos de dados de impressão 3270/SCS para LUTYPE0 e dispositi vos de impressão. LUTYPE1 LUTYPE3 Produtos de software de terceiros intercept am os dados de impressão, convertem os dados em dados de formato de impressão padrão com um caractere de controle ASA/MCH e colocam os dados no spool do JES para serem processados por sistemas de impressão	Uma API de saída de impressão on-line da Micro Focus (DFHUPRNT) permite que os dados de impressão sejam processados por fluxos de dados de VPSX/MFI when 3270/SCS impressão criados usando qualquer um desses métodos.

	baseados em mainframe que usam o JES.	
EXEC CICS SPOOLOPEN	Esse método é usado pelos programas de aplicação do CICS para gravar dados diretamente no spool do JES. Os dados então ficam disponíveis para serem processados por sistemas de impressão baseados em mainframe que usam o JES.	O Micro Focus Enterprise Server transfere os dados para o spool do Enterprise Server, onde eles podem ser processados pelo VPSX/MFI Batch Print Exit LRSPRTE6 () que transfere os dados para o VPSX.
DRS/API	Uma interface programát ica fornecida pelo LRS é usada para gravar dados de impressão no JES.	O VPSX/MFI fornece uma interface de substituição que transfere os dados de impressão diretamente para o VPSX.

Verificações de integridade da frota de impressoras

O LRS VPSX/MFI (LRS LoadX) pode realizar verificações de integridade detalhadas, incluindo gerenciamento de dispositivos e otimização operacional. O gerenciamento de dispositivos pode detectar falhas em um dispositivo de impressora e encaminhar a solicitação de impressão para uma impressora saudável. Para obter mais informações sobre verificações de integridade detalhadas para frotas de impressoras, consulte a documentação do LRS que está incluída na sua licença de produto.

Autorização e autenticação de impressão

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or an LDAP server. In addition to basic print authorization, LRS/DIStambém pode aplicar controles de segurança de impressão em nível granular nos seguintes casos de uso:

- Gerencie quem pode navegar pelo trabalho da impressora.
- Gerencie o nível de navegação dos trabalhos de outros usuários.
- Gerencie tarefas operacionais. Por exemplo, segurança em nível de comando, como suspender/liberar, limpar, modificar, copiar e redirecionar. A segurança pode ser configurada pelo ID do usuário ou pelo grupo (semelhante ao grupo AD ou grupo LDAP).

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Mova arquivos de mainframe diretamente para o Amazon S3 usando o Transfer Family

Criado por Luis Gustavo Dantas (AWS)

Resumo

Como parte da jornada de modernização, você pode enfrentar o desafio de transferir arquivos entre seus servidores on-premises e a nuvem da Amazon Web Services (AWS). Transferir dados de mainframes pode ser um desafio complexo porque os mainframes normalmente não conseguem acessar armazenamentos modernos de dados, como o Amazon Simple Storage Service (Amazon S3), o Amazon Elastic Block Store (Amazon EBS) ou o Amazon Elastic File System (Amazon EFS).

Muitos clientes usam recursos intermediários de preparação, como servidores Linux, Unix ou Windows on-premises, para transferir arquivos para a Nuvem AWS. Você pode evitar esse método indireto usando o AWS Transfer Family com o Secure Shell (SSH) Protocolo de Transferência de Arquivos (SFTP) para carregar arquivos de mainframe diretamente no Amazon S3.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) com uma sub-rede acessível por sua plataforma legada
- Um endpoint do Transfer Family para sua VPC
- Arquivos do Mainframe Virtual Storage Access Method (VSAM) convertidos em arquivos sequenciais de tamanho fixo (documentação da IBM)

Limitações

- O SFTP transfere arquivos no modo binário por definição, ou seja, os arquivos são enviados para o Amazon S3 com a codificação EBCDIC preservada. Se seu arquivo não contiver dados binários ou compactados, você poderá usar o subcomando sftp ascii (documentação da IBM) para converter seus arquivos em texto durante a transferência.
- Você deve descompactar arquivos de mainframe (Recomendações da AWS) que contenham conteúdo compactado e binário para usar esses arquivos em seu ambiente de destino.
- Os objetos do Amazon S3 podem variar em tamanho: de um mínimo de 0 byte a um máximo de 5 TB. Para obter mais informações sobre os recursos do Amazon S3, consulte Amazon S3. FAQs

Arquitetura

Pilha de tecnologia de origem

- Job Control Language (JCL)
- Shell z/OS Unix e ISPF
- SFTP
- VSAM e arquivos simples

Pilha de tecnologias de destino

- Transfer Family
- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)

Arquitetura de destino

O diagrama a seguir mostra uma arquitetura de referência para usar o Transfer Family com SFTP para carregar arquivos de mainframe diretamente em um bucket do S3.

O diagrama mostra o seguinte fluxo de trabalho:

1. Use uma tarefa de JCL para transferir seus arquivos de mainframe do mainframe herdado para a Nuvem AWS por meio do Direct Connect.
2. O Direct Connect permite que seu tráfego de rede permaneça na rede global da AWS e ignore a Internet pública. O Direct Connect também aumenta a velocidade da rede, começando em 50 Mbps e escalando até 100 Gbps.
3. O endpoint da VPC permite conexões entre os recursos da sua VPC e os serviços compatíveis sem usar a Internet pública. O acesso ao Transfer Family e ao Amazon S3 alcança alta disponibilidade por meio de interfaces de rede elástica localizadas em duas sub-redes privadas e zonas de disponibilidade.
4. O Transfer Family autentica os usuários e usa o SFTP para receber seus arquivos do ambiente herdado e movê-los para um bucket do S3.

Automação e escala

Depois que o serviço Transfer Family estiver em vigor, você poderá transferir um número ilimitado de arquivos do mainframe para o Amazon S3 usando uma tarefa de JCL como cliente SFTP. Você também pode automatizar a transferência de arquivos usando um agendador de tarefas em lote de mainframe para executar tarefas de SFTP quando for o momento de transferir os arquivos de mainframe.

Ferramentas

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.
- O AWS Transfer Family permite que você escale com segurança suas transferências recorrentes de business-to-business arquivos para o Amazon S3 e o Amazon EFS usando os protocolos SFTP, FTPS e FTP.

Épicos

Criar o bucket do S3 e a política de acesso

Tarefa	Descrição	Habilidades necessárias
Criar o bucket do S3.	Crie um bucket do S3 para hospedar os arquivos que você transfere do seu ambiente herdado.	AWS geral
Criar uma política e um perfil do IAM.	O Transfer Family usa seu perfil do AWS Identity and Access Management (IAM) para conceder acesso ao bucket do S3 criado anteriorm ente.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	Crie um perfil do IAM que inclua a seguinte política do IAM: `{ "Version": "2012-10-17", "Statement": [{ "Sid": "UserFolderListing", "Action": ["s3:ListBucket", "s3:GetBucketLocation"], "Effect": "Allow", "Resource": ["arn:aws:s3:::<your-bucket-name>"] }, { "Sid": "HomeDirObjectAccess", "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObjectAcl", "s3:GetObject",`	

Tarefa	Descrição	Habilidades necessárias

	<pre>"s3:DeleteObjectVersion",
	"s3:DeleteObject",
	"s3:PutObjectAcl",
	"s3:GetObjectVersion"
	],
	"Resource":
	"arn:aws:s3:::<your-bucket-name>/*"
	}
	]
	}</pre>
	Note
	Você deve escolher o caso de uso de transferência ao criar a função do IAM.	

Definir o serviço de transferência

Tarefa	Descrição	Habilidades necessárias
Crie o servidor SFTP.	1. Faça login no console de gerenciamento da AWS, abra o console do Transfer Family, e, em seguida, escolha Criar servidor. 2. Escolha somente SFTP (SSH File Transfer Protocol) – transferência	AWS geral

Tarefa	Descrição	Habilidades necessárias
	de arquivos pelo protocolo Secure Shell e, em seguida, Avançar. 3. Para o provedor de identidade, escolha Serviço gerenciado e, em seguida, escolha Próximo. 4. Em Tipo de endpoint, selecione VPC hospedada. 5. Em Acesso, escolha Interno. 6. Em VPC, escolha sua VPC. 7. Na seção Zonas de disponibilidade, escolha suas Zonas de Disponibilidade e sub-redes. 8. Na seção de Grupos de segurança, escolha seu grupo de segurança, e, em seguida, Próximo. 9. Em Domínio, escolha Amazon S3 e, em seguida, Avançar. 10. Mantenha as opções padrão na página Configurar detalhes adicionais e escolha Avançar. 11. Selecione Create server (Criar servidor).	

Tarefa	Descrição	Habilidades necessárias
	Note Para obter mais informações sobre como configurar um servidor SFTP, consulte Criar um servidor habilitado para SFTP (AWS Transfer Family User Guide).	
Obtenha o endereço do servidor.	1. Abra o console do Transfer Family e escolha o ID do servidor na coluna ID do servidor. 2. Na seção Detalhes do endpoint, em Tipo de endpoint, escolha o ID do endpoint. Isso leva você ao console do Amazon VPC. 3. Na guia Detalhes do console da Amazon VPC, encontre os nomes DNS ao lado dos Nomes DNS.	AWS geral
Crie o par de chaves do cliente SFTP.	Crie um par de chaves SSH para Microsoft Windows ou macOS/Linux/UNIX.	AWS geral, SSH

Tarefa	Descrição	Habilidades necessárias
Crie o servidor SFTP.	1. Abra o console do Transfer Family, escolha Servidores no painel de navegação e selecione seu servidor. 2. Na coluna ID do servidor, escolha o ID do servidor e, em seguida, Adicionar usuário. 3. Em Nome de usuário, insira um nome de usuário que corresponda ao par de chaves SSH. 4. Em Função, selecione o perfil do IAM que você criou anteriormente. 5. Em Diretório inicial, escolha o bucket do S3 criado anteriormente. 6. Em Chaves públicas SSH, insira o par de chaves criado anteriormente. 7. Escolha Adicionar.	AWS geral

Transferir o arquivo do mainframe

Tarefa	Descrição	Habilidades necessárias
Envie a chave privada SSH para o mainframe.	Use SFTP ou SCP para enviar a chave privada SSH para o ambiente herdado. Exemplo de SFTP:	Mainframe, shell Unix z/OS, FTP, SCP

Tarefa	Descrição	Habilidades necessárias

	`sftp [USERNAME@mainframeIP]`
	`[password]`
	`cd [/u/USERNAME]`
	`put [your-key-pair-file]`
	
	Exemplos de SCP:
	
	`scp [your-key-pair-file] [USERNAME@MainframeIP]:/[u/USERNAME]`
	
	Em seguida, armazene a chave SSH no sistema de arquivos z/OS Unix sob o nome de usuário que posteriormente executará a tarefa em lote da transferência de arquivos (por exemplo, `/u/CONTROLM`).
	
	Note
	Para obter mais informações sobre o shell z/OS Unix, consulte Uma introdução aos shells z/OS (documentação da IBM).	

Tarefa	Descrição	Habilidades necessárias

Crie o cliente JCL SFTP.	Como os mainframes não têm um cliente SFTP nativo, você deve usar o utilitário BPXBATCH para executar o cliente SFTP a partir do shell z/OS Unix.
	
	No editor ISPF, crie o cliente JCL SFTP. Por exemplo:
	
	`//JOBNAM JOB ...`
	`//************`
	`******************`
	`******************`
	`******************`
	`****`
	`//SFTP EXEC PGM=BPXBA`
	`TCH,REGION=0M`
	`//STDPARM DD *`
	`SH cp "//'MAINF`
	`RAME.FILE.NAME'"`
	` filename.txt;`
	`echo 'put filename.txt'`
	` > uplcmd;`
	`sftp -b uplcmd -i`
	` ssh_private_key_fi`
	`le ssh_username@<tran`
	`sfer service ip or`
	` DNS>;`
	`//SYSPRINT DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`//STDERR DD SYSOUT=*`
	
	Note
	Para obter mais informações sobre como executar um
		JCL, Mainframe, shell Unix z/OS

Tarefa	Descrição	Habilidades necessárias
	comando no shell do z/OS Unix, consulte O utilitário BPXBATCH (documentação da IBM). Para obter mais informações sobre como criar ou editar tarefas de JCL no z/OS, consulte O que é ISPF? e O editor ISPF (documentação da IBM).	
Execute o cliente JCL SFTP.	1. No editor ISPF, digite SUB e, em seguida, pressione a tecla ENTER após a criação da tarefa de JCL. 2. Monitore a atividade da tarefa em lotes de transferência de arquivos do mainframe no SDSF. **Note** Para obter mais informações sobre como verificar a atividade de trabalhos em lotes, consulte o Guia do Usuário do z/OS SDSF (documentação da IBM).	Mainframe, JCL, ISPF

Tarefa	Descrição	Habilidades necessárias
Validar a transferência de arquivos.	1. Faça login no console de gerenciamento da AWS, abra o Console do Amazon S3 e escolha Buckets no painel de navegação. 2. Escolha o bucket associado ao seu Transfer Family. 3. Na seção Objetos da guia Objetos, localize o arquivo que você transferiu do mainframe.	AWS geral
Crie o cliente JCL SFTP.	Use o agendador de tarefas para acionar automaticamente o cliente JCL SFTP. **Note** Você pode usar agendadores de tarefas de mainframe , como BMC Control-M ou CA Workload Automation, para automatizar trabalhos em lotes para transferências de arquivos com base no tempo e em outras dependências de trabalhos em lotes.	Agendador de tarefas

Recursos relacionados

- Como o AWS Transfer Family funciona
- Modernização do mainframe com a AWS

Proteja e simplifique o acesso de usuários em um banco de dados de federação Db2 na AWS usando contextos confiáveis

Criado por Sai Parthasaradhi (AWS)

Resumo

Muitas empresas estão migrando suas workloads de mainframe antigas para a Amazon Web Services (AWS). Essa migração inclui a transferência de bancos de dados IBM Db2 for z/OS para Db2 for Linux, Unix e Windows (LUW) na Amazon Elastic Compute Cloud (Amazon). EC2 Durante uma migração em fases do local para a AWS, talvez os usuários precisem acessar dados no IBM Db2 z/OS e no Db2 LUW na EC2 Amazon até que todos os aplicativos e bancos de dados sejam totalmente migrados para o Db2 LUW. Nesses cenários de acesso remoto a dados, a autenticação do usuário pode ser um desafio porque plataformas diferentes usam mecanismos de autenticação diferentes.

Esse padrão aborda como configurar um servidor de federação no Db2 para LUW com o Db2 para z/OS como um banco de dados remoto. O padrão usa um contexto confiável para propagar a identidade de um usuário do Db2 LUW para o Db2 z/OS sem precisar se autenticar novamente no banco de dados remoto. Para obter mais informações sobre contextos confiáveis, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância do Db2 em execução em uma instância da Amazon EC2
- Um banco de dados Db2 for z/OS remoto executado on-premises
- A rede local conectada à AWS por meio do AWS Site-to-SiteVPN ou do AWS Direct Connect

Arquitetura

Arquitetura de destino

Ferramentas

Serviços da AWS

- A Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável na Nuvem AWS. Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O AWS Site-to-Site VPN ajuda você a transmitir tráfego entre instâncias que você executa na AWS e sua própria rede remota.

Outras ferramentas

- db2cli é o comando interface de linha de comandos (CLI) do Db2.

Épicos

Habilite a federação no banco de dados Db2 LUW executado na AWS

Tarefa	Descrição	Habilidades necessárias
Habilite a federação no DB2 LUW DB.	Para habilitar a federação no DB2 LUW, execute o comando a seguir. `update dbm cfg using federated YES`	DBA
Reinicie o banco de dados.	Para reiniciar o banco de dados, execute o seguinte comando: `db2stop force; db2start;`	DBA

Catalogue o banco de dados remoto

Tarefa	Descrição	Habilidades necessárias
Catalogue o subsistema Db2 z/OS remoto.	Para catalogar o banco de dados remoto do Db2 z/OS no	DBA

Tarefa	Descrição	Habilidades necessárias
	Db2 LUW executado na AWS, use o seguinte exemplo de comando. `catalog TCPIP NODE tcpnode REMOTE mainframehost SERVER mainframeport`	
Catalogue o banco de dados remoto	Para excluir um banco de dados remoto, use o seguinte comando de exemplo. `catalog db dbnam1 as ndbnam1 at node tcpnode`	DBA

Crie a definição de servidor remoto

Tarefa	Descrição	Habilidades necessárias
Colete as credenciais do usuário para o banco de dados remoto do Db2 z/OS.	Antes de prosseguir com as próximas etapas, reúna as seguintes informações: • Nome do subsistema Db2 z/OS: o nome catalogado do Db2 z/OS no LUW da etapa anterior (por exemplo, `ndbnam1`) • Versão do Db2 z/OS: a versão do subsistema do Db2 z/OS (por exemplo, `12`) • ID de usuário do Db2 z/OS: o usuário com o privilégio BIND, necessário para	DBA

Tarefa	Descrição	Habilidades necessárias
	criar somente a definição do servidor (por exemplo, `dbuser1`) • Senha do Db2 z/OS: a senha para `dbuser1` (por exemplo, `dbpasswd`) • Usuário proxy do Db2 z/OS: o ID do usuário proxy, que será usado para estabelecer uma conexão confiável (por exemplo, `zproxy`) • Senha do proxy do Db2 z/OS: a senha do usuário `zproxy` (por exemplo, `zproxy`)	
Crie o encapsulamento do DRDA.	Para criar o encapsulamento do DRDA, execute o seguinte comando. `CREATE WRAPPER DRDA;`	DBA

Tarefa	Descrição	Habilidades necessárias
Crie a definição do servidor.	Para criar a definição do servidor, execute o comando de exemplo a seguir. `CREATE SERVER ndbserver TYPE DB2/ZOS VERSION 12 WRAPPER DRDA AUTHORIZATION "dbuser1" PASSWORD "dbpasswd " OPTIONS ( DBNAME 'ndbnam1',FED_PROXY_USER 'ZPROXY' );` Nessa definição, `FED_PROXY_USER` especifica o usuário proxy que será usado para estabelecer conexões confiáveis com o banco de dados Db2 z/OS. O ID de usuário e a senha de autorização são necessários somente para criar o objeto de servidor remoto no banco de dados Db2 LUW. Eles não serão usados posteriormente durante o runtime.	DBA

Crie mapeamentos de usuários

Tarefa	Descrição	Habilidades necessárias
Crie um mapeamento de usuário para o usuário proxy.	Para criar um mapeamento de usuário para o usuário do proxy, execute o comando a seguir.	DBA

Tarefa	Descrição	Habilidades necessárias
	`CREATE USER MAPPING FOR ZPROXY SERVER ndbserver OPTIONS (REMOTE_AUTHID 'ZPROXY', REMOTE_PASSWORD 'zproxy');`	
Crie mapeamentos de usuário para cada usuário no Db2 LUW.	Crie mapeamentos de usuário para todos os usuários no banco de dados Db2 LUW na AWS que precisam acessar dados remotos por meio do usuário proxy. Para criar os mapeamentos de usuário, execute o seguinte comando. `CREATE USER MAPPING FOR PERSON1 SERVER ndbserver OPTIONS (REMOTE_AUTHID 'USERZID', USE_TRUSTED_CONTEXT 'Y');` A declaração especifica que um usuário no Db2 LUW (`PERSON1`) pode estabelecer uma conexão confiável com o banco de dados remoto do Db2 z/OS (`USE_TRUSTED_CONTEXT 'Y'`). Depois que a conexão é estabelecida por meio do usuário proxy, o usuário pode acessar os dados usando o ID de usuário do Db2 z/OS (`REMOTE_AUTHID 'USERZID'`).	DBA

Crie o objeto de contexto confiável

Tarefa	Descrição	Habilidades necessárias

Crie o objeto de contexto confiável.	Para criar o objeto de contexto confiável no banco de dados remoto do Db2 z/OS, use o comando de exemplo a seguir.
	
	`CREATE TRUSTED CONTEXT`
	`CTX_LUW_ZOS`
	`BASED UPON CONNECTIO`
	`N USING SYSTEM AUTHID`
	`ZPROXY`
	`ATTRIBUTES (`
	`ADDRESS '10.10.10.10'`
	`)`
	`NO DEFAULT ROLE`
	`ENABLE`
	`WITH USE FOR PUBLIC`
	`WITHOUT AUTHENTIC`
	`ATION;`
	
	Nessa definição, `CTX_LUW_Z0S` é um nome arbitrário para o objeto de contexto confiável. O objeto contém o ID do usuário do proxy e o endereço IP do servidor do qual a conexão confiável deve se originar. Neste exemplo, o servidor é o banco de dados Db2 LUW na AWS. Você pode usar o nome do domínio em vez do endereço IP. A cláusula `WITH USE FOR PUBLIC WITHOUT AUTHENTICATION` indica que a troca da ID de usuário
		DBA

Tarefa	Descrição	Habilidades necessárias
	em uma conexão confiável é permitida para cada ID de usuário. Não é necessário fornecer uma senha.	

Recursos relacionados

- IBM Resource Access Control Facility (RACF)
- Federação IBM Db2 LUW
- Contextos confiáveis

Mais informações

Contextos confiáveis do Db2

Um contexto confiável é um objeto de banco de dados Db2 que define uma relação de confiança entre um servidor federado e um servidor de banco de dados remoto. Para definir um relacionamento confiável, o contexto confiável especifica atributos de confiança. Existem três tipos de atributos de confiança:

- A ID de autorização do sistema que faz a solicitação inicial de conexão com o banco de dados
- O endereço IP ou nome de domínio a partir do qual a conexão é feita
- A configuração de criptografia para comunicações de dados entre o servidor do banco de dados e o cliente do banco de dados

Uma conexão confiável é estabelecida quando todos os atributos de uma solicitação de conexão correspondem aos atributos especificados em qualquer objeto de contexto confiável definido no servidor. Existem dois tipos de conexões confiáveis: implícitas e explícitas. Depois que uma conexão confiável implícita é estabelecida, o usuário herda uma função que não está disponível para ele fora do escopo dessa definição de conexão confiável. Depois que uma conexão confiável explícita é estabelecida, os usuários podem ser ativados na mesma conexão física, com ou sem autenticação. Além disso, os usuários do Db2 podem receber funções que especificam privilégios que devem ser usados somente na conexão confiável. Esse padrão usa uma conexão confiável explícita.

Contexto confiável nesse padrão

Após a conclusão do padrão, PERSON1 no Db2, o LUW acessa dados remotos do Db2 z/OS usando um contexto confiável federado. A conexão para PERSON1 é estabelecida por meio de um usuário proxy se a conexão for originada do endereço IP ou nome de domínio especificado na definição de contexto confiável. Depois que a conexão é estabelecida, o ID de usuário PERSON1 do Db2 z/OS correspondente é trocado sem reautenticação, e o usuário pode acessar os dados ou objetos com base nos privilégios do Db2 configurados para esse usuário.

Benefícios dos contextos federados confiáveis

- Essa abordagem mantém o princípio do privilégio mínimo ao eliminar o uso de um ID de usuário ou ID de aplicativo comum que precisaria de um superconjunto de todos os privilégios exigidos por todos os usuários.
- A identidade real do usuário que realiza a transação no banco de dados federado e remoto é sempre conhecida e pode ser auditada.
- O desempenho melhora porque a conexão física está sendo reutilizada entre os usuários sem a necessidade de reautenticação do servidor federado.

Transferir dados do Db2 z/OS em grande escala para o Amazon S3 em arquivos CSV

Criado por Bruno Sahinoglu (AWS), Ivan Schuster (AWS) e Abhijit Kshirsagar (AWS)

Resumo

Um mainframe ainda é um sistema de registro em muitas empresas que contém uma grande quantidade de dados, incluindo entidades de dados mestres com registros de transações comerciais atuais e históricas. Geralmente é isolado e não é facilmente acessado pelos sistemas distribuídos dentro da mesma empresa. Com o surgimento da tecnologia de nuvem e a democratização de big data, as empresas estão interessadas em usar os insights ocultos nos dados do mainframe para desenvolver novos recursos de negócios.

Com esse objetivo, as empresas estão procurando abrir seus dados Db2 de mainframe em seu ambiente de nuvem da Amazon Web Services (AWS). Os motivos comerciais são diversos e os métodos de transferência variam de caso a caso. Talvez você prefira conectar seu aplicativo diretamente ao mainframe ou talvez prefira replicar seus dados quase em tempo real. Se o caso de uso for alimentar um data warehouse ou um data lake, ter uma up-to-date cópia não é mais uma preocupação, e o procedimento descrito nesse padrão pode ser suficiente, especialmente se você quiser evitar custos de licenciamento de produtos de terceiros. Outro caso de uso pode ser a transferência de dados do mainframe para um projeto de migração. Em um cenário de migração, os dados são necessários para realizar o teste de equivalência funcional. A abordagem descrita nesta postagem é uma forma econômica de transferir os dados do Db2 para o ambiente de Nuvem AWS.

Como o Amazon Simple Storage Service (Amazon S3) é um dos serviços mais integrados da AWS, você pode acessar os dados de lá e coletar insights diretamente usando outros serviços da AWS, como Amazon Athena, funções do AWS Lambda ou Amazon. QuickSight Você também pode carregar os dados no Amazon Aurora ou no Amazon DynamoDB usando o AWS Glue ou o AWS Database Migration Service (AWS DMS). Com esse objetivo em mente, isso descreve como descarregar dados do Db2 em arquivos CSV no formato ASCII no mainframe e transferir os arquivos para o Amazon S3.

Para esse fim, scripts de mainframe foram desenvolvidos para ajudar a gerar linguagens de controle de tarefas (JCLs) para descarregar e transferir quantas tabelas do Db2 forem necessárias.

Pré-requisitos e limitações

Pré-requisitos

- Um usuário do sistema operacional IBM z/OS com autorização para executar scripts Restructured Extended Executor (REXX) e JCL.
- Acesso ao z/OS Unix System Services (USS) para gerar chaves públicas e privadas SSH (Secure Shell).
- Um bucket do S3 gravável. Para obter mais informações, consulte Criar um bucket do S3 na documentação do Amazon S3.
- Um servidor habilitado para o AWS Transfer Family SSH File Transfer Protocol (SFTP) usando o serviço gerenciado como provedor de identidade e o Amazon S3 como serviço de armazenamento da AWS. Para obter mais informações, consulte Criar um servidor habilitado para SFTP na documentação do AWS Transfer Family.

Limitações

- Essa abordagem não é adequada para sincronização de dados quase em tempo real ou em tempo real.
- Os dados só podem ser movidos do Db2 z/OS para o Amazon S3, e não o contrário.

Arquitetura

Pilha de tecnologia de origem

- Mainframe executando Db2 em z/OS

Pilha de tecnologias de destino

- AWS Transfer Family
- Amazon S3
- Amazon Athena
- Amazon QuickSight
- AWS Glue
- Amazon Relational Database Service (Amazon RDS)
- Amazon Aurora
- Amazon Redshift

Arquitetura de origem e destino

O diagrama a seguir mostra o processo de geração, extração e transferência de dados do Db2 z/OS no formato ASCII CSV para um bucket do S3.

1. Uma lista de tabelas é selecionada para migração de dados do catálogo do Db2.
2. A lista é usada para impulsionar a geração de trabalhos de descarga com as colunas numéricas e de dados no formato externo.
3. Em seguida, os dados são transferidos para o Amazon S3 usando o AWS Transfer Family.
4. Uma tarefa de extração, transformação e carregamento (ETL) do AWS Glue pode transformar os dados e carregá-los em um bucket processado no formato especificado, ou o AWS Glue pode alimentar os dados diretamente no banco de dados.
5. O Amazon Athena e o Amazon QuickSight podem ser usados para consultar e renderizar os dados para impulsionar a análise.

O diagrama a seguir mostra um fluxo lógico de todo o processo.

1. O primeiro JCL, chamado TABNAME, usará o utilitário DSNTIAUL do Db2 para extrair e gerar a lista de tabelas que você planeja descarregar do Db2. Para escolher suas tabelas, você deve adaptar manualmente a entrada SQL para selecionar e adicionar critérios de filtro para incluir um ou mais esquemas do Db2.
2. O segundo JCL, chamado REXXEXEC, usará o esqueleto JCL e o programa REXX fornecido para processar a lista de tabelas criada pelo JCL TABNAME e gerar um JCL por nome de tabela. Cada JCL conterá uma etapa para descarregar a tabela e outra etapa para enviar o arquivo para o bucket do S3 usando o protocolo SFTP.
3. A última etapa consiste em executar o JCL para descarregar a tabela e transferir o arquivo para a AWS. Todo o processo pode ser automatizado usando um programador on-premises ou na AWS.

Ferramentas

Serviços da AWS

- O Amazon Athena é um serviço de consultas interativas que permite analisar dados diretamente no Amazon Simple Storage Service (Amazon S3) usando SQL padrão.

- O Amazon Aurora é um mecanismo de banco de dados relacional totalmente gerenciado criado para a nuvem e compatível com o MySQL e o PostgreSQL.
- O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar de forma confiável, limpar, enriquecer e mover dados de forma confiável entre armazenamento de dados e fluxos de dados.
- QuickSightA Amazon é um serviço de inteligência de negócios (BI) em escala de nuvem que ajuda você a visualizar, analisar e relatar seus dados em um único painel.
- O Amazon Redshift é um serviço de data warehouse em escala de petabytes gerenciado na Nuvem AWS.
- O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados relacional na Nuvem AWS.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Transfer Family é um serviço de transferência seguro que permite transferir arquivos para dentro e para fora de serviços de armazenamento da AWS.

Ferramentas de mainframe

- O SSH File Transfer Protocol (SFTP) é um protocolo seguro de transferência de arquivos que permite o login remoto e a transferência de arquivos entre servidores. O SSH fornece segurança criptografando todo o tráfego.
- O DSNTIAUL é um programa de exemplo fornecido pela IBM para descarregar dados.
- O DSNUTILB é um programa de utilitários em lote fornecido pela IBM para descarregar dados com opções diferentes do DSNTIAUL.
- O z/OS OpenSSH é uma porta de SSH de software de código aberto executada no Unix System Service sob o sistema operacional IBM z/OS. O SSH é um programa de conexão segura e criptografada entre dois computadores em execução em uma rede TCP/IP. Ele fornece vários utilitários, incluindo ssh-keygen.
- O script REXX (Restructured Extended Executor) é usado para automatizar a geração de JCL com as etapas Db2 Unload e SFTP.

Código

O código desse padrão está disponível no repositório GitHub unloaddb2.

Práticas recomendadas

Para o primeiro descarregamento, o gerado JCLs deve descarregar todos os dados da tabela.

Após o primeiro descarregamento completo, execute descargas incrementais para obter melhor desempenho e economia de custos. Atualize a consulta SQL no conjunto de modelos da JCL para acomodar quaisquer alterações no processo de descarga.

Você pode converter o esquema manualmente ou usando um script no Lambda com o Db2 SYSPUNCH como entrada. Para um processo industrial, a AWS Schema Conversion Tool (SCT) é a opção preferida.

Por fim, use um programador baseado em mainframe ou um programador na AWS com um agente no mainframe para ajudar a gerenciar e automatizar todo o processo.

Épicos

Configurar o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Para obter instruções, consulte Criar seu primeiro bucket do S3.	AWS geral

Configurar o servidor Transfer Family

Tarefa	Descrição	Habilidades necessárias
Criar um servidor habilitado para SFTP.	Para abrir e criar um servidor SFTP no console do AWS Transfer Family, faça o seguinte: 1. Na página Escolher protocolos, marque a caixa de seleção SFTP (SSH File Transfer Protocol) –	AWS geral

Tarefa	Descrição	Habilidades necessárias
	transferência de arquivos pelo Secure Shell. 2. Para o provedor de identidade, escolha Serviço gerenciado. 3. Para endpoint, escolha Publicamente acessível. 4. Para o domínio, escolha Amazon S3. 5. Na página Configura r detalhes adicionais, mantenha as configurações padrão. 6. Criar o servidor.	
Criar um perfil do IAM para o Transfer Family.	Para criar um perfil do AWS Identity and Access Management (IAM) para que a Transfer Family acesse o Amazon S3, siga as instruçõe s em Criar um perfil e uma política do IAM.	Administrador da AWS
Adicionar um usuário gerenciado por serviços do Amazon S3.	Para adicionar o usuário gerenciado pelo serviço Amazon S3, siga as instruçõe s na Documentação da AWS e use seu ID do usuário do mainframe.	AWS geral

Proteger o protocolo de comunicação

Tarefa	Descrição	Habilidades necessárias
Criar a chave SSH.	No ambiente do USS do mainframe, execute o comando a seguir. `ssh-keygen -t rsa` **Note** Quando for solicitad a uma frase secreta, mantenha-a vazia.	Desenvolvedor de mainframe

Fornecer os níveis de autorização corretos para a pasta SSH e os arquivos-chave.	Por padrão, as chaves pública e privada serão armazenad as no diretório do usuário `/u/home/username/.ssh` .
	Você deve dar a autorização 644 para os arquivos de chave e 700 para a pasta.
	`chmod 644 .ssh/id_rsa`
	`chmod 700 .ssh`
		Desenvolvedor de mainframe

Copiar o conteúdo da chave pública para seu usuário gerenciado pelo serviço Amazon S3.	Para copiar o conteúdo da chave pública gerada pelo USS, abra o console do AWS Transfer Family. 1. No painel de navegação, selecione Servidores. 2. Escolha o identificador na coluna ID do servidor para	Desenvolvedor de mainframe

Tarefa	Descrição	Habilidades necessárias
	consultar os Detalhes do servidor 3. Em Usuários, escolha um nome de usuário para consultar a página de Detalhes do usuário. 4. Em Chave pública SSH, escolha Adicionar chave pública SSH para adicionar uma nova chave pública a um usuário. Para a chave pública SSH, insira sua chave pública. Sua chave é validada pelo serviço antes que você possa adicionar seu novo usuário. 5. Escolha Adicionar chave.	

Gere o JCLs

Tarefa	Descrição	Habilidades necessárias
Gerar a lista de tabelas do Db2 dentro do escopo.	Forneça o SQL de entrada para criar uma lista das tabelas que têm como escopo a migração de dados. Essa etapa exige que você especifique os critérios de seleção consultando a tabela do catálogo Db2 SYSIBM.SYSTABLES, usando uma cláusula WHERE do SQL. Os filtros podem ser personalizados para incluir um	Desenvolvedor de mainframe

Tarefa	Descrição	Habilidades necessárias
	esquema específico ou nomes de tabelas que comecem com um prefixo específico ou com base em um timestamp para descarga incremental. A saída é capturada em um conjunto de dados sequencial físico (PS) no mainframe. Esse conjunto de dados funcionará como entrada para a próxima fase da geração do JCL. Antes de usar o JCL TABNAME (você pode renomeá-lo se necessário), faça as seguintes alterações: 1. Substitua <Jobcard> por uma classe de trabalho e um usuário autorizado a executar utilitários do Db2. 2. Substitua < HLQ1 > ou personalize os nomes dos conjuntos de dados de saída para atender aos padrões do seu site. 3. Atualize a pilha STEPLIB de PDSEs (conjunto de dados particionado estendido) de acordo com os padrões do seu site. O exemplo desse padrão usa os padrões da IBM.	

Tarefa	Descrição	Habilidades necessárias

	4. Substitua o nome do plano e LIB pelos valores específicos da instalação.
	5. Substitua <Esquema> e <Prefixo> com seus critérios de seleção pelo catálogo do Db2.
	6. Salve o JCL resultant e em uma biblioteca PDS (conjunto de dados particionado).
	7. Envie a JCL.
	
	Trabalho de extração da lista de tabelas do Db2
	
	`<Jobcard>`
	`//*`
	`//* UNLOAD ALL THE TABLE NAMES FOR A PARTICULAR SCHEMA`
	`//*`
	`//STEP01 EXEC PGM=IEFBR14`
	`//*`
	`//DD1 DD DISP=(MOD,DELETE,DELETE),`
	`// UNIT=SYSDA,`
	`// SPACE=(1000,(1,1)),`
	`// DSN=<HLQ1>.DSN81210.TABLIST`
	`//*`
	`//DD2 DD DISP=(MOD,DELETE,DELETE),`
	`// UNIT=SYSDA,`	

Tarefa	Descrição	Habilidades necessárias

	`//  SPACE=(1000,(1,1)),`
	`//  DSN=<HLQ1>.DSN81210.SYSPUNCH`
	`//*`
	`//UNLOAD  EXEC PGM=IKJEFT01,DYNAMNBR=20`
	`//SYSTSPRT DD SYSOUT=*`
	`//STEPLIB  DD DISP=SHR,DSN=DSNC10.DBCG.SDSNEXIT`
	`//  DD  DISP=SHR,DSN=DSNC10.SDSNLOAD`
	`//  DD  DISP=SHR,DSN=CEE.SCEERUN`
	`//  DD  DISP=SHR,DSN=DSNC10.DBCG.RUNLIB.LOAD`
	`//SYSTSIN  DD  *`
	`  DSN SYSTEM(DBCG)`
	`  RUN  PROGRAM(DSNTIAUL) PLAN(DSNTIB12) PARMS('SQL') -`
	`  LIB('DSNC10.DBCG.RUNLIB.LOAD')`
	`  END`
	`//SYSPRINT DD SYSOUT=*`
	`//*`
	`//SYSUDUMP DD SYSOUT=*`
	`//*`
	`//SYSREC00 DD DISP=(NEW,CATLG,DELETE),`
	`//  UNIT=SYSDA,SPACE=(32760,(1000,500)),`
	`//  DSN=<HLQ1>.DSN81210.TABLIST`
	`//*`
	`//SYSPUNCH DD DISP=(NEW,CATLG,DELETE),`	

Tarefa	Descrição	Habilidades necessárias

	<pre>// UNIT=SYSD
	A,SPACE=(32760,(10
	00,500)),
	// VOL=SER=S
	CR03,RECFM=FB,LREC
	L=120,BLKSIZE=12
	// DSN=<HLQ1
	>.DSN81210.SYSPUNCH
	//*
	//SYSIN DD *
	   SELECT CHAR(CREA
	TOR), CHAR(NAME)
	     FROM SYSIBM.SY
	STABLES
	    WHERE OWNER =
	 '<Schema>'
	      AND NAME LIKE
	 '<Prefix>%'
	      AND TYPE = 'T';
	/*</pre>	

Tarefa	Descrição	Habilidades necessárias
Modificar os modelos da JCL.	Os modelos JCL fornecidos com esse padrão contêm um cartão de trabalho genérico e nomes de bibliotecas. No entanto, a maioria dos sites de mainframe terá seus próprios padrões de nomenclatura para nomes do conjunto de dados, nomes de bibliotec as e cartões de trabalho. Por exemplo, uma classe de trabalho específica pode ser necessária para executar trabalhos do Db2. O Job Entry Subsytem é implement ado JES2 e JES3 pode impor mudanças adicionai s. As bibliotecas de carga padrão podem ter um primeiro qualificador diferente de SYS1, que é o padrão da IBM. Portanto, personalize os modelos de acordo com os padrões específicos do seu site antes de executá-los. Faça as seguintes alterações no esqueleto JCL UNLDSKEL: 1. Modifique o cartão de trabalho por uma classe de trabalho e um usuário autorizado a executar utilitários do Db2.	Desenvolvedor de mainframe

Tarefa	Descrição	Habilidades necessárias
	2. Personalize os nomes do conjunto de dados de saída para atender aos padrões do seu site. 3. Atualize a pilha STEPLIB de PDSEs acordo com os padrões do seu site. O exemplo desse padrão usa os padrões da IBM. 4. Substitua <DSN> pelo seu nome do subsistema e ID de correlação do Db2. 5. Salve o JCL resultante em uma biblioteca PDS que faz parte da sua pilha ISPSLIB, que é a bibliotec a de modelos de esqueleto padrão para o ISPF. Esqueleto JCL de descarga e SFTP `//&USRPFX.U JOB (DB2UNLOAD),'JOB', CLASS=A,MSGCLASS=A, //  TIME=1440 ,NOTIFY=&USRPFX //* DELETE DATASETS //STEP01  EXEC PGM=IEFBR14 //DD01  DD DISP=(MOD ,DELETE,DELETE), //  UNIT=SYSD A, //  SPACE=(TR K,(1,1)),`	

Tarefa	Descrição	Habilidades necessárias

	`// DSN=&USRPFX..DB2.PUNCH.&JOBNAME`
	`//DD02 DD DISP=(MOD,DELETE,DELETE),`
	`// UNIT=SYSDA,`
	`// SPACE=(TRK,(1,1)),`
	`// DSN=&USRPFX..DB2.UNLOAD.&JOBNAME`
	`//*`
	`//* RUNNING DB2 EXTRACTION BATCH JOB FOR AWS DEMO`
	`//*`
	`//UNLD01 EXEC PGM=DSNUTILB,REGION=0M,`
	`// PARM='<DSN>,UNLOAD'`
	`//STEPLIB DD DISP=SHR,DSN=DSNC10.DBCG.SDSNEXIT`
	`// DD DISP=SHR,DSN=DSNC10.SDSNLOAD`
	`//SYSPRINT DD SYSOUT=*`
	`//UTPRINT DD SYSOUT=*`
	`//SYSOUT DD SYSOUT=*`
	`//SYSPUN01 DD DISP=(NEW,CATLG,DELETE),`
	`// SPACE=(CYL,(1,1),RLSE),`
	`// DSN=&USRPFX..DB2.PUNCH.&JOBNAME`
	`//SYSREC01 DD DISP=(NEW,CATLG,DELETE),`
	`// SPACE=(CYL,(10,50),RLSE),`
	`// DSN=&USRPFX..DB2.UNLOAD.&JOBNAME`
	`//SYSPRINT DD SYSOUT=*`	

Tarefa	Descrição	Habilidades necessárias

	`//SYSIN DD *`
	`UNLOAD`
	`DELIMITED COLDEL ','`
	`FROM TABLE &TABNAME`
	`UNLDDN SYSREC01`
	`PUNCHDDN SYSPUN01`
	`SHRLEVEL CHANGE`
	`ISOLATION UR;`
	`/*`
	`//*`
	`//* FTP TO AMAZON S3`
	`BACKED FTP SERVER IF`
	`UNLOAD WAS SUCCESSFUL`
	`//*`
	`//SFTP EXEC PGM=BPXBA`
	`TCH,COND=(4,LE),RE`
	`GION=0M`
	`//STDPARM DD *`
	`SH cp "//'&USRP`
	`FX..DB2.UNLOAD.&JO`
	`BNAME'"`
	`&TABNAME..csv;`
	`echo "ascii`
	`" >> uplcmd;`
	`echo "PUT &TABNAME.`
	`.csv " >>>> uplcmd;`
	`sftp -b uplcmd -i .ssh/`
	`id_rsa &FTPUSER.`
	`@&FTPSITE;`
	`rm &TABNAME..csv;`
	`//SYSPRINT DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`//STDERR DD SYSOUT=*`	

Tarefa	Descrição	Habilidades necessárias
Gerar o JCL de descarga em massa.	Essa etapa envolve a execução de um script REXX em um ambiente ISPF usando JCL. Forneça a lista de tabelas dentro do escopo criadas na primeira etapa como entrada para a geração de JCL em massa em relação ao nome `TABLIST DD`. O JCL gerará um novo JCL por nome de tabela em um conjunto de dados particion ado especificado pelo usuário em relação ao nome `ISPFILE DD`. Aloque essa bibliotec a com antecedência. Cada novo JCL terá duas etapas: uma etapa para descarregar a tabela Db2 em um arquivo e uma etapa para enviar o arquivo para o bucket do S3. Faça as seguintes alteraçõe s no JCL REXXEXEC (você pode alterar o nome): 1. Substitua `Job card user ID` por um ID de usuário de mainframe que tenha autoridade de descarga nas tabelas. Substitua o valor `SYSPROC`, `ISPPLIB`, `ISPSLIB`, `ISPMLIB`, e `ISPTLIB` `<HLQ1>` ou personalize o `DSN` para	Desenvolvedor de mainframe

Tarefa	Descrição	Habilidades necessárias
	atender aos padrões do seu site. Para descobrir os valores específicos da instalação, você usa o comando `TSO ISRDDN`. 2. Substitua `<MFUSER>` por um ID de usuário que tenha privilégios de execução de trabalhos em sua instalaçã o. 3. Substitua `<FTPUSER>` por um ID do usuário que tenha privilégios USS e FTP em sua instalação. Supõe-se que esse ID do usuário e suas chaves de segurança SSH estejam no diretório apropriado do Unix Systems Services no mainframe. 4. Substitua `<AWS TransferFamily IP>` pelo endereço IP do AWS Transfer Family ou pelo nome do domínio. Esse endereço será usado para a etapa SFTP. 5. Envie o JCL após aplicar a acomodação padrão do site e atualizar o programa REXX conforme descrito abaixo.	

Tarefa	Descrição	Habilidades necessárias

	Trabalho de geração de JCL em massa
	
	`//RUNREXX JOB (CREATEJCL),'RUNS ISPF TABLIST', CLASS=A,MSGCLASS=A,`
	
	`//  TIME=1440 ,NOTIFY=&SYSUID`
	`//* Most of the values required can be updated to your site specific`
	`//* values using the command 'TSO ISRDDN' in your ISPF session.`
	`//* Update all the lines tagged with //update marker to desired`
	`//* site specific values.`
	`//ISPF EXEC PGM=IKJEFT01,REGION=2048K,DYNAMNBR=25`
	`//SYSPROC DD DISP=SHR,DSN=USER.Z23D.CLIST`
	`//SYSEXEC DD DISP=SHR,DSN=<HLQ1>.TEST.REXXLIB`
	`//ISPPLIB DD DISP=SHR,DSN=ISP.SISPPENU`
	`//ISPSLIB DD DISP=SHR,DSN=ISP.SISPSENU`
	`//  DD DISP=SHR,DSN=<HLQ1>.TEST.ISPSLIB`
	`//ISPMLIB DD DSN=ISP.SISPMENU,DISP=SHR`	

Tarefa	Descrição	Habilidades necessárias

	`//ISPTLIB DD`
	` DDNAME=ISPTABL`
	`//  DD DSN=ISP.S`
	`ISPTENU,DISP=SHR`
	`//ISPTABL DD`
	` LIKE=ISP.SISPTENU,`
	`UNIT=VIO`
	`//ISPPROF DD`
	` LIKE=ISP.SISPTENU,`
	`UNIT=VIO`
	`//ISPLOG DD`
	` SYSOUT=*,RECFM=VA,`
	`LRECL=125`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSPRT DD`
	` SYSOUT=*`
	`//SYSUDUMP DD`
	` SYSOUT=*`
	`//SYSDBOUT DD`
	` SYSOUT=*`
	`//SYSTSPRT DD`
	` SYSOUT=*`
	`//SYSUDUMP DD`
	` SYSOUT=*`
	`//SYSDBOUT DD`
	` SYSOUT=*`
	`//SYSHELP DD`
	` DSN=SYS1.HELP,DISP`
	`=SHR`
	`//SYSOUT DD SYSOUT=*`
	`//* Input list of`
	` tablenames`
	`//TABLIST DD`
	` DISP=SHR,DSN=<HLQ1`
	`>.DSN81210.TABLIST`
	`//* Output pds`
	`//ISPFILE DD`
	` DISP=SHR,DSN=<HLQ1`
	`>.TEST.JOBGEN`
	`//SYSTSIN DD *`	

Tarefa	Descrição	Habilidades necessárias
	``` ISPSTART CMD(ZSTEPS <MFUSER> <FTPUSER> <AWS TransferFamily IP>) /* ```	
	Antes de usar o script REXX, faça as seguintes alterações: 1. Salve o script REXX em uma biblioteca PDS definida na pilha `SYSEXEC` no JCL REXXEXEC editado na etapa anterior com ZSTEPS como nome do membro. Se quiser renomeá-lo, você deve atualizar o JCL para acomodar as suas necessidades. 2. Esse script usa a opção trace para imprimir informações adicionais caso haja erros. Em vez disso, você pode adicionar o código de tratamento de erros após as instruções `EXECIO`, `ISPEXEC` e `TSO`, e remover a linha de rastreamento. 3. Esse script gera nomes do membro usando a convenção de nomenclatura `L0Dnnnnn`, que pode suportar até 100.000 membros. Se você tiver	

Tarefa	Descrição	Habilidades necessárias
	mais de 100.000 tabelas, use um prefixo mais curto e ajuste os números na declaração `tempjob`. Script ZSTEPS REXX `/*REXX - - -

Tarefa	Descrição	Habilidades necessárias
	`ADDRESS ISPEXEC "FTINCL UNLDSKEL" /* member will be saved in ISPDSN library allocated in JCL */ ADDRESS ISPEXEC "FTCLOSE NAME("tempjob")" END ADDRESS TSO "FREEF(TABLIST) " ADDRESS TSO "FREEF(ISPFILE) " exit 0`	

Execute o JCLs

Tarefa	Descrição	Habilidades necessárias
Executar a etapa Db2 Unload.	Após a geração do JCL, você terá JCLs quantas tabelas precisarem ser descarregadas. Esse histórico usa um exemplo gerado pela JCL para explicar a estrutura e as etapas mais importantes. Não é necessária nenhuma ação de sua parte. As informações a seguir são destinadas somente para referência. Se sua intenção é enviar o JCLs que você	Desenvolvedor de mainframe, engenheiro de sistemas

Tarefa	Descrição	Habilidades necessárias
	gerou na etapa anterior, vá para Enviar a LODnnnnn JCLs tarefa. Ao descarregar dados do Db2 usando um JCL com o utilitári o DSNUTILB Db2 fornecido pela IBM, você deve garantir que os dados descarregados não contêm dados numéricos compactados. Para fazer isso, use o parâmetro DSNUTILB `DELIMITED` . O parâmetro `DELIMITED` tem suporte para o descarreg amento dos dados no formato CSV adicionando um caractere como delimitador e aspas duplas ao campo de texto, removendo o preenchim ento na coluna VARCHAR e convertendo todos os campos numéricos em FORMATO EXTERNO, incluindo os campos de DATA. O exemplo a seguir mostra a aparência da etapa de descarga no JCL gerado, usando o caractere de vírgula como delimitador. `UNLOAD`	

Tarefa	Descrição	Habilidades necessárias
	DELIMITED COLDEL ',' FROM TABLE SCHEMA_NAME.TBNAME UNLDDN SYSREC01 PUNCHDDN SYSPUN01 SHRLEVEL CHANGE ISOLATION UR;	

Tarefa	Descrição	Habilidades necessárias
Executar a etapa SFTP.	Para usar o protocolo SFTP de um JCL, use o utilitário BPXBATCH. O utilitário SFTP não pode acessar os conjuntos de dados MVS diretamente. Você pode usar o comando copy (`cp`) para copiar o arquivo sequencial `&USRPFX..DB2.UNLOAD.&JOBNAME` para o diretório USS, onde ele se torna `&TABNAME..csv` . Execute o comando `sftp` usando a chave privada (`id_rsa`) e usando o ID de usuário do RACF como nome de usuário para se conectar ao endereço IP do AWS Transfer Family. `SH cp "//'&USRPFX..DB2.UNLOAD.&JOBNAME'" &TABNAME..csv; echo "ascii " >> uplcmd; echo "PUT &TABNAME..csv " >>>> uplcmd; sftp -b uplcmd -i .ssh/id_rsa &FTPUSER.@&FTP_TF_SITE; rm &TABNAME..csv;`	Desenvolvedor de mainframe, engenheiro de sistemas

Tarefa	Descrição	Habilidades necessárias
Envie LODnnnnn JCLs o.	O JCL anterior gerou todas as tabelas LODnnnnn JCL que precisam ser descarregadas, transformadas em CSV e transferidas para o bucket do S3. Execute o `submit` comando em todos os JCLs que foram gerados.	Desenvolvedor de mainframe, engenheiro de sistemas

Recursos relacionados

Para obter mais informações sobre as diferentes ferramentas e soluções usadas neste documento, consulte o seguinte:

- Guia do usuário do z/OS OpenSSH
- Db2 z/OS – Exemplos de instruções de controle UNLOAD
- Db2 z/OS – Descarregar arquivos delimitados
- Transfer Family – Criar um servidor habilitado para SFTP
- Transfer Family – Trabalhar com usuários gerenciados por serviços

Mais informações

Depois de ter seus dados do Db2 no Amazon S3, você tem várias maneiras de desenvolver novos insights. Como o Amazon S3 se integra aos serviços de análise de dados da AWS, você pode consumir ou expor livremente esses dados no lado distribuído. Por exemplo, você pode fazer o seguinte:

- Crie um data lake no Amazon S3 e extraia informações valiosas usando query-in-place ferramentas de análise e aprendizado de máquina sem mover os dados.
- Inicie uma função do Lambda configurando um fluxo de trabalho de processamento pós upload integrado ao AWS Transfer Family.

- Desenvolva novos microsserviços para acessar os dados no Amazon S3 ou em um banco de dados totalmente gerenciado usando o AWS Glue, que é um serviço de integração de dados de tecnologia sem servidor que facilita a descoberta, preparação e combinação de dados para análise, machine learning e desenvolvimento de aplicativos.

Em um caso de uso de migração, como você pode transferir qualquer dado do mainframe para o S3, você pode fazer o seguinte:

- Retire a infraestrutura física e crie uma estratégia de arquivamento de dados econômica com o Amazon S3 Glacier e o S3 Glacier Deep Archive.
- crie soluções de backup e restauração escaláveis, duráveis e seguras com o Amazon S3 e outros serviços da AWS, como o S3 Glacier e o Amazon Elastic File System (Amazon EFS), para aumentar ou substituir os recursos on-premises existentes.

Mais padrões

- Implemente as automações de segurança para a AWS WAF solução usando o Terraform
- Replique bancos de dados de mainframe para AWS usando o Precisely Connect

Gerenciamento

Tópicos

- Gerenciamento de custos
- Computação de alta performance
- Nuvem híbrida
- Gerenciamento e governança
- Mensagens e comunicações

Gerenciamento de custos

Tópicos

- Crie relatórios detalhados de custo e uso para trabalhos do AWS Glue usando o Explorador de Custos da AWS
- Crie relatórios detalhados de custo e uso para clusters do Amazon EMR usando o Explorador de Custos da AWS
- Mais padrões

Crie relatórios detalhados de custo e uso para trabalhos do AWS Glue usando o Explorador de Custos da AWS

Criado por Parijat Bhide (AWS) e Aromal Raj Jayarajan (AWS)

Resumo

Esse padrão mostra como rastrear os custos de uso dos trabalhos de integração de dados do AWS Glue configurando tags de alocação de custos definidas pelo usuário. Você pode usar essas tags para criar relatórios detalhados de custo e uso no Explorador de Custos da AWS para trabalhos em várias dimensões. Por exemplo, você pode monitorar os custos de uso no nível da equipe, do projeto ou do centro de custos.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um ou mais trabalhos do AWS Glue com tags definidas pelo usuário ativadas

Arquitetura

Pilha de tecnologias de destino

- AWS Glue
- AWS Cost Explorer

O diagrama a seguir mostra como você pode aplicar tags para rastrear os custos de uso de trabalhos do AWS Glue.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um engenheiro de dados ou administrador da AWS cria tags de alocação de custos definidas pelo usuário para os trabalhos do AWS Glue.
2. Um administrador da AWS ativa as tags.
3. As tags reportam metadados para o Explorador de Custos da AWS.

Ferramentas

- O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele ajuda você a categorizar, limpar, enriquecer e mover dados de forma confiável entre armazenamentos de dados e fluxos de dados.
- O Explorador de Custos da AWS permite que você visualize e analise seus custos e uso do AWS.

Épicos

Criar e ativar tags para suas tarefas do AWS Glue

Tarefa	Descrição	Habilidades necessárias
Crie tags de alocação de custos definidas pelo usuário para suas tarefas do AWS Glue.	Para adicionar tags a uma tarefa existente do AWS Glue 1. Faça login no Console de Gerenciamento da AWS e abra o console do AWS Glue. 2. No painel de navegação à esquerda, em ETL, escolha Trabalhos. 3. Na seção Seus trabalhos, escolha o nome do trabalho que você está marcando. 4. Escolha a guia Job details (Detalhes do trabalho). Em seguida, expanda a seção Propriedades avançadas. 5. Em Tags, escolha Adicionar nova tag. 6. Em Chave, insira um nome para sua tag.	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
	7. (Opcional) Em Valor, insira um valor que você deseja associar à chave. 8. (Opcional) Repita as etapas 5 a 7 para cada tag que você deseja criar para o trabalho. 9. Escolha Salvar. Para adicionar tags a um trabalho novo do AWS Glue 1. Crie um trabalho novo do AWS Glue com base nos requisitos do seu caso de uso. Para obter instruções, consulte Trabalho com tarefas no Console do AWS Glue no Guia do desenvolvedor do AWS Glue. 2. Ao definir as configurações de Detalhes do trabalho, siga as etapas 4 a 9 da seção Para adicionar tags a um trabalho existente do AWS Glue desta tarefa. Note Para obter mais informações, consulte as tags da AWS no AWS Glue no Guia	

Tarefa	Descrição	Habilidades necessárias
	do desenvolvedor do AWS Glue.	
Ativar as tags de alocação de custos definidas pelo usuário.	Siga as instruções em Ativação de tags de alocação de custos definidas pelo usuário no Guia do usuário do AWS Billing.	Administrador da AWS

Crie relatórios detalhados de custo e uso para seus trabalhos do AWS Glue

Tarefa	Descrição	Habilidades necessárias
Crie relatórios de custo e uso para seus trabalhos do AWS Glue usando filtros de tag no Explorador de Custos da AWS.	1. Faça login no Console de Gerenciamento da AWS e abra o console de gerenciamento de custos do AWS. 2. No painel de navegação à esquerda, escolha Relatórios. 3. Escolha Criar novo relatório. 4. Em Selecionar um tipo de relatório, escolha Custo e uso (recomendado). Depois, escolha Criar relatório. 5. Em Filtros, escolha Serviço. A lista suspensa Serviço é exibida. 6. Marque a caixa de seleção ao lado em Glue. Em	AWS geral, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	seguida, escolha Aplicar filtros. 7. Em Filtros, escolha Tag. O menu suspenso Tag é exibido. 8. Escolha Equipe. Em seguida, marque as caixas de seleção ao lado das equipes às quais você atribuiu tags. Exclua todas as equipes às quais você não atribuiu tags. Em seguida, escolha Aplicar filtros. 9. Na parte superior do gráfico, escolha Tag. Em seguida, escolha as tags para os trabalhos do AWS Glue para os quais você deseja criar um relatório. 10. Na parte superior do gráfico, escolha a lista suspensa Últimos 3 meses e escolha o período que você deseja que o relatório cubra. Em seguida, escolha a lista suspensa Mensal e escolha como você deseja que os itens de linha no relatório sejam agregados com base no período. 11. Escolha Save as (Salvar). Em seguida, insira um título para seu relatório.	

Tarefa	Descrição	Habilidades necessárias
	12Escolha Salvar relatório. Para obter mais informações, consulte Explorar seus dados usando o Cost Explorer no Guia do usuário do AWS Cost Management.	

Crie relatórios detalhados de custo e uso para clusters do Amazon EMR usando o Explorador de Custos da AWS

Criado por Parijat Bhide (AWS) e Aromal Raj Jayarajan (AWS)

Resumo

Esse padrão mostra como rastrear os custos de uso dos clusters do Amazon EMR configurando tags de alocação de custos definidas pelo usuário. Você pode usar essas tags para criar relatórios detalhados de custo e uso no Explorador de Custos da AWS para clusters em várias dimensões. Por exemplo, você pode monitorar os custos de uso no nível da equipe, do projeto ou do centro de custos.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um ou mais clusters EMR com tags definidas pelo usuário ativadas

Arquitetura

Pilha de tecnologias de destino

- Amazon EMR
- AWS Cost Explorer

Arquitetura de destino

O diagrama a seguir mostra como você pode aplicar tags para rastrear os custos de uso de clusters específicos do Amazon EMR.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um engenheiro de dados ou administrador da AWS cria tags de alocação de custos definidas pelo usuário para os clusters do Amazon EMR.
2. Um administrador da AWS ativa as tags.
3. As tags reportam metadados para o Explorador de Custos da AWS.

Ferramentas

Ferramentas

- O Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de big data para processar e analisar grandes volumes de dados.
- O Explorador de Custos da AWS permite que você visualize e analise seus custos e uso.

Épicos

Crie e ative tags para seus clusters do Amazon EMR

Tarefa	Descrição	Habilidades necessárias
Crie tags de alocação de custos definidas pelo usuário para seus clusters do Amazon EMR.	Para adicionar tags a um cluster existente do Amazon EMR Siga as instruções em Adicionar tags a um cluster existente no Guia de gerenciamento do Amazon EMR. Para adicionar tags a um novo cluster do Amazon EMR Siga as instruções em Adicionar tags a um novo cluster no Guia de gerenciam ento do Amazon EMR. Para obter mais informaçõ es sobre como configurar um cluster do Amazon EMR, consulte Planejar e configurar clusters no Guia de gerenciam ento do Amazon EMR.	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
Ativar as tags de alocação de custos definidas pelo usuário.	Siga as instruções em Ativação de tags de alocação de custos definidas pelo usuário no Guia do usuário do AWS Billing.	Administrador da AWS

Crie relatórios de custo e uso para seus clusters do Amazon EMR

Tarefa	Descrição	Habilidades necessárias
Crie relatórios de custo e uso para seus clusters do Amazon EMR usando filtros de tag no Explorador de Custos da AWS.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Console de Gerenciamento da AWS. 2. No painel de navegação à esquerda, escolha Relatórios. 3. Escolha Criar novo relatório. 4. Em Selecionar um tipo de relatório, escolha Custo e uso (recomendado). Depois, escolha Criar relatório. 5. Em Filtros, escolha Serviço. A lista suspensa Serviço é exibida. 6. Marque as caixas de seleção ao lado de EMR (Elastic MapReduce) e EC2-Instances (Elastic Compute Cloud —	AWS geral, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Compute). Em seguida, escolha Aplicar filtros. 7. Em Filtros, escolha Tag. O menu suspenso Tag é exibido. 8. Escolha Equipe. Em seguida, marque as caixas de seleção ao lado das equipes às quais você atribuiu tags. Exclua todas as equipes às quais você não atribuiu tags. Em seguida, escolha Aplicar filtros. 9. Na parte superior do gráfico, escolha Tag. Em seguida, escolha as tags para os clusters do Amazon EMR para os quais você deseja criar um relatório. 10. Na parte superior do gráfico, escolha a lista suspensa Últimos três meses e escolha o período que você deseja que o relatório cubra. Em seguida, escolha a lista suspensa Mensal e escolha como você deseja que os itens de linha no relatório sejam agregados com base no período.	

Tarefa	Descrição	Habilidades necessárias
	11 Escolha Save as (Salvar). Em seguida, insira um título para seu relatório. 12 Escolha Salvar relatório. Para obter mais informações, consulte Explorar seus dados usando o Cost Explorer no Guia do usuário do AWS Cost Management.	

Mais padrões

- Automatize as operações de AWS infraestrutura usando o Amazon Bedrock
- Faça o inventário automático de AWS recursos em várias contas e regiões
- Automatize a criação de recursos AppStream 2.0 usando a AWS CloudFormation
- Arquivar automaticamente itens no Amazon S3 usando o DynamoDB TTL
- Pare e inicie automaticamente uma instância de banco de dados Amazon RDS usando o Windows AWS Systems Manager de manutenção
- Crie relatórios detalhados de custos e uso para o Amazon RDS e o Amazon Aurora
- Exclua volumes não utilizados do Amazon EBS usando e AWS ConfigAWS Systems Manager
- Estime os custos de armazenamento de uma tabela do Amazon DynamoDB
- Expressa o custo de uma tabela do DynamoDB para capacidade sob demanda
- Configure o escalonamento automático orientado por eventos no Amazon EKS usando o Amazon EKS Pod Identity e o KEDA
- Coordene a dependência de recursos e a execução de tarefas usando a AWS Fargate WaitCondition construção de gancho

Computação de alta performance

Tópicos

- Implemente um sistema de arquivos Lustre para processamento de dados de alto desempenho usando o Terraform e o DRA
- Configure um painel de monitoramento da Grafana para a AWS ParallelCluster
- Configure uma infraestrutura de desktop virtual com escalabilidade automática usando o NICE EnginFrame e o NICE DCV Session Manager

Implemente um sistema de arquivos Lustre para processamento de dados de alto desempenho usando o Terraform e o DRA

Criado por Arun Bagal (AWS) e Ishwar Chauthaiwale (AWS)

Resumo

Esse padrão implanta automaticamente um sistema de arquivos Lustre AWS e o integra ao Amazon Elastic Compute Cloud (Amazon) EC2 e ao Amazon Simple Storage Service (Amazon S3).

Essa solução ajuda você a configurar rapidamente um ambiente de computação de alta performance (HPC) com armazenamento integrado, recursos computacionais e acesso a dados do Amazon S3. Ele combina os recursos de armazenamento do Lustre com as opções de computação flexíveis fornecidas pela Amazon EC2 e o armazenamento de objetos escalável no Amazon S3, para que você possa lidar com cargas de trabalho com uso intenso de dados em aprendizado de máquina, HPC e análise de big data.

O padrão usa um módulo HashiCorp Terraform e o Amazon for Lustre FSx para simplificar o seguinte processo:

- Provisionando um sistema de arquivos Lustre
- Estabelecendo uma associação de repositório de dados (DRA) entre FSx o Lustre e um bucket do S3 para vincular o sistema de arquivos Lustre aos objetos do Amazon S3
- Criação de uma EC2 instância
- Montagem do sistema de arquivos Lustre com o DRA vinculado ao Amazon S3 na instância EC2

Os benefícios dessa solução incluem:

- Design modular. Você pode facilmente manter e atualizar os componentes individuais dessa solução.
- Escalabilidade. Você pode implantar rapidamente ambientes consistentes em Contas da AWS nossas regiões.
- Flexibilidade. Você pode personalizar a implantação para atender às suas necessidades específicas.
- Melhores práticas. Esse padrão usa módulos pré-configurados que seguem as AWS melhores práticas.

Para obter mais informações sobre os sistemas de arquivos Lustre, consulte o site Lustre.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Uma política de privilégios mínimos AWS Identity and Access Management (IAM) (consulte as instruções)

Limitações

FSx for Lustre limita o sistema de arquivos Lustre a uma única zona de disponibilidade, o que pode ser uma preocupação se você tiver requisitos de alta disponibilidade. Se a zona de disponibilidade que contém o sistema de arquivos falhar, o acesso ao sistema de arquivos será perdido até a recuperação. Para obter alta disponibilidade, você pode usar o DRA para vincular o sistema de arquivos Lustre ao Amazon S3 e transferir dados entre zonas de disponibilidade.

Versões do produto

- Terraform versão 1.9.3 ou posterior
- HashiCorp AWS Provider versão 4.0.0 ou posterior

Arquitetura

O diagrama a seguir mostra a arquitetura do Lustre e a complementar Serviços da AWS no Nuvem AWS. FSx

A arquitetura inclui o seguinte:

- Um bucket S3 é usado como um local de armazenamento de dados durável, escalável e econômico. A integração entre FSx o Lustre e o Amazon S3 fornece um sistema de arquivos de alto desempenho que está perfeitamente vinculado ao Amazon S3.
- FSx for Lustre executa e gerencia o sistema de arquivos Lustre.
- O Amazon CloudWatch Logs coleta e monitora dados de log do sistema de arquivos. Esses registros fornecem informações sobre o desempenho, a integridade e a atividade do seu sistema de arquivos Lustre.

- A Amazon EC2 é usada para acessar sistemas de arquivos Lustre usando o cliente Lustre de código aberto. EC2 as instâncias podem acessar sistemas de arquivos de outras zonas de disponibilidade dentro da mesma nuvem privada virtual (VPC). A configuração de rede permite o acesso entre sub-redes dentro da VPC. Depois que o sistema de arquivos Lustre for montado na instância, você poderá trabalhar com seus arquivos e diretórios da mesma forma que usaria um sistema de arquivos local.
- AWS Key Management Service (AWS KMS) aumenta a segurança do sistema de arquivos fornecendo criptografia para dados em repouso.

Automação e escala

O Terraform facilita a implantação, o gerenciamento e a escalabilidade de seus sistemas de arquivos Lustre em vários ambientes. No FSx Lustre, um único sistema de arquivos tem limitações de tamanho, então talvez seja necessário escalar horizontalmente criando vários sistemas de arquivos. Você pode usar o Terraform para provisionar vários sistemas de arquivos Lustre com base nas suas necessidades de carga de trabalho.

Ferramentas

Serviços da AWS

- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas e aplicativos, Serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- O Amazon FSx for Lustre torna fácil e econômico lançar, executar e escalar um sistema de arquivos Lustre de alto desempenho.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Repositório de código

O código desse padrão está disponível no sistema de arquivos GitHub Provision FSx for Lustre usando o repositório Terraform.

Práticas recomendadas

- As variáveis a seguir definem o sistema de arquivos Lustre. Certifique-se de configurá-los corretamente com base em seu ambiente, conforme as instruções na seção Epics.
  - `storage_capacity`— A capacidade de armazenamento do sistema de arquivos Lustre, em GiBs. A configuração mínima e padrão é 1200 GiB.
  - `deployment_type`— O tipo de implantação do sistema de arquivos Lustre. Para obter uma explicação das duas opções `PERSISTENT_1` e `PERSISTENT_2` (padrão), consulte a documentação do FSx Lustre.
  - `per_unit_storage_throughput`— A taxa de transferência de leitura e gravação, em MBs por segundo por TiB.
  - `subnet_id`— O ID da sub-rede privada em que você deseja FSx implantar o Lustre.
  - `vpc_id`— O ID da sua nuvem privada virtual AWS onde você deseja FSx implantar o Lustre.
  - `data_repository_path`— O caminho para o bucket do S3 que será vinculado ao sistema de arquivos Lustre.
  - `iam_instance_profile`— O perfil da instância do IAM a ser usado para iniciar a EC2 instância.
  - `kms_key_id`— O Amazon Resource Name (ARN) da AWS KMS chave que será usada para criptografia de dados.
- Garanta o acesso e o posicionamento adequados da rede na VPC usando as variáveis `security_group` e. `vpc_id`
- Execute o `terraform plan` comando conforme descrito na seção Epics para visualizar e verificar as alterações antes de aplicá-las. Isso ajuda a detectar possíveis problemas e garante que você esteja ciente do que será implantado.
- Use o `terraform validate` comando conforme descrito na seção Epics para verificar erros de sintaxe e confirmar se sua configuração está correta.

Épicos

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Instale o Terraform.	Para instalar o Terraform em sua máquina local, siga as instruções na documentação do Terraform.	AWS DevOps, DevOps engenheiro
Configure as AWS credencia is.	Para configurar o perfil AWS Command Line Interface (AWS CLI) para a conta, siga as instruções na AWS documentação.	AWS DevOps, DevOps engenheiro
Clone o GitHub repositório.	Para clonar o GitHub repositór io, execute o comando: `git clone https://g ithub.com/aws-samp les/provision-fsx- lustre-with-terraf orm.git`	AWS DevOps, DevOps engenheiro

Configure e implante FSx para Lustre

Tarefa	Descrição	Habilidades necessárias
Atualize a configuração de implantação.	1. No repositório clonado em sua máquina local, navegue até o `fsx_deployment` diretório: `cd fsx_deployment`	AWS DevOps, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	2. Abra o `terraform.tfvars` arquivo e atualize os valores das seguintes variáveis: • `vpc_id` • `subnet_id` • `data_repository_path` • `iam_instance_profile` • `kms_key_id` Para obter descrições dessas variáveis, consulte a seção Melhores práticas. 3. No mesmo diretório, abra o `locals.tf` arquivo e atualize os intervalos CIDR para as variáveis `fsx_inress` e do grupo `fsx_egress` de segurança. 4. Se necessário, abra o `variables.tf` arquivo e atualize os valores padrão dessas variáveis: • `storage_capacity` • `deployment_type` • `per_unit_storage_throughput`	

Tarefa	Descrição	Habilidades necessárias
	Para obter descrições dessas variáveis, consulte a seção Melhores práticas.	
Inicialize o ambiente Terraform.	Para inicializar seu ambiente para executar o `fsx_deployment` módulo Terraform, execute: `terraform init`	AWS DevOps, DevOps engenheiro
Valide a sintaxe do Terraform.	Para verificar erros de sintaxe e confirmar se sua configuração está correta, execute: `terraform validate`	AWS DevOps, DevOps engenheiro
Valide a configuração do Terraform.	Para criar um plano de execução do Terraform e visualizar a implantação, execute: `terraform plan -var-file terraform.tfvars`	AWS DevOps, DevOps engenheiro
Implante o módulo Terraform.	Para implantar os recursos do FSx for Lustre, execute: `terraform apply -var-file terraform.tfvars`	AWS DevOps, DevOps engenheiro

Limpe AWS os recursos

Tarefa	Descrição	Habilidades necessárias

Remova AWS os recursos.	Depois de terminar de usar seu ambiente FSx for Lustre, você pode remover os AWS recursos implantados pelo Terraform para evitar cobranças desnecessárias. O módulo Terraform fornecido no repositório de código automatiza essa limpeza.
	1. No seu repositório local, navegue até o `fsx_deployment` diretório:
	`cd fsx_deployment`
	2. Execute o comando :
	`terraform destroy -var-file terraform.tfvars`
		AWS DevOps, DevOps engenheiro

Solução de problemas

Problema	Solução
FSx for Lustre retorna erros.	Para obter ajuda com FSx problemas do Lustre, consulte Solução de problemas do Amazon FSx for Lustre na documentação do FSx for Lustre.

Recursos relacionados

- Construindo o Amazon FSx for Lustre usando o Terraform (referência do AWS provedor na documentação do Terraform)
- Introdução ao Amazon FSx for Lustre (FSx para documentação do Lustre)
- AWS postagens de blog sobre Amazon FSx for Lustre

Configure um painel de monitoramento da Grafana para a AWS ParallelCluster

Criado por Dario La Porta (AWS) e William Lu (AWS)

Resumo

ParallelCluster A AWS ajuda você a implantar e gerenciar clusters de computação de alta performance (HPC). Ele oferece suporte aos agendadores de trabalhos de código aberto AWS Batch e Slurm. Embora a AWS ParallelCluster esteja integrada à Amazon CloudWatch para registro e métricas, ela não fornece um painel de monitoramento para a carga de trabalho.

O painel Grafana para AWS ParallelCluster (GitHub) é um painel de monitoramento para a AWS. ParallelCluster Ele fornece informações sobre o agendador de tarefas e métricas detalhadas de monitoramento no nível do sistema operacional (SO). Para obter mais informações sobre os painéis incluídos nessa solução, consulte Exemplos de painéis no GitHub repositório. Essas métricas ajudam você a entender melhor a workload de HPC e seu desempenho. No entanto, o código do painel não é atualizado para as versões mais recentes da AWS ParallelCluster ou para os pacotes de código aberto usados na solução. Esse padrão aprimora a solução para fornecer os seguintes benefícios:

- Compatível com AWS ParallelCluster v3
- Usa a versão mais recente dos pacotes de código aberto, incluindo Prometheus, Grafana, Prometheus Slurm Exporter e NVIDIA DCGM-Exporter
- Aumenta o número de núcleos de CPU e GPUs que os trabalhos do Slurm usam
- Adiciona um painel de monitoramento de trabalhos
- Aprimora o painel de monitoramento de nós da GPU para nós com 4 ou 8 unidades de processamento gráfico () GPUs

Essa versão da solução aprimorada foi implementada e verificada no ambiente de produção de HPC de um cliente da AWS.

Pré-requisitos e limitações

Pré-requisitos

- AWS ParallelCluster CLI, instalada e configurada.

- Uma configuração de rede compatível com a AWS ParallelCluster. Esse padrão usa a AWS ParallelCluster usando a configuração de duas sub-redes, o que requer uma sub-rede pública, uma sub-rede privada, um gateway de internet e um gateway NAT.
- Todos os nós de ParallelCluster cluster da AWS devem ter acesso à Internet. Isso é necessário para que os scripts de instalação possam baixar o software de código aberto e as imagens do Docker.
- Um par de chaves na Amazon Elastic Compute Cloud (Amazon EC2). Os recursos que têm esse par de chaves têm acesso Secure Shell (SSH) ao nó principal.

Limitações

- Esse padrão foi projetado para suportar Ubuntu 20.04 LTS. Se você estiver usando uma versão diferente do Ubuntu ou se usar Amazon Linux ou CentOS, precisará modificar os scripts fornecidos com essa solução. Essas modificações não estão incluídas nesse padrão.

Versões do produto

- Ubuntu 20.04 LTS
- ParallelCluster 3.X

Considerações sobre faturamento e custos

- A solução implantada nesse padrão não é coberta pelo nível gratuito. As cobranças se aplicam à Amazon EC2, ao Amazon FSx for Lustre, ao gateway NAT no Amazon VPC e ao Amazon Route 53.

Arquitetura

Arquitetura de destino

O diagrama a seguir mostra como um usuário pode acessar o painel de monitoramento da AWS ParallelCluster no nó principal. O nó principal executa NICE DCV, Prometheus, Grafana, Prometheus Slurm Exporter, Prometheus Node Exporter e NGINX Open Source. Os nós de computação executam o Prometheus Node Exporter e também executam o NVIDIA DCGM-Exporter se o nó contiver. GPUs O nó principal recupera informações dos nós de computação e exibe esses dados no painel da Grafana.

Na maioria dos casos, o nó principal não está muito carregado porque o agendador de tarefas não exige uma quantidade significativa de CPU ou memória. Os usuários acessam o painel no nó principal usando SSL na porta 443.

Todos os espectadores autorizados podem visualizar anonimamente os painéis de monitoramento. Somente o administrador da Grafana pode modificar os painéis. Você configura uma senha para o administrador da Grafana no `aws-parallelcluster-monitoring/docker-compose/docker-compose.head.yml` arquivo.

Ferramentas

Serviços da AWS

- O NICE DCV é um protocolo de exibição remota de alto desempenho que ajuda você a fornecer desktops remotos e streaming de aplicativos de qualquer nuvem ou datacenter para qualquer dispositivo, em diferentes condições de rede.
- ParallelClusterA AWS ajuda você a implantar e gerenciar clusters de computação de alta performance (HPC). Ele oferece suporte aos agendadores de trabalhos de código aberto AWS Batch e Slurm.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você.

Outras ferramentas

- O Docker é um conjunto de produtos de plataforma como serviço (PaaS) que usam a virtualização no nível do sistema operacional para fornecer software em contêineres.
- O Grafana é um software de código aberto que ajuda você a consultar, visualizar, alertar e explorar métricas, registros e rastreamentos.
- O NGINX Open Source é um servidor web de código aberto e proxy reverso.
- O NVIDIA Data Center GPU Manager (DCGM) é um conjunto de ferramentas para gerenciar e monitorar unidades de processamento gráfico (GPUs) de data center NVIDIA em ambientes de

cluster. Nesse padrão, você usa o DCGM-Exporter, que ajuda a exportar métricas de GPU do Prometheus.

- O Prometheus é um kit de ferramentas de monitoramento de sistema de código aberto que coleta e armazena suas métricas como dados de séries temporais com pares de valores-chave associados, chamados de rótulos. Nesse padrão, você também usa o Prometheus Slurm Exporter para coletar e exportar métricas e usa o Prometheus Node Exporter para exportar métricas dos nós de computação.
- O Ubuntu é um sistema operacional de código aberto baseado em Linux, projetado para servidores corporativos, desktops, ambientes de nuvem e IoT.

Repositório de código

O código desse padrão está disponível no GitHub pcluster-monitoring-dashboardrepositório.

Épicos

Crie os recursos necessários

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Crie um bucket do Amazon S3. Você usa esse bucket para armazenar os scripts de configuração. Para obter instruções, consulte Criação de um bucket na documentação do Amazon S3.	AWS geral
Clonar o repositório.	Clone o GitHub pcluster-monitoring-dashboardrepositório executando o comando a seguir. `git clone https://github.com/aws-samples/parallelcluste`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`r-monitoring-dashb oard.git`	
Crie uma senha de administr ador.	1. Escolha a `aws-paral lelcluster-monitor ing` pasta, escolha a `docker-compose` pasta e abra o arquivo docker-co mpose.head.yml. 2. Na `GF_SECURI TY_ADMIN_ PASSWORD` variável, substitua `Grafana4PC!` por uma senha da sua escolha. Essa é a senha administrativa que você usa para gerenciar a conta Grafana. 3. Salve e feche o arquivo docker-compose.head.yml.	Fazer scripts de shell Linux
Copie os arquivos necessários para o bucket do S3.	Copie o script post_inst all.sh e a aws-parallelcluste r-monitoringpasta no bucket do S3 que você criou. Para obter instruções, consulte Fazer uploads de objetos na documentação do Amazon S3.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Configure um grupo de segurança adicional para o nó principal.	1. Crie um grupo de segurança para o nó principal. Esse grupo de segurança permitirá tráfego de entrada para os painéis de monitoramento no nó principal. Para obter instruções, consulte Criar um grupo de segurança na documentação da Amazon VPC. 2. Adicione regras de entrada ao grupo de segurança . Para obter instruções, consulte Adicionar regras a um grupo de segurança na documentação do Amazon VPC. Use os parâmetros a seguir para a regra: • Tipo: HTTPS • Protocol (Protocolo): TCP • Intervalo de portas: 443 • Fonte: insira seu endereço IP • Descrição: permitir que os usuários acessem o painel de monitoramento	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Configure uma política do IAM para o nó principal.	Crie uma política do baseada em identidade para o nó principal. Essa política permite que o nó recupere dados métricos da Amazon CloudWatch. O GitHub repositório contém um exemplo de política. Para obter instruções, consulte Criar políticas do IAM na documentação do AWS Identity and Access Management (IAM).	Administrador da AWS
Configure uma política do IAM para os nós de computação.	Crie uma política do baseada em identidade para os nós de computação. Essa política permite que o nó crie as tags que contêm o ID do trabalho e o proprietário do trabalho. O GitHub repositório contém um exemplo de política. Para obter instruções, consulte Criação de políticas do IAM na documentação do IAM. Se usar o arquivo de exemplo fornecido, substitua os seguintes valores: • <REGION>: a região da AWS em que o cluster está hospedado. • <ACCOUNT_ID>: o ID de conta da AWS.	Administrador da AWS

Criar um cluster

Tarefa	Descrição	Habilidades necessárias
Modifique o arquivo de modelo de cluster fornecido.	Crie o ParallelCluster cluster da AWS. Use o arquivo de modelo cluster.yaml CloudFormation AWS fornecido como ponto de partida para criar o cluster. Substitua os seguintes valores no modelo fornecido: • <REGION>: a região da AWS em que o cluster está hospedado. • <HEADNODE_SUBNET>: a sub-rede pública da VPC. • <ADDITIONAL_HEAD_NODE_SG>: o nome do grupo de segurança que você criou para o nó principal. • <KEY_NAME>— Insira o nome de um par de EC2 chaves da Amazon existente. Os recursos que têm esse par de chaves têm acesso Secure Shell (SSH) ao nó principal. • <ALLOWED_IPS>: insira o intervalo de endereços IP formatado em CIDR que tem permissão para fazer conexões SSH com o nó principal.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	• <ADDITIONAL_HEAD_NODE_POLICY>: insira o nome da política do IAM que você criou para o nó principal. • <BUCKET_NAME>: insira o nome do bucket do S3 que você criou. • <COMPUTE_SUBNET>: insira o nome da sub-rede privada na VPC. • <ADDITIONAL_COMPUTE_NODE_POLICY>: insira o nome da política do IAM que você criou para o nó de computação.	
Crie o cluster.	Na AWS ParallelCluster CLI, insira o seguinte comando. Isso implanta o CloudFormation modelo e cria o cluster. Para obter mais informações sobre esse comando, consulte pcluster create-cluster na documentação da AWS. ParallelCluster `pcluster create-cluster -n <cluster_name> -c cluster.yaml`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Monitore a criação do cluster.	Insira o comando a seguir para monitorar a criação do cluster. Para obter mais informações sobre esse comando, consulte pcluster describe-cluster na documentação da AWS. ParallelCluster `pcluster describe-cluster -n <cluster_name>`	Administrador da AWS

Usar os painéis do Grafana

Tarefa	Descrição	Habilidades necessárias
Acesso ao portal Grafana.	1. Insira o comando a seguir para recuperar o endereço IP público do nó principal. `pcluster describe-cluster -n <cluster_name> --query headNode.publicIpAddress` 2. Em um navegador da web, navegue até o seguinte URL para acessar o painel da Grafana. https://<head_node_public_ip_address> 3. Na página inicial da Grafana, escolha o ícone	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	do Painel de 4 quadrados no menu à esquerda e escolha Geral. Isso mostra uma lista de painéis de configuração. Os seguintes painéis estão disponíveis no Grafana: • Custo do cluster: contém informações sobre o custo do cluster • Logs do cluster: contém informações sobre os registros do cluster • Detalhes do nó de computação: contém informações sobre estatísticas de uso dos nós de computação • Lista de nós de computação: contém a lista dos nós de computação do cluster • Nós da GPU: contém informações sobre as estatísticas de uso dos nós da GPU • Detalhes do trabalho: contém informações sobre a utilização dos recursos do trabalho • Detalhes do nó principal : contém informações	

Tarefa	Descrição	Habilidades necessárias
	sobre as estatísticas de uso do nó principal • ParallelCluster Resumo — Contém informações sobre o uso do cluster	

Limpe a solução para parar de incorrer em custos associados

Tarefa	Descrição	Habilidades necessárias
Excluir o cluster.	Insira o comando a seguir para excluir o cluster. Para obter mais informações sobre esse comando, consulte pcluster delete-cluster na documentação da AWS. ParallelCluster `pcluster delete-cluster -n <cluster_name>`	Administrador da AWS
Exclua as políticas do IAM.	Exclua as políticas que você criou para o nó principal e o nó de computação. Para obter mais informações sobre como excluir políticas, consulte Criação de políticas do IAM na documentação do IAM.	Administrador da AWS
Para excluir a regra e o grupo de segurança	Exclua o grupo de segurança que você criou para o nó principal. Para obter mais informações, consulte Excluir regras de grupos de segurança e Excluir um grupo	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	de segurança na documentação do Amazon VPC.	
Exclua o bucket do S3.	Exclua o bucket do S3 que você criou para armazenar os scripts de configuração. Para obter mais informações, consulte Excluir um bucket na documentação do Amazon S3	AWS geral

Solução de problemas

Problema	Solução
O nó principal não está acessível no navegador.	Verifique o grupo de segurança e confirme se a porta de entrada 443 está aberta.
Grafana não abre.	No nó principal, verifique o log do contêiner `docker logs Grafana`.
Algumas métricas não têm dados.	No nó principal, verifique os logs de todos os contêineres.

Recursos relacionados

Documentação da AWS

- Políticas do IAM para a Amazon EC2

Outros recursos da AWS

- AWS ParallelCluster
- Painel de monitoramento para a AWS ParallelCluster (publicação no blog da AWS)

Outros recursos

- Sistema de monitoramento Prometheus
- Grafana

Configure uma infraestrutura de desktop virtual com escalabilidade automática usando o NICE EnginFrame e o NICE DCV Session Manager

Criado por Dario La Porta (AWS) e Salvatore Maccarone (AWS)

Resumo

O NICE DCV é um protocolo de exibição remota de alto desempenho que ajuda você a transmitir desktops e aplicativos remotos de qualquer nuvem ou datacenter para qualquer dispositivo, em diferentes condições de rede. Com o NICE DCV e o Amazon Elastic Compute Cloud (Amazon EC2), você pode executar aplicativos com uso intensivo de gráficos remotamente nas instâncias da EC2 Amazon e transmitir suas interfaces de usuário para máquinas clientes remotas mais simples. Isso elimina a necessidade de estações de trabalho dedicadas caras e a necessidade de transferir grandes quantidades de dados entre a nuvem e as máquinas do cliente.

Esse padrão configura uma infraestrutura de área de trabalho virtual (VDI) Linux e Windows totalmente funcional e com ajuste de escala automático, acessível por meio de uma interface de usuário baseada na web. A solução VDI fornece aos usuários de pesquisa e desenvolvimento (P&D) uma interface de usuário acessível e de alto desempenho para enviar solicitações de análise com uso intensivo de gráficos e revisar os resultados remotamente.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Permissões de administrador e um conjunto de chaves de acesso.
- AWS Cloud Development Kit (AWS CDK) Kit de ferramentas, instalado e configurado. Para obter mais informações, consulte Instalar a AWS CDK.
- AWS Command Line Interface (AWS CLI), instalado e configurado para o seu Conta da AWS. Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI.
- Python, instalado e configurado. Para obter mais informações, consulte Versões de origem (site da Python).
- Uma ou mais nuvens privadas virtuais (VPCs) disponíveis.
- Dois ou mais endereços IP elásticos disponíveis. Para obter mais informações sobre o limite padrão, consulte Limite de endereço IP elástico.

- Para as EC2 instâncias Linux da Amazon, configure um par de chaves Secure Shell (SSH). Para obter mais informações, consulte Pares de chaves e instâncias do Linux.

Versões do produto

- AWS CDK versão 2.26.0 ou posterior
- Python, versão 3.8 ou superior

Arquitetura

Arquitetura de destino

A figura a seguir mostra os diferentes componentes dessa solução de VDI. O usuário interage com o NICE EnginFrame para iniciar EC2 instâncias da Amazon de acordo com os grupos do Amazon EC2 Auto Scaling para instâncias NICE DCV do Windows e Linux.

Automação e escala

O código incluído nesse padrão cria uma VPC personalizada, sub-redes públicas e privadas, um gateway de internet, gateway NAT, Application Load Balancer, grupos de segurança e políticas (IAM). AWS Identity and Access Management AWS CloudFormation também é usado para criar a frota de servidores Linux e Windows NICE DCV.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- O NICE DCV é um protocolo de exibição remota de alto desempenho que ajuda você a fornecer desktops remotos e streaming de aplicativos de qualquer nuvem ou datacenter para qualquer dispositivo, em diferentes condições de rede. Nesse padrão, ele fornece uma experiência com eficiência de largura de banda que transmite gráficos 3D de computação de alta performance (HPC - high performance computing) remotamente.

- O NICE DCV Session Manager ajuda você a criar e gerenciar o ciclo de vida das sessões NICE DCV em uma frota de servidores NICE DCV.
- EnginFrameO NICE é uma interface web avançada de front-end para acessar aplicativos técnicos e científicos na nuvem.

Repositório de código

O código desse padrão está disponível na solução VDI de escalonamento automático com o repositório NICE EnginFrame e NICE DCV Session Manager.

Épicos

Implemente a infraestrutura de área de trabalho virtual

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Clone o repositório que contém o código: `git clone https://github.com/aws-samples/elastic-vdi-infrastructure.git`	Arquiteto de nuvem

Instale as AWS CDK bibliotecas necessárias.	Instale as AWS CDK bibliotecas:
	`cd elastic-vdi-infrastructure`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip3 install -r requirements.txt`
		Arquiteto de nuvem

Atualize os parâmetros.	1. Abra o arquivo app.py com seu editor de texto de preferência.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	2. Substitua o valor `CHANGE_ME` pelos seguintes parâmetros obrigatórios: • `region`— O alvo Região da AWS. Para obter uma lista completa, consulte Regiões da AWS. • `account`— O ID do alvo Conta da AWS. Para obter mais informações, consulte Encontrando seu Conta da AWS ID. • `key_name`— O par de chaves usado para acessar as EC2 instância s Linux da Amazon. 3. (Opcional) Modifique os valores dos seguintes parâmetros para personali zar a solução para seu ambiente: • `ec2_type_enginfram e` — O tipo de EnginFrame instância • `ec2_type_broker` : o tipo de instância do Session Manager Broker • `ebs_enginframe_siz e` — O tamanho do volume do Amazon Elastic Block Store	

Tarefa	Descrição	Habilidades necessárias
	(Amazon EBS) para a instância EnginFrame • `ebs_broker_size` — O tamanho do volume do Amazon EBS para a instância do Session Manager Broker • `TagName and TagValue`: a etiqueta de cobrança dos recursos • `efadmin_uid` — O identificador exclusivo do EnginFrame usuário administrador (efadmin) • `linux_shared_storage_size` : o tamanho do OpenZFS em gibibytes (GiB) • `Shared_Storage_Linux` : o ponto de montagem do armazenamento compartilhado • `Enginframe_installer` — O link para download de EnginFrame • `Session_Manager_Broker_Installer` : o link para download do Session Manager Broker 4. Salve e feche o arquivo app.py.	

Tarefa	Descrição	Habilidades necessárias

Implante a solução.	Execute os seguintes comandos em sequência:
	`cdk bootstrap`
	`cdk deploy Assets-Stack Parameters-Stack`
	`cdk deploy Elastic-Vdi-Infrastructure`
	Quando a implantação estiver concluída, as duas saídas a seguir serão retornadas:
	• `Elastic-Vdi-Infrastructure.EnginFrameURL` — O endereço HTTPS do EnginFrame portal
	• `Elastic-Vdi-InfrastruSecretEFadminPassword` : o nome do recurso da Amazon (ARN) do segredo que contém a senha do usuário efadmin
	Anote esses valores. Você os usa posteriormente nesse padrão.
		Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Implante a frota de servidores Linux.	1. Faça login no AWS Management Console e abra o CloudFormation console. 2. Selecione Criar pilha e Com novos recursos. 3. Na pasta cloudformation_files, selecione o arquivo.yaml. dcv-linux-fleet 4. Na página Especificar detalhes da pilha, defina os seguintes parâmetros: • Nome da pilha: o nome da pilha. • DcvFleet— O nome da frota NICE DCV. Não deixe esse valor em branco nem use espaços. • InstanceType— O tipo de instância da frota. • RootVolumeSize— O tamanho do volume raiz da EC2 instância Linux Amazon. • MinSize— O número mínimo de nós que devem estar disponíveis e não executar nenhuma sessão de DCV. Por exemplo, se você inserir 2, a solução começa com 2 nós. Quando um usuário cria uma	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	sessão, o número de nós disponíveis diminui para 1, e a solução cria outro nó para manter o mínimo. • MaxSize— O número máximo de nós na frota. Os usuários não podem iniciar novas sessões se o máximo tiver sido atingido. • BillingTagName— O nome da tag usada para cobrança. Esse nome de tag deve ser diferente daquele usado para a pilha do Windows. • BillingTagValue— O valor da tag usado para faturamento. 5. Conclua o assistente de criação da pilha e escolha Enviar para começar a criar a pilha.	

Tarefa	Descrição	Habilidades necessárias
Implante a frota de servidores Windows.	1. Faça login no AWS Management Console e abra o CloudFormation console. 2. Selecione Criar pilha e Com novos recursos. 3. Na pasta cloudformation_files, selecione o arquivo.yaml. dcv-windows-fleet 4. Na página Especificar detalhes da pilha, defina os seguintes parâmetros: • Nome da pilha: o nome da pilha. • DcvFleet— O nome da frota NICE DCV. Não deixe esse valor em branco nem use espaços. • InstanceType— O tipo de instância da frota. • RootVolumeSize— O tamanho do volume raiz da EC2 instância Amazon do Windows. • MinSize— O número mínimo de nós que devem estar disponíveis e não executar nenhuma sessão de DCV. • MaxSize— O número máximo de nós na frota.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	• BillingTagName— O nome da tag usada para cobrança. Esse nome de tag deve ser diferente daquele usado para a pilha Linux. • BillingTagValue— O valor da tag usado para faturamento. 5. Conclua o assistente de criação da pilha e escolha Enviar para começar a criar a pilha.	

Acesse o ambiente implantado

Tarefa	Descrição	Habilidades necessárias
Recupere a senha do EnginFrame administrador.	A conta de EnginFrame administração é chamada efadmin e a senha é armazenada AWS Secrets Manager como um segredo. O ARN do segredo é gerado dinamicamente e é visível na saída da implantação. AWS CDK 1. No épico anterior, na história Implantar a solução, abaixo da `Elastic-VDI-Infrastructure.SecretEFadminPassw`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`ord` saída, encontre o ARN do segredo gerado. 2. Siga um destes procedimentos para recuperar o segredo: • Use o console do Secrets Manager. Para obter mais informações, consulte Recuperar segredos. • Digite o comando get-secret-value . `aws secretsmanager get-secret-value \ --secret-id <secret_arn> \ --query SecretString \ --output text`	
Acesse o EnginFrame portal.	1. No épico anterior, na história Implantar a solução, abaixo da `Elastic-Vdi-Infrastructure.EnginFrameURL` saída, encontre o endereço HTTPS do EnginFrame portal. 2. Em um navegador da web, digite o endereço HTTPS do portal. 3. Insira as credenciais do usuário efadmin.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Inicie uma sessão do Windows.	1. No EnginFrame portal, no menu, escolha Área de trabalho do Windows. 2. Quando você for solicitado a entrar como administrador do Windows, digite a mesma senha usada para o usuário efadmin. 3. Confirme se a sessão do Windows foi iniciada com êxito.	Arquiteto de nuvem
Inicie uma sessão do Linux.	1. No EnginFrame portal, no menu, escolha Linux Desktop. 2. Quando você for solicitado a entrar, insira as credenciais do usuário efadmin. 3. Confirme se a sessão do Linux foi iniciada com sucesso.	Arquiteto de nuvem

Limpeza

Tarefa	Descrição	Habilidades necessárias
Exclua as pilhas.	No CloudFormation console, exclua as pilhas das frotas de servidores Windows e Linux. Para obter mais informações, consulte Excluir uma pilha.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Exclua a infraestrutura.	Exclua a infraestrutura implantada usando o seguinte AWS CDK comando: `cdk destroy --all`	Arquiteto de nuvem

Solução de problemas

Problema	Solução
A implantação não foi concluída porque foi interrompida.	Siga as instruções do épico Limpar e repita esse padrão para implantar o ambiente novamente.

Recursos relacionados

- NICE DCV
- BOM EnginFrame

Nuvem híbrida

Tópicos

- Configure uma extensão de datacenter para a VMware nuvem na AWS usando o modo vinculado híbrido
- Configurar o VMware vRealize Automation para provisionar VMs na VMware nuvem na AWS
- Integre o VMware vRealize Network Insight com a VMware nuvem na AWS
- Migre VMs para a VMware nuvem na AWS usando a migração assistida do sistema operacional HCX
- Envie registros do VMware Cloud on AWS para o Splunk usando o VMware Aria Operations for Logs
- Configure um pipeline de CI/CD para cargas de trabalho híbridas no Amazon ECS Anywhere usando o AWS CDK e GitLab
- Mais padrões

Configure uma extensão de datacenter para a VMware nuvem na AWS usando o modo vinculado híbrido

Criado por Deepak Kumar (AWS)

Resumo

Aviso: a partir de 30 de abril de 2024, o VMware Cloud on não AWS é mais revendido AWS nem por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu AWS representante para obter detalhes.

Esse padrão descreve como você pode usar o Hybrid Linked Mode para visualizar e gerenciar inventários em um datacenter local e em um data center definido por software (SDDC) VMware na nuvem na AWS usando uma única interface vSphere Client. VMware

Ao configurar o Modo Vinculado Híbrido, você pode migrar suas máquinas virtuais (VMs) e aplicativos locais para o SDDC na nuvem. Suas equipes de TI podem então gerenciar seus recursos baseados em nuvem com VMware ferramentas familiares e sem a necessidade de novas ferramentas. Você também pode garantir operações consistentes e administração simplificada usando o VMware Cloud Gateway Appliance.

Esse padrão fornece duas opções para configurar o Hybrid Linked Mode, mas você só pode usar uma opção por vez. A primeira opção instala o Cloud Gateway Appliance e o usa para se conectar do vCenter Server on-premises ao SDDC na nuvem. A segunda opção configura o Hybrid Linked Mode a partir do SDDC na nuvem.

Pré-requisitos e limitações

Pré-requisitos (ambas as opções)

- Um datacenter on-premises existente e um SDDC de nuvem.
- Uma conexão existente entre o datacenter on-premises e o SDDC na nuvem, usando o AWS Direct Connect, uma VPN ou ambos.
- O datacenter on-premises e o SDDC na nuvem são sincronizados com o network time protocol (NTP – protocolo de tempo de rede) ou outra fonte de horário autorizada.
- A latência máxima de um tempo de ida e volta entre o datacenter on-premises e o SDDC na nuvem não excede 100 ms.

- Administradores de nuvem com acesso ao seu ambiente on-premises.
- O nome de domínio totalmente qualificado (FQDN) do vCenter Server deve ser resolvido para um endereço IP privado.

Pré-requisitos para a Opção 1

- O ambiente on-premises deve ser executado no vSphere 6.5.0d ou superior.
- O Cloud Gateway Appliance e o vCenter Server podem se comunicar pelo AWS Direct Connect, por uma VPN ou por ambos.
- O Cloud Gateway Appliance atende aos requisitos de hardware.
- As portas do firewall estão abertas.

Pré-requisitos para a Opção 2

- O vCenter Server on-premises é executado no vSphere 6.0 Update 3 ou superior, ou no vSphere 6.5.0d ou superior.
- As credenciais de logon estão disponíveis para o domínio de autenticação única (SSO) do vSphere no on-premises.
- Os usuários no ambiente on-premises têm acesso somente de leitura ao nome distinto básico (Base DN).
- O servidor DNS (Sistema de Nomes de Domínio) local está configurado para o VMware Management Gateway.
- Implemente testes de conectividade de rede usando o Validador de VMware Conectividade.
- As portas do firewall estão abertas.

Limitações

- O Hybrid Linked Mode só pode conectar um domínio on-premises do modo vinculado aprimorado do vCenter Server.
- O Hybrid Linked Mode oferece suporte somente ao vCenter Server on-premises executando a versão 6.7 ou superior.

Arquitetura

O diagrama a seguir mostra as duas opções para configurar o Hybrid Linked Mode.

Migração de diferentes tipos de workload usando o Hybrid Linked Mode

O Modo Vinculado Híbrido suporta a migração de cargas de trabalho entre um data center local e um SDDC na nuvem usando uma migração a frio ou uma migração ativa com o vSphere vMotion. VMware Os fatores que devem ser considerados ao escolher o método de migração incluem o tipo e a versão do switch virtual, o tipo de conexão com o SDDC na nuvem e a versão do hardware virtual.

Uma migração a frio é apropriada para o tempo de inatividade VMs dessa experiência. Você pode desligá-los VMs, migrá-los e depois ativá-los novamente. O tempo de migração é mais rápido porque não há necessidade de copiar a memória ativa. Recomendamos usar uma migração a frio para aplicativos que aceitam tempo de inatividade (por exemplo, aplicativos de nível 3 ou workloads de desenvolvimento e teste). Se você VMs não tiver tempo de inatividade, considere uma migração ao vivo usando o vMotion para seus aplicativos essenciais.

O diagrama a seguir fornece uma visão geral dos diferentes tipos de migração de workload usando o Hybrid Linked Mode.

Ferramentas

- VMware O Cloud on AWS é uma oferta de nuvem integrada desenvolvida em conjunto pela AWS e. VMware
- VMware O Cloud Gateway Appliance permite vários casos de uso de nuvem híbrida em que os recursos locais estão conectados aos recursos da nuvem.
- VMware O vSphere é a plataforma VMware de virtualização do vSphere, que transforma data centers em infraestruturas computacionais agregadas que incluem recursos de CPU, armazenamento e rede.

Épicos

Opção 1: use o Hybrid Linked Mode com o Cloud Gateway Appliance

Tarefa	Descrição	Habilidades necessárias
Configure o Cloud Gateway Appliance.	1. Faça login no console VMware Cloud on AWS e baixe o Cloud Gateway Appliance. 2. Instale o Cloud Gateway Appliance em seu ambiente on-premises com as duas etapas a seguir: • Selecione Iniciar configuração e implante o Cloud Gateway Appliance . • Configure o Hybrid Linked Mode. Para obter mais informaçõ es e etapas detalhadas, consulte Configurando o modo vinculado híbrido usando o vCenter Cloud Gateway Appliance na documentação. VMware	Administrador de nuvem

Opção 2: use o Hybrid Linked Mode do SDDC na nuvem

Tarefa	Descrição	Habilidades necessárias
Configure o Hybrid Linked Mode a partir do SDDC na nuvem.	1. Faça login na VMware nuvem no console da AWS e use o validador de conectividade para verificar toda a conectividade de rede necessária. Para obter mais informações sobre isso, consulte Validar a conectividade de rede para o Modo Vinculado Híbrido na VMware documentação. 2. Faça login no vSphere Client do SDDC na nuvem, selecione Menu, então Administração e, em seguida, selecione Domínios. 3. Na seção Nuvem híbrida, selecione Domínios vinculados e conecte-se ao seu vCenter Server on-premises. 4. Adicione uma fonte de identidade ao domínio SDDC do Lightweight Directory Access Protocol (LDAP) na nuvem. Para obter mais informaçõ es sobre isso, consulte Adicionar uma fonte de identidade ao domínio	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	LDAP do SDDC na documentação. VMware	

Recursos relacionados

- Como configurar o Hybrid Linked Mode
- Configurando o modo vinculado híbrido para VMware nuvem na AWS

Configurar o VMware vRealize Automation para provisionar VMs na VMware nuvem na AWS

Criado por Deepak Kumar (AWS)

Resumo

Aviso: a partir de 30 de abril de 2024, o VMware Cloud on não AWS é mais revendido AWS nem por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu AWS representante para obter detalhes.

VMware O vRealize Automation é um software de automação que você pode usar para solicitar e gerenciar recursos de TI. Ao optar por configurar o vRealize Automation com a VMware nuvem na AWS, você pode automatizar a entrega de máquinas virtuais (VMs), aplicativos e serviços de TI em vários datacenters e ambientes de nuvem.

Suas equipes de TI podem então criar itens de catálogo para configurar o provisionamento de serviços e os recursos operacionais que seus usuários podem solicitar e usar com suas ferramentas existentes do vRealize Automation. Você também pode melhorar sua agilidade e eficiência de TI integrando o VMware Cloud on AWS com o vRealize Automation Cloud Assembly.

Esse padrão descreve como configurar o VMware vRealize Automation para criar VMs ou aplicar automaticamente recursos no VMware Cloud on AWS.

Pré-requisitos e limitações

Pré-requisitos

- Um datacenter local existente e um data center definido por software (SDDC) na VMware nuvem na AWS. Para obter mais informações sobre o SDCC na nuvem, consulte Sobre data centers definidos por software na documentação. VMware
- Uma conexão existente entre o datacenter on-premises e o SDDC na nuvem, usando o AWS Direct Connect (baseado em política ou rota), uma VPN ou ambos.
- O datacenter on-premises e o SDDC na nuvem são sincronizados com o network time protocol (NTP – protocolo de tempo de rede) ou outra fonte de horário autorizada.
- A latência máxima de um tempo de ida e volta entre o datacenter on-premises e o SDDC na nuvem não excede 100 ms.

- O nome de domínio totalmente qualificado (FQDN) do vCenter Server deve ser resolvido para um endereço IP privado.
- Usuários do Cloud SDDC com acesso ao seu ambiente on-premises.
- Acesso do proprietário da organização no perfil de serviço vRealize Automation Cloud Assembly.
- Usuários finais com permissão no vRealize Automation Service Broker para consumir o serviço.
- O intervalo Classless Inter-Domain Routing (CIDR) do datacenter local deve estar aberto para a geração de tokens de API a partir do console Cloud VMware on AWS. A lista a seguir fornece as funções mínimas necessárias para gerar tokens de API:
  - Membro da organização
  - Proprietário da organização
  - Funções de serviço — VMware Nuvem na AWS
  - Administrador
  - Administrador do NSX Cloud
  - Auditor do NSX Cloud

Para obter mais informações sobre isso, consulte Opções de conectividade para VMware nuvem na AWS no blog SDDCs da rede de parceiros da AWS.

Limitações

- Você só pode configurar 20 contas de VMware nuvem com endpoints públicos em um vRealize Automation. Para obter mais informações sobre isso, consulte Máximos de escalabilidade e simultaneidade na documentação. VMware

Versões do produto

- vRealize Automation versão 8.x ou superior
- VMware vRealize Identity Manager versão 3.x ou posterior
- VMware vRealize Suite Lifecycle Manager versão 8.x ou posterior

Arquitetura

O diagrama a seguir mostra os serviços do vRealize Automation que podem usar a infraestrutura de ambientes locais e VMware em nuvem na AWS.

VMware Componentes de montagem em nuvem

VMware O Cloud Assembly é um componente essencial do vRealize Automation e você pode usá-lo para implantar, provisionar VMs e computar recursos. A tabela a seguir descreve os componentes do VMware Cloud Assembly que devem ser configurados para provisionamento VMs no VMware Cloud on AWS.

Componentes	Definição
Conta na nuvem	A Conta Cloud fornece detalhes da conexão (por exemplo, nome do servidor, nome de usuário e senha, chave de acesso e token de API). VMware O Cloud Assembly usa a Cloud Account para coletar um inventário dos seus recursos.
Zonas de nuvem	As zonas de nuvem identificam limites de recursos na conta da nuvem (por exemplo, regiões da AWS e o SDDC na nuvem). As zonas de nuvem associam recursos de computação ao projeto Cloud Assembly.
Projetos	Um projeto é uma entidade lógica que consiste em usuários e recursos, como zonas de nuvem. Também consiste em cotas de recursos e políticas de nomenclatura de VM que são usadas ao criar a VM.
Mapeamentos de variações	O mapeamento de variações fornece informaçõ es sobre a capacidade da VM (por exemplo, número CPUs e quantidade de memória) que são usadas no Cloud Template.
Mapeamentos de imagens	O mapeamento de imagens mapeia o modelo de VM do VMware vSphere e a imagem da Amazon Web Services (AWS) que são usados no modelo de nuvem. Para obter mais informações sobre isso, consulte Saiba mais

	sobre mapeamentos de imagem no vRealize Automation na documentação. VMware
Perfil de rede	O perfil de rede controla a decisão de posiciona mento para escolher uma rede durante o provisionamento da VM.
Perfil de armazenamento	O perfil de armazenamento controla a decisão de posicionamento para escolher o armazenam ento durante o provisionamento da VM.
Modelos de nuvem	VMware Os modelos de nuvem são um componente importante do vRealize Automatio n porque definem o provisionamento e a orquestração da infraestrutura de nuvem. Os modelos de nuvem são especificações para os recursos e incluem o tipo de recurso, as propriedades do recurso e as informações a serem coletadas dos usuários.

Ferramentas

- VMware vRealize Automation — O vRealize Automation é uma plataforma de automação de infraestrutura com gerenciamento de estado e conformidade orientados por eventos. Ele foi projetado para ajudar as organizações a controlar e proteger nuvens de autoatendimento, automação multinuvem com governança e entrega de infraestrutura DevOps baseada.
- VMware Nuvem na AWS — A VMware nuvem na AWS é uma oferta de nuvem integrada desenvolvida em conjunto pela AWS e. VMware

Épicos

Gerar os tokens da API

Tarefa	Descrição	Habilidades necessárias
Gere os tokens de API da sua conta do VMware Cloud on AWS.	1. Faça login no VMware Cloud Console. 2. Na barra de ferramentas de serviços em VMware nuvem, escolha Minha conta e, em seguida, escolha Token de API. 3. Insira um nome para seu token de API, forneça a vida útil necessária e defina os escopos do token. 4. Escolha a caixa de seleção Abrir ID e, em seguida, escolha Gerar. 5. Registre as credenciais do token da API. Para obter mais informações sobre isso, consulte Como faço para gerar tokens de API na VMware documentação.	Administrador de nuvem

Instale o vRealize Automation em seu datacenter on-premises

Tarefa	Descrição	Habilidades necessárias
Download do software necessário.	Baixe o arquivo ISO do VMware vRealize Suite no Meu VMware Portal. Esse	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	pacote contém o vRealize Suite Lifecycle Manager, o VMware Identity Manager e o vRealize Automation.	
Instale o software.	Instale o software e conecte-se à sua SDCC na nuvem seguindo as instruções de Instalação do vRealize Suite Lifecycle Manager com o Easy Installer for vRealize Automation VMware and Identity Manager na documentação. VMware ⚠ Important Certifique-se de que o seguinte esteja disponível para sua instalação: • A configuração local do VMware vCenter Server e as credenciais de login • Os detalhes da rede para o IP e a sub-rede do vRealize Automation • A chave de licença do vRealize Automation	Administrador de nuvem, arquiteto de nuvem

Conecte a VMware nuvem na AWS com o VMware Cloud Assembly

Tarefa	Descrição	Habilidades necessárias
Configure suas contas na nuvem.	1. No VMware Cloud Console, abra a guia Infraestrutura, escolha Gerenciar — Contas na nuvem e, em seguida, escolha Adicionar contas na nuvem. 2. Escolha VMware Cloud on AWS como o tipo. 3. Cole as informações do token da API que você registrou anteriormente. Isso preenche todas as nuvens disponíveis SDDCs em sua organização VMware Cloud on AWS. 4. Escolha o SDCC na nuvem necessário e, em seguida, forneça o nome de usuário e a senha do vCenter para o SDDC. 5. Depois de ser autenticado com sucesso, você pode visualizar a conta integrada do VMware Cloud on AWS com o status OK. Para obter mais informaçõ es sobre isso, consulte Criar uma conta na VMware nuvem Cloud on AWS no vRealize	Arquiteto de nuvem, administr ador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Automation na VMware documentação.	
Configure o projeto.	1. No Console do VMware Cloud, abra a guia Projetos e escolha Novo projeto. 2. Insira o nome do seu projeto. 3. Abra a guia Cloud Zones e escolha a conta padrão VMware Cloud on AWS Cloud.	Administrador de nuvem
Configure a zona de nuvem.	1. No VMware Cloud Console, abra Cloud Zones e escolha a zona de nuvem para seu data center SDDC. 2. Por padrão, `cloudadmin@vmc.local` (essa é a ID de usuário local padrão para o vCenter do SDDC na nuvem) só tem acesso ao provisionamento no `Compute-ResourcePool`. 3. Abra a guia Computação em Zonas de nuvem e escolha Compute-. ResourcePool	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure o mapeamento de variações.	1. Abra a guia Mapeamentos de variações e crie um novo mapeamento de variações. 2. Insira o nome da variação, escolha a conta VMware Cloud on AWS e, em seguida, forneça o número de v CPUs e a quantidade de memória.	Administrador de nuvem
Configure o mapeamento de imagens.	1. Abra Mapeamentos de imagem e crie um novo mapeamento de imagem. 2. Insira o nome da imagem. 3. Escolha a conta VMware Cloud on AWS e forneça os modelos de conta na nuvem que são necessári os.	Administrador de nuvem
Configure o perfil de rede.	1. Abra o Perfil de rede e crie um novo perfil de rede. 2. Insira o nome do perfil de rede. 3. Abra a guia Rede e escolha a rede existente que você deseja usar para provision amento.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Configure o perfil de armazenamento.	1. Abra o Perfil de armazenamento e escolha Novo perfil de armazenamento. 2. Insira o nome do perfil de armazenamento. 3. Na página Policies (Políticas), escolha Create a policy (Criar uma política). 4. Escolha Workload Datastore. Por padrão, `cloudadmin@vmc.local` só tem acesso ao provisionamento no armazenamento de datastore da workload.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Crie o modelo de nuvem.	1. Abra a guia Design, escolha Modelos de nuvem e, em seguida, escolha Novo de e Tela em branco. 2. Forneça o nome e a descrição do modelo de nuvem. 3. Selecione o projeto que você criou anteriormente. 4. Na página de design de recursos do modelo de nuvem, arraste os componentes para a tela em branco de acordo com seus requisitos. 5. Escolha Testar para testar o modelo e corrigir quaisquer problemas. 6. Escolha Deploymen t e forneça o nome da implantação para implantar VMs o. Para obter mais informações sobre isso, consulte Criar um modelo básico de nuvem na VMware documentação.	Administrador de nuvem

Recursos relacionados

- Conectar o vRealize Automation versão 8.x ao seu SDDC:
- Implemente um SDDC a partir da VMware nuvem no console da AWS

- Integração do AWS Direct Connect com a VMware nuvem na AWS

Integre o VMware vRealize Network Insight com a VMware nuvem na AWS

Criado por Deepak Kumar (AWS), Piotr Pitera (AWS) e Sachin Trivedi (AWS)

Resumo

Aviso: a partir de 30 de abril de 2024, o VMware Cloud on não AWS é mais revendido AWS nem por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu AWS representante para obter detalhes.

Esse padrão descreve como integrar o VMware vRealize Network Insight com o VMware Cloud on AWS e inspecionar o fluxo de tráfego de suas máquinas virtuais. Essa integração também ajuda você a planejar migrações de aplicativos para o VMware Cloud on AWS.

O vRealize Network Insight oferece visibilidade da sua infraestrutura de rede. Ele fornece recursos de monitoramento e análise de rede para melhorar a segurança, reduzir os riscos de migração e otimizar o desempenho. Você pode usar essa ferramenta para monitorar os fluxos de tráfego de suas máquinas virtuais e visualizar as regras de segurança recomendadas com base no tráfego observado. Para obter mais informações sobre o vRealize Network Insight, consulte a VMware documentação.

VMware O Cloud on AWS é um serviço pay-as-you-go (sob demanda) que permite que empresas de todos os tamanhos executem cargas de trabalho em ambientes de nuvem VMware baseados no vSphere usando uma ampla variedade de. Serviços da AWS Você pode começar com um mínimo de 2 hosts por cluster SDDC e aumentar a escala verticalmente até 16 hosts por cluster em seu ambiente de produção. Para obter mais informações, consulte o AWS site VMware Cloud on. Para saber mais SDDCs, consulte Sobre data centers definidos por software na documentação. VMware

Pré-requisitos e limitações

Pré-requisitos

- VMware Nuvem no AWS SDDC, implantado

Limitações

- Para ver as limitações conhecidas, consulte a VMware documentação.

Versões do produto

- vRealize Network Insight versão 5.0.0
- VMware Nuvem no AWS SDDC versão 1.24

Arquitetura

Pilha de tecnologia de origem

- vRealize Network Insight

Pilha de tecnologias de destino

- VMware Nuvem ativada AWS

Arquitetura de destino

O diagrama a seguir mostra a conectividade entre o VMware Cloud on AWS e o vRealize Network Insight no local.

Ferramentas

- VMware O Cloud on AWS é uma oferta de nuvem integrada desenvolvida em conjunto por e. AWS VMware
- VMware O vRealize Network Insight é uma ferramenta de monitoramento e análise que fornece visibilidade da infraestrutura de rede para planejamento e solução de problemas de segurança.

Épicos

Configure seu ambiente para o vRealize Network Insight

Tarefa	Descrição	Habilidades necessárias
Crie uma conta VMware de usuário.	Crie uma conta de VMware usuário ou faça login na sua VMware conta existente.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Para abrir uma nova conta: 1. Inscreva-se em uma conta VMware do Customer Connect preenchendo o formulário de registro. Novos usuários receberão um e-mail para ativar suas contas. 2. Insira o código de autenticação do e-mail. 3. Faça login no Customer Connect.	
Baixe os arquivos OVA para o vRealize Network Insight.	Baixe os arquivos OVA para o vRealize Network Insight:. 1. Navegue até a página de download VMware do produto em https://my.vmware.com/group/vmware/home. 2. Pesquise o vRealize Network Insight. 3. Baixe a plataforma mais recente do vRealize Network Insight versão 5.0.0 e os arquivos OVA do coletor.	Administrador de nuvem
Implante o vRealize Network Insight.	Para obter instruções de implantação, consulte a VMware documentação.	Administrador de nuvem

Adicionar uma fonte de dados e um coletor

Tarefa	Descrição	Habilidades necessárias
Adicione uma fonte de dados.	1. Faça login no vRealize Network Insight. 2. Escolha Configurações, Contas e Fontes de Dados, Adicionar Fonte. 3. Em Tipo, escolha Servidor vCenter local. Para obter mais informações, consulte a documentação do VMware .	Administrador de nuvem
Configure um coletor para a fonte de dados.	Para obter instruções, consulte a VMware documentação.	Administrador de nuvem

Analise as dependências do aplicativo

Tarefa	Descrição	Habilidades necessárias
Crie uma aplicação.	Se você não tiver um aplicativo existente no vRealize Network Insight, siga as etapas na VMware documentação para criar um.	Administrador de nuvem
Descubra e analise seu aplicativo.	1. Use o vRealize Network Insight para descobrir seu aplicativo. Para obter instruções, consulte a VMware documentação.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	2. Analise seu aplicativo. Para obter instruções, consulte a VMware documentação.	

Recursos relacionados

- Implemente um VMware SDDC na AWS usando o VMware Cloud on AWS (orientação AWS prescritiva)
- Configurar uma extensão de data center para o VMware Cloud on AWS usando o modo vinculado híbrido (AWS orientação prescritiva)
- Migre o VMware SDDC para a VMware nuvem AWS usando o VMware HCX (AWS orientação prescritiva)
- VMware Documentação do vRealize Network Insight (VMware site)

Migre VMs para a VMware nuvem na AWS usando a migração assistida do sistema operacional HCX

Criado por Deepak Kumar (AWS) e Himanshu Gupta (AWS)

Resumo

> Aviso: a partir de 30 de abril de 2024, o VMware Cloud on não AWS é mais revendido AWS nem por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu AWS representante para obter detalhes.

Esse padrão descreve como migrar uma máquina virtual (VM) de um ambiente não vSphere para a VMware nuvem na Amazon Web Services (AWS) usando a migração assistida por sistema operacional (OSAM).

O OSAM faz parte da VMware Hybrid Cloud Extension (HCX), que está incluída no VMware Cloud on AWS. Você pode usar o OSAM para migrar um ambiente que não seja do vSphere, como VMware KVM ou Hyper-V, para a nuvem na AWS. VMware O OSAM usa o software Sentinel, que você instala em uma VM convidada Windows ou Linux para ajudar na replicação da VM do seu ambiente local para um data center definido por software (SDDC) na nuvem na AWS. VMware

Esse padrão explica como habilitar o OSAM, instalar o software Sentinel em uma VM do Windows, conectar-se e registrar-se com um dispositivo HCX Sentinel Gateway (SGW) no local de origem e estabelecer uma conexão de encaminhamento com um dispositivo HCX Sentinel Data Receiver (SDR) no local de destino para iniciar a migração.

Para obter mais informações sobre o OSAM, consulte a VMware documentação.

Pré-requisitos e limitações

Pré-requisitos

- Instale o HCX em seus ambientes de origem e destino. Para os pré-requisitos do HCX, consulte Migrar VMware SDDC para a VMware nuvem na AWS VMware usando o HCX na documentação do AWS Prescriptive Guidance.
- Para os pré-requisitos do OSAM, consulte a lista de verificação de instalação na documentação. VMware

- Para obter informações sobre a porta OSAM, consulte os requisitos de porta VMware HCX no site VMware Ports and Protocols.

Limitações

- VMware Limites de configuração do HCX 4.2.0
- Considerações sobre a implantação do OSAM
- Sistemas operacionais convidados compatíveis
- Considerações sobre o sistema operacional convidado

Versões do produto

- VMware HCX 4.2.0
- VMware SDDC 1.12

Arquitetura

O diagrama a seguir mostra como o HCX OSAM trabalha com o software Sentinel para replicar o que não é vSphere VMs do seu ambiente local para o Cloud on AWS. VMware

O OSAM consiste em três componentes:

- O dispositivo Sentinel Gateway (SGW), usado para conectar e encaminhar cargas de trabalho e aplicativos no ambiente baseado na origem VMware
- O Sentinel Data Receiver (SDR), que é usado no ambiente Cloud VMware on AWS de destino para receber cargas de trabalho migradas da fonte
- O software Sentinel, que deve ser instalado em cada VM convidada que você deseja migrar

O OSAM usa o software Sentinel instalado no Windows ou Linux como convidado VMs para auxiliar na replicação de uma VM do local para um SDDC. VMware O software Sentinel que você instala no convidado VMs coleta as configurações do sistema da VM convidada e auxilia na replicação de dados. Essas informações também são usadas para criar o inventário de convidados VMs para migração e ajudam a preparar os discos na VM de réplica para fins de replicação e migração.

Ferramentas

- VMware HCX 4.2.0
- VMware Nuvem no AWS SDDC

Épicos

Configurar o HCX

Tarefa	Descrição	Habilidades necessárias
Implemente o HCX Cloud e o HCX Connector.	Siga as instruções em HCX Connector e HCX Cloud Installations na VMware documentação.	Administrador de nuvem, administrador de sistemas

Configurar o OSAM e migrar VMs

Tarefa	Descrição	Habilidades necessárias
Instale o HCX Sentinel.	Para instalar o Sentinel no Linux: 1. No vCenter Server para o HCX Connector, escolha Interconectar, Malha de serviços em vários sites, Gerenciamento do Sentinel. 2. Escolha Baixar pacote Linux. 3. Instale o agente Sentinel em uma máquina Linux. Para obter mais informações, consulte Baixar e instalar o	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	software HCX Sentinel Agent na documentação. VMware	

Tarefa	Descrição	Habilidades necessárias
Migrar. VMs	Para migrar seus grupos VMs internos (chamados de grupos de mobilidade), siga estas etapas: 1. No vSphere Client, no plug-in HCX, escolha Serviços, Migração. 2. Escolha Migrate (Migrar). 3. Escolha Inventário não vSphere, Conexões remotas. Isso mostrará a lista na VMs qual você instalou o HCX Sentinel. 4. Em Nome do grupo, insira o nome do grupo de mobilidade que você deseja criar para VMs o. 5. Escolha o VMs que você deseja migrar e, em seguida, escolha Adicionar para adicioná-lo ao grupo de mobilidade. 6. Para cada VM: a. Selecione o contêiner de computação de destino. b. Selecione o armazenamento de destino. c. Selecione o perfil de migração. d. Selecione a pasta de destino.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	7. Para iniciar o processo de migração, escolha Ir. O HCX valida suas seleções de VM antes do início da migração. Para obter mais informaçõ es, consulte Migração de máquinas virtuais com grupos de mobilidade e Monitoram ento e estimativa da migração com grupos de mobilidade na documentação. VMware	

Recursos relacionados

VMware documentação:

- VMware Guia do usuário do HCX
- Instale a lista de verificação B - HCX com um ambiente de destino VMC SDDC
- VMware HCX na VMware nuvem na AWS
- Migração assistida do sistema operacional HCX para VMware nuvem na AWS
- VMware Notas de lançamento do HCX 4.2.1

Envie registros do VMware Cloud on AWS para o Splunk usando o VMware Aria Operations for Logs

Criado por Deepak Kumar (AWS) e Piotr Pitera (AWS)

Resumo

Aviso: a partir de 30 de abril de 2024, o VMware Cloud on não AWS é mais revendido AWS nem por seus parceiros de canal. O serviço continuará disponível pela Broadcom. Recomendamos que você entre em contato com seu AWS representante para obter detalhes.

Esse padrão descreve como encaminhar AWS eventos ou registros do VMware Cloud on para um syslog ou um endpoint HTTP, como o Splunk, usando o VMware Aria Operations for Logs.

VMware O Aria Operations for Logs é uma ferramenta de análise de registros que oferece visibilidade aprimorada e solução de problemas acelerada no AWS ambiente VMware Cloud on. Você pode configurar essa ferramenta para enviar todos ou uma parte dos registros ou eventos no VMware Cloud on AWS para um syslog ou endpoint HTTP. O endpoint pode ser um endpoint de software como serviço (SaaS) ou um endpoint local, como o Splunk. (Esse padrão fornece as instruções para o Splunk.) Para saber mais sobre VMware Aria Operations for Logs, consulte a VMware documentação.

VMware O Cloud on AWS é um serviço pay-as-you-go (sob demanda) que permite que empresas de todos os tamanhos executem cargas de trabalho em ambientes de nuvem VMware baseados no vSphere usando uma ampla variedade de. Serviços da AWS Você pode começar com um mínimo de 2 hosts por cluster de data center definido por software (SDDC) e escalar até 16 hosts por cluster em seu ambiente de produção. Para obter mais informações, consulte o AWS site VMware Cloud on. Para saber mais SDDCs, consulte Sobre data centers definidos por software na documentação. VMware

Pré-requisitos e limitações

Pré-requisitos

- Splunk, configurado localmente

Limitações

Você pode se inscrever para uma assinatura de teste gratuita do VMware Aria Operations for Logs. Essa assinatura é válida por 30 dias e tem as seguintes limitações:

- Tamanho máximo de registros que você pode encaminhar: 50 GB de registros por dia
- Número máximo de configurações de encaminhamento de registros que você pode criar: 10
- Número máximo de configurações de encaminhamento de registros que você pode ativar: 5

Para acessar todos os recursos do serviço, você deve fazer o upgrade para uma assinatura premium.

Para obter mais informações sobre assinaturas de teste e premium, consulte Assinaturas e faturamento do VMware Aria Operations for Logs (SaaS) na documentação. VMware Para obter mais informações sobre limites de uso, consulte Limitações de uso de recursos na VMware documentação.

Versões do produto

- VMware Cloud on AWS SDDC versão 1.24
- VMware Aria Operations for Logs versão 8.10
- Splunk local, versão 9.x

Arquitetura

Pilha de tecnologia de origem

- VMware Nuvem ativada AWS
- VMware Operações Aria para registros

Pilha de tecnologias de destino

- Splunk local

Arquitetura de destino

O diagrama a seguir mostra a conectividade entre um data center corporativo e o VMware Aria Operations for Logs in VMware Cloud on AWS.

Ferramentas

- VMware O Cloud on AWS é uma oferta de nuvem integrada desenvolvida em conjunto por e. AWS VMware
- VMware O Aria Operations for Logs é uma ferramenta de análise e solução de problemas de registros para o VMware Cloud on AWS.

Épicos

Implemente um SDDC e habilite a operação VMware Aria para registros

Tarefa	Descrição	Habilidades necessárias
Implemente uma VMware nuvem no AWS SDDC.	Siga as instruções em Implantar um VMware SDDC AWS usando o VMware Cloud on AWS na orientação AWS prescritiva.	Arquiteto de nuvem, administrador de nuvem
Inscreva-se no VMware Aria Operations for Logs.	Para obter instruções, consulte a VMware documentação.	Arquiteto de nuvem

Implemente um proxy na nuvem

Tarefa	Descrição	Habilidades necessárias
Implemente um proxy na nuvem.	Para encaminhar registros para uma instância local do Splunk, você deve adicionar um proxy de nuvem para o VMware Aria Operations for Logs. Esse proxy recebe informações do data center local e as envia para a	Administrador de nuvem, arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	VMware Aria Operations for Logs para análise. Para baixar e instalar o proxy na nuvem: 1. Certifique-se de que as portas 443, 22 e 514 estejam abertas entre seu ambiente local e VMware o Cloud on. AWS Para portas adicionais, você pode usar 1514/TCP ou 6514/TCP. Para obter mais informaçõ es sobre portas, consulte Recomendações de firewall do VMware Aria Operation s for Logs na VMware documentação. 2. Faça login no VMware Aria Operations for Logs. 3. Na página inicial, escolha Adicionar coletor no widget. 4. Na tela do Cloud Proxy Virtual Appliance, copie a chave do token. Você deve usar essa chave dentro de 24 horas para concluir as etapas a seguir. 5. Escolha o link de download do arquivo OVA. 6. Navegue até o cliente web VMware vSphere, escolha	

Tarefa	Descrição	Habilidades necessárias
	seu cluster e selecione Implantar modelo OVF. 7. Quando você for solicitado a fornecer a chave, cole a chave de token que você copiou na etapa 4. 8. Escolha Concluir para instalar o proxy na nuvem.	

Encaminhe os registros para um endpoint local do Splunk

Tarefa	Descrição	Habilidades necessárias
Configure o encaminhamento de registros.	Para encaminhar registros para o endpoint do Splunk: 1. Faça login no VMware Aria Operations for Logs. 2. Navegue até Gerenciamento de registros. 3. Escolha Encaminhamento de registros. 4. Escolha Nova configuração e conclua as seguintes configurações: • Forneça um nome para a configuração de encaminhamento de registros. • Em Destino, escolha No local. • Para o Cloud Proxy, selecione o proxy de	

Tarefa	Descrição	Habilidades necessárias
	nuvem que você instalou anteriormente. • Em Endpoint Type, escolha TCP. • Para o URL do Endpoint, forneça seu URL local do Splunk no formato: `tcp://x.x.x.x (your Splunk IP address): 514` • (Opcional) Para Tags, você pode especificar nomes e valores de tags para facilitar a consulta. • Escolha Aplicar a todos os registros ou Aplicar a registros específicos. Se você quiser enviar todos os registros do VMware Cloud on AWS para o Splunk, escolha Aplicar a todos os registros. 5. Escolha Verificar. 6. Escolha Salvar. Para obter mais informações, consulte Forward Logs from VMware Aria Operations for Logs na VMware documentação.	

Recursos relacionados

- VMware Nuvem no AWS site
- Sobre data centers definidos por software (documentação) VMware
- Implemente um VMware SDDC AWS usando o VMware Cloud on AWS (orientação AWS prescritiva)
- Migre cargas de trabalho para a VMware nuvem AWS usando o VMware HCX (AWS orientação prescritiva)
- Configurar uma extensão de data center para o VMware Cloud on AWS usando o modo vinculado híbrido (AWS orientação prescritiva)

Configure um pipeline de CI/CD para cargas de trabalho híbridas no Amazon ECS Anywhere usando o AWS CDK e GitLab

Criado pelo Dr. Rahul Sharad Gaikwad (AWS)

Resumo

Aviso: CodeCommit A AWS não está mais disponível para novos clientes. Os clientes atuais da AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais.

O Amazon ECS Anywhere é uma extensão do Amazon Elastic Container Service (Amazon ECS). Ele fornece suporte para registrar uma instância externa, como um servidor on-premises ou uma máquina virtual (VM), no cluster do Amazon ECS. Esse atributo ajuda a reduzir custos e mitigar operações e orquestrações de contêineres on-premises. Você pode usar o ECS Anywhere para implantar e executar aplicativos de contêiner em ambientes on-premises e na nuvem. Isso elimina a necessidade de sua equipe aprender vários domínios e conjuntos de habilidades ou gerenciar softwares complexos por conta própria.

Esse padrão descreve uma step-by-step abordagem para provisionar um cluster do Amazon ECS com instâncias do Amazon ECS Anywhere usando pilhas do Cloud Development Kit (AWS CDK) da Amazon Web Services (AWS). Em seguida, você usa CodePipeline a AWS para configurar um pipeline de integração e implantação contínuas (CI/CD). Em seguida, você replica seu repositório de GitLab código para a AWS CodeCommit e implanta seu aplicativo em contêineres no cluster Amazon ECS.

Esse padrão foi projetado para ajudar aqueles que usam a infraestrutura local para executar aplicativos de contêiner e gerenciar GitLab a base de código do aplicativo. Você pode gerenciar essas workloads usando os serviços de Nuvem AWS, sem perturbar sua infraestrutura on-premises existente.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo de contêiner executado na infraestrutura on-premises.
- Um GitLab repositório onde você gerencia a base de código do seu aplicativo. Para obter mais informações, consulte Repositório (GitLab).

- AWS Command Line Interface (AWS CLI), instalada e configurada. Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI (Documentação da AWS CLI).
- AWS CDK Toolkit, instalado e configurado globalmente. Para obter mais informações, consulte Instalar o AWS CDK na documentação do AWS CDK Workshop.
- npm, instalado e configurado para o AWS CDK em. TypeScript Para obter mais informações, consulte Como baixar e instalar o Node.js e o npm (documentação do npm).

Limitações

- Para limitações e considerações, consulte Instâncias externas (Amazon ECS Anywhere) na documentação do Amazon ECS.

Versões do produto

- AWS CDK Toolkit versão 2.27.0 ou superior
- npm versão 7.20.3 ou superior
- Node.js versão 16.6.1 ou superior

Arquitetura

Pilha de tecnologias de destino

- AWS CDK
- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon ECS Anywhere
- Amazon Elastic Container Registry (Amazon ECR)
- AWS Identity and Access Management (IAM)
- AWS Systems Manager
- GitLab repositório

Arquitetura de destino

Esse diagrama representa dois fluxos de trabalho principais descritos nesse padrão, provisionando o cluster do Amazon ECS e configurando o CI/CD pipeline that sets up and deploys the CI/CD pipeline, da seguinte forma:

1. Provisionar o cluster do Amazon ECS
    a. Quando você implanta a primeira pilha de CDK da AWS, ela cria uma CloudFormation pilha na AWS.
    b. Essa CloudFormation pilha provisiona um cluster do Amazon ECS e recursos relacionados da AWS.
    c. Para registrar uma instância externa com um cluster do Amazon ECS, você deve instalar o AWS Systems Manager Agent (SSM Agent) na sua VM e registrar a VM como uma instância gerenciada do AWS Systems Manager.
    d. Você deve instalar o agente de contêiner do Amazon ECS e o Docker na sua VM para registrá-la como instância externa com o cluster do Amazon ECS.
    e. Quando a instância externa é registrada e configurada com o cluster Amazon ECS, ela pode executar vários contêineres na sua VM, que é registrada como uma instância externa.
    f. O cluster do Amazon ECS está ativo e pode executar as cargas de trabalho do aplicativo por meio de contêineres. A instância de contêiner Amazon ECS Anywhere é executada em um ambiente on-premises, mas está associada ao cluster do Amazon ECS na nuvem.
2. Configurando e implantando o pipeline de CI/CD
    a. Quando você implanta a segunda pilha de CDK da AWS, ela cria outra CloudFormation pilha na AWS.
    b. Essa CloudFormation pilha provisiona um pipeline CodePipeline e recursos relacionados da AWS.
    c. Você envia e mescla as alterações do código do aplicativo em um repositório local GitLab .
    d. O GitLab repositório é automaticamente replicado para o CodeCommit repositório.
    e. As atualizações do CodeCommit repositório são CodePipeline iniciadas automaticamente.
    f. CodePipeline copia o código CodeCommit e cria o aplicativo implantável integrado. CodeBuild
    g. CodePipeline cria uma imagem Docker do ambiente de CodeBuild construção e a envia para o repositório Amazon ECR.
    h. CodePipeline inicia CodeDeploy ações que extraem a imagem do contêiner do repositório Amazon ECR.

i. CodePipeline implanta a imagem do contêiner no cluster Amazon ECS.

Automação e escala

Esse padrão usa o AWS CDK como uma ferramenta de infraestrutura como código (IaC) para configurar e implantar essa arquitetura. O AWS CDK ajuda você a orquestrar os recursos da AWS e configurar o Amazon ECS Anywhere e o pipeline de CI/CD.

Ferramentas

Serviços da AWS

- O AWS Cloud Development Kit (AWS CDK) é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar a infraestrutura da Nuvem AWS em código.
- CodeCommitA AWS é um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.
- CodePipelineA AWS ajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.
- O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster. Esse padrão também usa o Amazon ECS Anywhere, que fornece suporte para registrar um servidor on-premises ou uma VM no cluster do Amazon ECS.

Outras ferramentas

- O Node.js é um ambiente de tempo de JavaScript execução orientado a eventos projetado para criar aplicativos de rede escaláveis.
- O npm é um registro de software executado em um ambiente Node.js e usado para compartilhar ou emprestar pacotes e gerenciar a implantação de pacotes privados.

- O Vagrant é um utilitário de código aberto para criar e manter ambientes portáteis de desenvolvimento de software virtual. Para fins de demonstração, esse padrão usa o Vagrant para criar uma VM on-premises.

Repositório de código

O código desse padrão está disponível no pipeline de GitHub CI/CD do Amazon ECS Anywhere usando o repositório AWS CDK.

Práticas recomendadas

Considere as seguintes práticas recomendadas ao implantar esse padrão:

- Melhores práticas para desenvolver e implantar infraestrutura em nuvem com o AWS CDK
- Melhores práticas para desenvolver aplicativos em nuvem com o AWS CDK (publicação no blog da AWS)

Épicos

Verifique a configuração do AWS CDK

Tarefa	Descrição	Habilidades necessárias
Verifique a versão do AWS CDK.	Verifique a versão do AWS CDK Toolkit inserindo o comando a seguir. `cdk --version` Este padrão requer a versão 2.27.0 ou superior. Se você tiver uma versão anterior, siga as instruções na documentação do AWS CDK para atualizá-la.	DevOps engenheiro
Verificar a versão do npm.	Verifique a versão do npm inserindo o comando a seguir.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`npm --version` Este padrão requer a versão 7.20.3 ou superior. Se você tiver uma versão anterior, siga as instruções na documentação do npm para atualizá-la.	

Configurar credenciais da AWS.	Configure as credenciais da AWS inserindo o comando `aws configure` e seguindo as instruções.
	
	`$aws configure`
	`AWS Access Key ID`
	` [None]: <your-access-key-ID>`
	`AWS Secret Access Key`
	` [None]: <your-secret-access-key>`
	`Default region name`
	` [None]: <your-Region-name>`
	`Default output format`
	` [None]:`
		DevOps engenheiro

Faça o bootstrap do ambiente do AWS CDK

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de códigos do AWS CDK.	1. Clone o pipeline de CI/CD para o Amazon ECS Anywhere usando o repositório AWS CDK para esse padrão digitando o seguinte comando.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`git clone https://github.com/aws-samples/amazon-ecs-anywhere-cicd-pipeline-cdk-sample.git`
	2. Navegue até o diretório clonado inserindo o comando a seguir.
	`cd amazon-ecs-anywhere-cicd-pipeline-cdk-sample`	

Faça o bootstrap do ambiente.	Implante o CloudFormation modelo na conta e na região da AWS que você deseja usar inserindo o seguinte comando. `cdk bootstrap <account-number>/<Region>` Para obter mais informações, consulte Inicialização na documentação do AWS CDK.	DevOps engenheiro

Crie e implante a infraestrutura do Amazon ECS Anywhere

Tarefa	Descrição	Habilidades necessárias
Instale as dependências do pacote e compile os TypeScript arquivos.	Instale as dependências do pacote e compile os TypeScript arquivos digitando os seguintes comandos.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`$cd EcsAnywhereCdk`
	`$npm install`
	`$npm fund`
	
	Esses comandos instalam todos os pacotes do repositór io de exemplo. Para obter mais informações, consulte npm ci e npm install na documentação do npm. Se você receber algum erro sobre pacotes ausentes ao inserir esses comandos, consulte a seção Solução de problemas desse padrão.	

Crie o projeto.	Para compilar o código do projeto, digite o comando a seguir. `npm run build` Para obter mais informações sobre como criar e implantar o projeto, consulte Seu primeiro aplicativo da AWS CDK na documentação da AWS CDK.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Implante a pilha de infraestrutura do Amazon ECS Anywhere.	1. Liste as pilhas inserindo os comandos abaixo.
	`$cdk list`
	2. Confirme se a saída retorna as pilhas `EcsAnywhereInfraStack` e `ECSAnywherePipelineStack`.
	3. Implemente a pilha do `EcsAnywhereInfraStack` inserindo os comandos abaixo.
	`$cdk deploy EcsAnywhereInfraStack`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Verifique a criação e a saída da pilha.	1. Faça login no AWS Management Console e abra o CloudFormation console em https://console.aws.amazon.com/cloudformation/. 2. Na página Stacks, selecione a pilha `EcsAnywhereInfraStack` . 3. Confirme se o status da pilha é `CREATE_IN_PROGRESS` ou `CREATE_COMPLETE` . A configuração do cluster do Amazon ECS pode levar algum tempo. Não prossiga até que a criação da pilha esteja concluída.	DevOps engenheiro

Configurar uma VM on-premises

Tarefa	Descrição	Habilidades necessárias
Configurar a VM.	Crie uma VM Vagrant inserindo o comando `vagrant up` do diretório raiz onde o Vagrantfile está localizado. Para obter mais informações, consulte a documentação do Vagrant.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Registre sua VM como uma instância externa.	1. Faça login na VM Vagrant usando o comando `vagrant ssh`. Para obter mais informações, consulte a documentação do Vagrant. 2. Instale a AWS CLI na VM seguindo as instruções de instalação da AWS CLI e inserindo os seguintes comandos. `$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" \ > -o "awscliv2.zip" $sudo apt install unzip $unzip awscliv2.zip $sudo ./aws/install $aws configure AWS Access Key ID [None]: <your-access-key-ID> AWS Secret Access Key [None]: <your-secret-access-key> Default region name [None]: <your-Region-name> Default output format [None]:` 1. Crie um código de ativação e um ID que você possa usar para registrar sua VM	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	no AWS Systems Manager e ativar sua instância externa. A saída desse comando inclui os valores do ID de ativação e do código de ativação.
	
	`aws ssm create-activation \`
	`> --iam-role EcsAnywhereInstanceRole \`
	`> | tee ssm-activation.json`
	
	Se você receber um erro ao executar esse comando, consulte a seção Solução de problemas.
	2. Exporte o ID de ativação e os valores do código.
	
	`export ACTIVATION_ID=<activation-ID>`
	`export ACTIVATION_CODE=<activation-code>`
	3. Baixe o script de instalação na VM.
	
	`curl --proto "https" -o "ecs-anywhere-install.sh" \`
	`> "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywher`	

Tarefa	Descrição	Habilidades necessárias
	e-install-latest.s h" 4. Execute o script de instalação na sua VM. sudo bash ecs-anywh ere-install.sh \ --cluster EcsAnywhe reCluster \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <region-n ame> Isso configura sua VM como uma instância externa do Amazon ECS Anywhere e registra a instância no cluster do Amazon ECS. Para obter mais informações, consulte Registro de uma instância externa em um cluster na documentação do Amazon ECS. Se você tiver algum problema, consulte a seção Solução de problemas.	

Tarefa	Descrição	Habilidades necessárias

Verifique o status do Amazon ECS Anywhere e da VM externa.	Para verificar se sua VM está conectada ao ambiente de gerenciamento do Amazon ECS e em execução, use os seguintes comandos.
	`$aws ssm describe-instance-information`
	`$aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps engenheiro

Implante o pipeline de CI/CD

Tarefa	Descrição	Habilidades necessárias
Crie uma ramificação no CodeCommit repositório.	Crie uma ramificação nomeada `main` no CodeCommit repositório criando o primeiro commit para o repositório. Você pode seguir a documentação da AWS para criar um commit in CodeCommit. O comando a seguir é um exemplo. `aws codecommit put-file \ --repository-name EcsAnywhereRepo \ --branch-name main \ --file-path README.md \ --file-content "Test" \ --name "Dev Ops" \`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`--email "devops@example.com" \ --commit-message "Adding README."`	
Configure o espelhamento do repositório.	Você pode espelhar um GitLab repositório de e para fontes externas. Você pode selecionar qual repositório serve como fonte. Ramificações, tags e commits são sincronizados automaticamente. Configure um push mirror entre o GitLab repositório que hospeda seu aplicativo e o CodeCommit repositório. Para obter instruções, consulte Configurar um espelho de pressão de GitLab para CodeCommit (GitLab documentação). **Note** Por padrão, o espelhamento sincroniza automaticamente o repositório. Se você quiser atualizar manualmente os repositórios, consulte Atualizar um espelho (GitLab documentação).	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Implante a pilha de pipeline de CI/CD.	Implemente a pilha do `EcsAnywherePipelineStack` inserindo os comandos abaixo. `$cdk deploy EcsAnywherePipelineStack`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Testar o pipeline de CI/CD.	1. Faça alterações no código do aplicativo e envie-o para o repositório local de GitLab origem. Para obter mais informaçõ es, consulte Opções de push (GitLab documenta ção). Por exemplo, edite o arquivo `../applic ation/index.html` para atualizar o valor da versão do aplicativo. 2. Quando o código é replicado para o CodeCommit repositório, isso inicia o pipeline de CI/ CD. Execute um destes procedimentos: • Se você estiver usando o espelhamento automátic o para sincronizar o GitLab repositório com o CodeCommit repositório, vá para a próxima etapa. • Se você estiver usando o espelhamento manual, envie as alterações do código do aplicativo para o CodeCommit repositór io seguindo as instruções em Atualizar um espelho (GitLab documentação). 3. Em sua máquina local, em um navegador da Web,	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	digite http://localhost:80. Isso abre a página da web do NGINX porque a porta 80 é encaminhada para o localhost no Vagrantfile. Confirme se você pode visualizar o valor da versão atualizada do aplicativo. Isso valida a implantação do pipeline e da imagem. 4. (Opcional) Se você deseja verificar a implantação no Console de Gerenciamento da AWS, faça o seguinte: a. Abra o console do Amazon ECS em https://console.aws.amazon.com/ecs/. b. Na barra de navegação, selecione a Região a ser usada. c. No painel de navegação, escolha Clusters. d. Na página Clusters, selecione o EcsAnywhereClustercluster. e. Escolha Definições de tarefas. f. Confirme se o contêiner está funcionando.	

Limpeza

Tarefa	Descrição	Habilidades necessárias

Limpe e exclua os recursos.	Depois de percorrer esse padrão, você deve remover os proof-of-concept recursos que criou. Para limpar, insira os comandos a seguir.
	`$cdk destroy EcsAnywhe rePipelineStack`
	`$cdk destroy EcsAnywhe reInfraStack`
		DevOps engenheiro

Solução de problemas

Problema	Solução

Erros sobre pacotes ausentes ao instalar dependências de pacotes.	Insira um dos comandos a seguir para resolver pacotes ausentes.
	`$npm ci`
	or
	`$npm install -g @aws-cdk/<package_ name>`

Ao executar o comando `aws ssm create-ac tivation` na VM, você receberá o seguinte erro. `An error occurred (Validati onException) when calling the CreateActivation operation: Nonexistent role or missing ssm`	A pilha do `EcsAnywhereInfraStack` não está totalmente implantada e o perfil do IAM necessário para executar esse comando ainda não foi criado. Verifique o status da pilha no CloudFormation console. Use o comando novamente depois que o status muar para `CREATE_COMPLETE` .

Problema	Solução
`service principal in trust policy: arn:aws:iam::000000000000:role/EcsAnywhereInstanceRole`	

Uma verificação de integridade do Amazon ECS retorna `UNHEALTHY` e você vê o seguinte erro na seção Serviços do cluster no console do Amazon ECS.
 	
`service EcsAnywhereService was unable to place a task because no container instance met all of its requirements. Reason: No Container Instances were found in your cluster.`
	Reinicie o agente do Amazon ECS na VM do Vagrant inserindo os comandos a seguir.
	
	`$vagrant ssh`
	`$sudo systemctl restart ecs`
	`$sudo systemctl status ecs`

Recursos relacionados

- Página de marketing do Amazon ECS Anywhere
- Documentação do Amazon ECS Anywhere
- Demonstração do Amazon ECS Anywhere (vídeo)
- GitHubAmostras de workshops do Amazon ECS Anywhere ()
- Espelhamento do repositório (documentação) GitLab

Mais padrões

- Automatizar a configuração do emparelhamento entre regiões com o AWS Transit Gateway
- Gerencie aplicativos de contêineres on-premises configurando o Amazon ECS Anywhere com o AWS CDK
- Migre dados do Hadoop para o Amazon S3 usando o Migrator WANdisco LiveData
- Migre VMware VMs com o HCX Automation usando o PowerCLI
- Modifique os cabeçalhos HTTP ao migrar de F5 para um Application Load Balancer na AWS
- Redefinir a hospedagem de workloads on-premises na Nuvem AWS: lista de verificação de migração
- Use as consultas do BMC Discovery para extrair dados de migração para o planejamento da migração

Gerenciamento e governança

Tópicos

- Identifique e alerte quando os recursos do Amazon Data Firehose não estiverem criptografados com uma chave AWS KMS
- Automatizar a adição ou atualização de entradas de registro do Windows usando o AWS Systems Manager
- Crie automaticamente um RFC no AMS usando Python
- Pare e inicie automaticamente uma instância de banco de dados Amazon RDS usando o Windows AWS Systems Manager de manutenção
- Centralize a distribuição de pacotes de software no AWS Organizations usando o Terraform
- Configure o registro em log para aplicativos.NET no Amazon CloudWatch Logs usando NLog
- Copie os produtos do AWS Service Catalog em diferentes contas e regiões da AWS
- Crie uma matriz RACI ou RASCI para um modelo operacional em nuvem
- Crie alarmes para métricas personalizadas usando a detecção de CloudWatch anomalias da Amazon
- Crie um AWS Cloud9 IDE que usa volumes do Amazon EBS com criptografia padrão
- Crie CloudWatch painéis da Amazon baseados em tags automaticamente
- Documente seu projeto de landing zone na AWS
- Melhore o desempenho operacional habilitando o Amazon DevOps Guru em várias regiões e contas da AWS e OUs com o AWS CDK
- Implemente o Account Factory for Terraform (AFT) usando um pipeline de bootstrap
- Gerencie produtos do AWS Service Catalog em várias contas e regiões da AWS
- Migre uma conta membro da AWS do AWS Organizations para o AWS Control Tower
- Monitore clusters do SAP RHEL Pacemaker usando os serviços da AWS
- Monitore a atividade do aplicativo usando o CloudWatch Logs Insights
- Monitore o uso de uma Amazon Machine Image compartilhada em várias Contas da AWS
- Configure alertas para encerramentos programáticos de contas no AWS Organizations
- Ver os detalhes do snapshot do EBS para sua conta ou organização da AWS
- Mais padrões

Identifique e alerte quando os recursos do Amazon Data Firehose não estiverem criptografados com uma chave AWS KMS

Criado por Ram Kandaswamy (AWS)

Resumo

Para fins de conformidade, algumas organizações devem ter a criptografia ativada em recursos de entrega de dados, como o Amazon Data Firehose. Esse padrão mostra uma forma de monitorar, detectar e notificar quando os recursos estão fora de conformidade.

Para manter o requisito de criptografia, esse padrão pode ser usado AWS para fornecer monitoramento e detecção automatizados dos recursos de entrega do Amazon Data Firehose que não são criptografados com uma chave AWS Key Management Service (AWS KMS). A solução envia notificações de alerta e pode ser estendida para realizar a correção automática. Essa solução pode ser aplicada a uma conta individual ou a um ambiente de várias contas, como um ambiente que usa um AWS landing zone ou. AWS Control Tower

Pré-requisitos e limitações

Pré-requisitos

- Fluxo de entrega do Amazon Data Firehose
- Permissões e familiaridade suficientes com AWS CloudFormation o que é usado nessa automação de infraestrutura

Limitações

- A solução não é em tempo real porque usa AWS CloudTrail eventos para detecção e há um atraso entre o momento em que um recurso não criptografado é criado e a notificação é enviada.

Arquitetura

Pilha de tecnologias de destino

A solução usa tecnologia sem servidor e os seguintes serviços:

- AWS CloudTrail

- Amazon CloudWatch
- AWS Command Line Interface (AWS CLI)
- AWS Identity and Access Management (IAM)
- Amazon Data Firehose
- AWS Lambda
- Amazon Simple Notification Service (Amazon SNS)

Arquitetura de destino

O diagrama ilustra essas etapas:

1. Um usuário cria ou modifica o Amazon Data Firehose.
2. Um CloudTrail evento é detectado e correspondido.
3. Lambda é invocado.
4. Recursos não compatíveis são identificados.
5. Notificação por e-mail é enviada.

Automação e escala

Você pode usar AWS CloudFormation StackSets para aplicar essa solução a várias contas Regiões da AWS ou a várias contas com um único comando.

Ferramentas

- AWS CloudTrailé um AWS service (Serviço da AWS) que ajuda você a viabilizar a governança, a conformidade e a auditoria operacional e de risco do seu Conta da AWS. As ações realizadas por um usuário, função ou um AWS service (Serviço da AWS) são registradas como eventos em CloudTrail. Os eventos incluem ações realizadas nas operações AWS Management Console AWS CLI, AWS SDKs, e da API.
- A Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja Serviços da AWS usando comandos em seu shell de linha de comando.

- AWS Identity and Access Management (IAM) é um serviço web que ajuda você a controlar com segurança o acesso aos AWS recursos. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.
- O Amazon Data Firehose é um serviço totalmente gerenciado para fornecer dados de streaming em tempo real. Com o Firehose, você não precisa criar aplicativos ou gerenciar recursos. Configure os produtores de dados para enviar dados ao Firehose e ele entregará automaticamente os dados ao destino especificado.
- AWS Lambdaé um serviço de computação que oferece suporte à execução de código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo. Você paga somente pelo tempo de computação que consome. Não há cobrança quando seu código não está em execução.
- O Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens de editores para assinantes (também conhecidos como produtores e consumidores).

Épicos

Aplicar a criptografia para fins de conformidade

Tarefa	Descrição	Habilidades necessárias
Implantar AWS CloudFormation StackSets.	No AWS CLI, use o `firehose-encryption-checker.yaml` modelo (anexado) para criar o conjunto de pilhas executando o comando a seguir. Forneça um nome do recurso da Amazon (ARN) do tópico do Amazon SNS válido para o parâmetro. A implantação deve criar com sucesso regras de CloudWatch eventos, a função Lambda e uma função do IAM com as permissõe	Arquiteto de nuvem, administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	s necessárias, conforme descrito no modelo. `aws cloudformation create-stack-set --stack-set-name my-stack-set -- template-body file://firehose-encryption-checker.yaml`	
Crie instâncias da pilha.	As pilhas podem ser criadas na Regiões da AWS sua escolha, bem como em uma ou mais contas. Para criar instâncias de pilha, execute o comando a seguir. Substitua o nome da pilha, os números da conta e as regiões pelos seus. `aws cloudformation create-stack-instances --stack-set-name my-stack-set --accounts 123456789012 223456789012 -- regions us-east-1 us-east-2 us-west-1 us-west-2 --operation-preferences FailureToleranceCount=1`	Arquiteto de nuvem, administrador de sistemas

Recursos relacionados

- Trabalhando com AWS CloudFormation StackSets
- O que é Amazon CloudWatch Events?

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Automatizar a adição ou atualização de entradas de registro do Windows usando o AWS Systems Manager

Criado por Appasaheb Bagali (AWS)

Resumo

O AWS Systems Manager é uma ferramenta de gerenciamento remoto para instâncias do Amazon Elastic Compute Cloud (Amazon EC2). O Systems Manager fornece visibilidade e controle sobre sua infraestrutura no Amazon Web Services. Essa ferramenta versátil pode ser usada para corrigir alterações no registro do Windows que são identificadas como vulnerabilidades pelo relatório de verificação de vulnerabilidades de segurança.

Esse padrão abrange as etapas para manter seguras as EC2 instâncias que executam o sistema operacional Windows, automatizando as alterações no registro recomendadas para a segurança do seu ambiente. O padrão usa o comando de execução para executar um documento de comando. O código está anexado e uma parte dele está incluída na seção Código.

Pré-requisitos e limitações

- Uma conta AWS ativa
- Permissões para acessar a EC2 instância e o Systems Manager

Arquitetura

Pilha de tecnologias de destino

- Uma nuvem privada virtual (VPC) com duas sub-redes e um gateway de conversão de endereços de rede (NAT)
- Um documento de comando do Systems Manager para adicionar ou atualizar o nome de registro e o valor
- Systems Manager Run Command para executar o documento de comando nas EC2 instâncias especificadas

Arquitetura de destino

Ferramentas

Ferramentas

- Políticas do IAM e perfis: o AWS Identity and Access Management (IAM) é um serviço da web que ajuda você a controlar o acesso aos recursos da AWS com segurança. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.
- Amazon Simple Storage Service: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet. Ele foi projetado para facilitar a computação de escala na web para os desenvolvedores. Nesse padrão, um bucket do S3 é usado para armazenar os logs do Systems Manager.
- AWS Systems Manager: o AWS Systems Manager é um serviço da AWS que você pode usar para visualizar e controlar sua infraestrutura na AWS. O Systems Manager ajuda você a manter a segurança e a conformidade verificando suas instâncias gerenciadas e gerando relatórios (ou tomando medidas corretivas) sobre quaisquer violações de políticas detectadas.
- Documento de comando do AWS Systems Manager: os documentos de comando do AWS Systems Manager são usados pelo comando de execução. A maioria dos documentos Command é suportada em todos os sistemas operacionais Linux and Windows aos quais oferecem o Systems Manager.
- Comando de execução do AWS Systems Manager: o comando de execução do AWS Systems Manager oferece uma maneira de gerenciar a configuração de suas instâncias gerenciadas de forma remota e segura. O Executar comando permite que você automatize tarefas administrativas comuns e execute alterações de configuração ad-hoc em grande escala.

Código

Você pode usar o código de exemplo a seguir para adicionar ou atualizar um nome de registro do Microsoft Windows para `Version`, um caminho de registro para `HKCU:\Software\ScriptingGuys\Scripts` e um valor para 2.

```
#Windows registry path which needs to add/update
$registryPath ='HKCU:\\Software\\ScriptingGuys\\Scripts'
#Windows registry Name  which needs to add/update
$Name = 'Version'
#Windows registry value  which needs to add/update
$value = 2
```

```
# Test-Path cmdlet to see if the registry key exists.
IF(!(Test-Path $registryPath))
        {
           New-Item -Path $registryPath -Force | Out-Null
           New-ItemProperty -Path $registryPath -Name $name -Value     $value ` -
PropertyType DWORD -                 Force | Out-        Null
        } ELSE {
                      New-ItemProperty -Path $registryPath -Name $name -Value $value `
 -PropertyType            DWORD        -Force | Out-Null
            }
echo 'Registry Path:'$registryPath
 echo 'Registry Name:'$registryPath
 echo 'Registry Value:'(Get-ItemProperty -Path $registryPath -Name $Name).version
```

O exemplo completo do código JavaScript Object Notation (JSON) do documento de comando do Systems Manager Command está anexado.

Épicos

Configurar uma VPC

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC.	No Console de Gerenciamento da AWS, crie uma VPC com sub-redes públicas e privadas e um gateway NAT. Para obter mais informações, consulte a documentação da AWS.	Administrador de nuvem
Criar grupos de segurança.	Certifique-se de que cada grupo de segurança permite o acesso ao Remote Desktop Protocol (RDP) a partir do endereço IP de origem.	Administrador de nuvem

Criar uma política do IAM e um perfil do IAM

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM.	Crie uma política do IAM que forneça acesso ao Amazon S3 EC2, Amazon e Systems Manager.	Administrador de nuvem
Criar um perfil do IAM.	Crie uma função do IAM e anexe a política do IAM que fornece acesso ao Amazon S3 EC2, Amazon e Systems Manager.	Administrador de nuvem

Execute a automação

Tarefa	Descrição	Habilidades necessárias
Crie um documento de comando do Systems Manager.	Crie um documento de comando do Systems Manager que implantará as alterações do registro do Microsoft Windows para adicionar ou atualizar.	Administrador de nuvem
Execute o Executar Comando do Systems Manager.	Execute o comando de execução do Systems Manager, selecionando o documento de comando e as instâncias de destino do Systems Manager. Em seguida, a alteração do registro do Microsoft Windows no documento de comando	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	selecionado é enviada para as instâncias de destino.	

Recursos relacionados

- AWS Systems Manager
- Documentos do AWS Systems Manager
- Executar comando do AWS Systems Manager

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie automaticamente um RFC no AMS usando Python

Criado por Gnanasekaran Kailasam (AWS)

Resumo

O AWS Managed Services (AMS) ajuda você a operar sua infraestrutura baseada em nuvem com mais eficiência e segurança, fornecendo gerenciamento contínuo da sua infraestrutura da Amazon Web Services (AWS). Para fazer uma alteração em seu ambiente gerenciado, você precisa criar e enviar uma nova solicitação de alteração (RFC) que inclua uma ID do tipo de alteração (CT) para uma operação ou ação específica.

No entanto, a criação manual de um RFC pode levar cerca de cinco minutos e as equipes da sua organização talvez precisem enviar vários RFCs todos os dias. Esse padrão ajuda você a automatizar o processo de criação de RFC, reduzir o tempo de criação de cada RFC e eliminar erros manuais.

Esse padrão descreve como usar o código Python para criar automaticamente o `Stop EC2 instance` RFC que interrompe as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em sua conta AMS. Em seguida, você pode aplicar a abordagem desse padrão e a automação do Python a outros tipos de RFC.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta do AMS Advanced. Para obter mais informações sobre isso, consulte ps Planos de operações do AMS na documentação do AWS Managed Services.
- Pelo menos uma EC2 instância existente na sua conta do AMS.
- Uma compreensão de como criar e enviar RFCs no AMS.
- Familiaridade com o Python.

Limitações

- Você só pode usar RFCs para alterações em sua conta do AMS. Sua conta da AWS usa processos diferentes para mudanças semelhantes.

Arquitetura

Pilha de tecnologia

- AMS
- AWS Command Line Interface (AWS CLI)
- AWS SDK para Python (Boto3)
- Python e seus pacotes necessários (JSON e Boto3)

Automação e escala

Esse padrão fornece código de exemplo para automatizar a `Stop EC2 instance` RFC, mas você pode usar o código de amostra e a abordagem desse padrão para outros. RFCs

Ferramentas

- AWS Managed Services: o AMS ajuda você a operar sua infraestrutura da AWS com mais eficiência e segurança.
- AWS CLI: o AWS Command Line Interface (AWS CLI) é uma ferramenta unificada para gerenciar os serviços da AWS. No AMS, a API de gerenciamento de alterações fornece operações para criar e gerenciar RFCs.
- AWS SDK para Python (Boto3): o SDK para Python facilita a integração do seu aplicativo, biblioteca ou script do Python aos serviços da AWS.

Código

O arquivo `AMS Stop EC2 Instance.zip` (anexado) contém o código Python para criar uma `Stop EC2 instance` RFC. Você também pode configurar esse código para enviar uma única RFC para várias EC2 instâncias.

Épicos

Opção 1 – Configurar ambiente para macOS ou Linux

Tarefa	Descrição	Habilidades necessárias
Instale e valide o Python.	1. Abra uma janela de terminal e execute o comando `brew install python3`. 2. Valide se o Python está instalado corretamente executando o comando `python --version` . 3. Valide se o `pip` está instalado corretame nte executando o comando .`pip --version`	Administrador de sistemas AWS
Instale a AWS CLI.	Execute o comando `pip install awscli --upgrade –user` para instalar a AWS CLI.	Administrador de sistemas AWS
Instale o Boto3.	Execute o comando `pip install boto3` para instalar o Boto3.	Administrador de sistemas AWS
Instale o JSON.	Execute o comando `pip install json` para instalar o JSON.	Administrador de sistemas AWS
Configure o AMS CLI.	Faça login no Console de Gerenciamento da AWS, abra o console do AMS e escolha Documentação. Baixe o arquivo .zip que contém a CLI do AMS, descompacte-o	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	e instale-o em sua máquina local. Depois que instalar o AMS CLI, execute o comando `aws amscm help`. A saída fornece informações sobre o processo de gerenciamento de alterações do AMS.	

Opção 2 – Configurar ambiente para Windows

Tarefa	Descrição	Habilidades necessárias
Instale e valide o Python.	1. Abra a página de lançamentos do Python para Windows, baixe a versão mais recente e instale o Python. 2. Valide se o Python está instalado corretamente executando o comando `python --version` . 3. Valide se o `pip` está instalado corretamente executando o comando .`pip --version`	Administrador de sistemas AWS
Instale a AWS CLI.	Execute o comando `pip install awscli --upgrade –user` para instalar a AWS CLI.	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
Instale o Boto3.	Execute o comando `pip install boto3` para instalar o Boto3.	Administrador de sistemas AWS
Instale o JSON.	Execute o comando `pip install json` para instalar o JSON.	Administrador de sistemas AWS
Configure o AMS CLI.	Faça login no Console de Gerenciamento da AWS, abra o console do AMS e escolha Documentação. Baixe o arquivo .zip que contém a CLI do AMS, descompacte-o e instale-o em sua máquina local. Depois que instalar o AMS CLI, execute o comando `aws amscm help`. A saída fornece informações sobre o processo de gerenciamento de alterações do AMS.	Administrador de sistemas AWS

Extraia o ID do CT e os parâmetros de execução do RFC

Tarefa	Descrição	Habilidades necessárias
Extraia o ID do CT, versão e os parâmetros de execução do RFC.	Cada RFC tem uma ID de CT, versão e parâmetro s de execução diferente s. É possível extrair essas informações usando uma das seguintes opções:	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	1. Siga as instruções de Como encontrar uma alteração (RFC) com a seção CLI nos exemplos de uso de RFC na documentação do AWS Managed Services. 2. Abra uma RFC existente de um tipo similar ou crie uma nova RFC como teste por meio do console AMS. Use o ID de CT e os parâmetros de execução do RFC. Para obter mais informações sobre isso, consulte Como encontrar um RFC com o console na documentação do AWS Managed Services. **Note** Para adaptar a automação do Python desse padrão para outra RFCs, substitua o tipo de CT e os valores dos parâmetros no arquivo de código `ams_stop_ec2_instance` Python do `AMS Stop EC2 Instance.zip` arquivo (anexado)	

Tarefa	Descrição	Habilidades necessárias
	pelos que você extraiu.	

Execute a automação do Python

Tarefa	Descrição	Habilidades necessárias
Execute a automação do Python.	1. Baixe o arquivo `AMS Stop EC2 Instance.zip` (anexado) em sua máquina local e extraia o arquivo. 2. Atualize `input_instances` com as informações da sua EC2 instância. 3. Abra um terminal e navegue até o caminho do código extraído 4. Execute o comando `pythonams_stop_ec2_instance.py` .	Administrador de sistemas AWS

Recursos relacionados

- Quais são os tipos de mudança?
- Tutorial de CLI: pilha de duas camadas de alta disponibilidade (Linux/RHEL)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Pare e inicie automaticamente uma instância de banco de dados Amazon RDS usando o Windows AWS Systems Manager de manutenção

Criado por Ashita Dsilva (AWS)

Resumo

Esse padrão demonstra como parar e iniciar automaticamente uma instância de banco de dados Amazon Relational Database Service (Amazon RDS) em um cronograma específico (por exemplo, desligar uma instância de banco de dados fora do horário comercial para reduzir custos) usando o Windows de manutenção. AWS Systems Manager

AWS Systems Manager A automação fornece os runbooks `AWS-StopRdsInstance` e `AWS-StartRdsInstance` runbooks para interromper e iniciar instâncias de banco de dados do Amazon RDS. Isso significa que você não precisa escrever uma lógica personalizada com AWS Lambda funções ou criar uma regra do Amazon CloudWatch Events.

O Systems Manager fornece dois recursos para agendar tarefas: State Manager e Maintenance Windows. O State Manager define e mantém a configuração de estado necessária para recursos em sua conta da Amazon Web Services (AWS) uma vez ou em um cronograma específico. O Maintenance Windows executa tarefas nos recursos da sua conta durante uma janela de tempo específica. Embora você possa usar a abordagem desse padrão com o Gerenciador de Estado ou o Windows de Manutenção, recomendamos que você use o Windows de Manutenção porque ele pode executar uma ou mais tarefas com base na prioridade atribuída e também pode executar AWS Lambda funções e AWS Step Functions tarefas. Para obter mais informações sobre o State Manager e as janelas de manutenção, consulte Escolhendo entre o State Manager e as janelas de manutenção na documentação do Systems Manager.

Esse padrão fornece etapas detalhadas para configurar duas janelas de manutenção separadas que usam expressões cron para parar e, em seguida, iniciar uma instância de banco de dados Amazon RDS.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- Uma instância de banco de dados Amazon RDS existente que você deseja interromper e iniciar em um cronograma específico.

- Expressões Cron para o cronograma necessário. Por exemplo, a expressão `cron(0 9 ? * MON-FRI *)` executa a tarefa às 09:00 todas as segundas, terças, quartas, quintas e sextas-feiras. Para obter mais informações, consulte Cron e expressões de taxa para janelas de manutenção na documentação do Systems Manager.
- Familiarize-se com o Systems Manager.
- Permissões para iniciar e parar a instância do RDS. Para obter mais informações, consulte a seção Epics.

Limitações

- Uma instância de banco de dados Amazon RDS pode ser interrompida por até sete dias ao mesmo tempo. Depois de sete dias, a instância de banco de dados reinicia automaticamente para garantir que receba todas as atualizações de manutenção necessárias.
- Não é possível interromper uma instância de banco de dados que tem uma réplica de leitura ou que é uma réplica de leitura.
- Você não pode interromper uma instância de banco de dados do Amazon RDS para SQL Server em uma configuração multi-AZ.
- As Service quotas se aplicam ao Maintenance Windows e ao Systems Manager Automation. Para obter mais informações sobre cotas de serviço, consulte AWS Systems Manager endpoints e cotas na documentação. Referência geral da AWS
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Os diagramas a seguir mostram o fluxo de trabalho para parar e iniciar uma instância de banco de dados do Amazon RDS automaticamente.

O fluxo de trabalho consiste nas seguintes etapas:

1. Crie uma janela de manutenção e use expressões cron para definir o cronograma de parada e início para suas instâncias de banco de dados do Amazon RDS.

2. Registre uma tarefa do Systems Manager Automation na janela de manutenção usando o runbook `AWS-StopRdsInstance` ou `AWS-StartRdsInstance`.

3. Registre um destino na janela de manutenção usando um grupo de recursos baseado em tags para suas instâncias de banco de dados do Amazon RDS.

Pilha de tecnologia

- AWS CloudFormation
- AWS Identity and Access Management (IAM)
- Amazon RDS
- Systems Manager

Automação e escala

Você pode parar e iniciar várias instâncias de banco de dados Amazon RDS ao mesmo tempo marcando as instâncias de banco de dados do Amazon RDS necessárias, criando um grupo de recursos que inclua todas as instâncias de banco de dados marcadas e registrando esse grupo de recursos como destino para a janela de manutenção.

Ferramentas

- AWS CloudFormationé um serviço que ajuda você a modelar e configurar seus AWS recursos.
- AWS Identity and Access Management (IAM) é um serviço web que ajuda você a controlar com segurança o acesso aos AWS recursos.
- O Amazon Relational Database Service (Amazon RDS) é um serviço web que facilita a configuração, a operação e a escalabilidade de um banco de dados relacional no. Nuvem AWS
- AWS Resource Groupsajuda você a organizar AWS recursos em grupos, marcar recursos e gerenciar, monitorar e automatizar tarefas em recursos agrupados.
- AWS Systems Manageré um AWS service (Serviço da AWS) que você pode usar para visualizar e controlar sua infraestrutura AWS. Esse padrão usa os seguintes recursos do Systems Manager:
  - AWS Systems Manager A automação simplifica as tarefas comuns de manutenção e implantação de instâncias do Amazon Elastic Compute Cloud EC2 (Amazon) e outros AWS recursos.
  - AWS Systems Manager O Windows de manutenção ajuda você a definir um cronograma para quando realizar ações potencialmente disruptivas em suas instâncias.

Épicos

Crie e configure um perfil de serviço para o Systems Manager Automation

Tarefa	Descrição	Habilidades necessárias
Configure o perfil de serviço do IAM para o Systems Manager Automation.	Faça login no AWS Management Console e crie uma função de serviço para Systems Manager Automatio n. É possível usar um dos dois métodos a seguir para criar esse perfil de serviço: • Use AWS CloudFormation para configurar uma função de serviço para Systems Manager Automation • Use o IAM para configura r perfis para o Systems Manager Automation O fluxo de trabalho do Systems Manager Automatio n invoca o Amazon RDS usando um perfil de serviço para realizar ações de início e término na instância de banco de dados Amazon RDS. O perfil de serviço deve ser configurado com a seguinte política em linha, que tem permissões para iniciar e interromper a instância de banco de dados Amazon RDS:	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	    "Version":
	"2012-10-17",
	    "Statement": [
	        {
	            "Sid":
	"RdsStartStop",
	            "Effect":
	"Allow",
	            "Action": [
	
	"rds:StopDBInstance",
	
	"rds:StartDBInstance"
	            ],
	            "Resource":
	"<RDS_Instance_ARN>"
	
	        },
	        {
	            "Sid":
	"RdsDescribe",
	            "Effect":
	"Allow",
	            "Action":
	"rds:DescribeDBIns
	tances",
	            "Resource":
	"*"
	        }
	    ]
	}</pre>
	Certifique-se de substituir pelo `<RDS_Instance_ARN>` Amazon Resource Name (ARN) da sua instância de banco de dados Amazon RDS.	

Tarefa	Descrição	Habilidades necessárias
	Se você não estiver familiarizado com o uso de políticas e funções do IAM, siga as instruções na seção Visão geral da solução da postagem do AWS Systems Manager blog Schedule Amazon RDS para parar e começar a usar. **Important** Certifique-se de registrar o ARN da função de serviço.	

Ciar um grupo de recursos

Tarefa	Descrição	Habilidades necessárias
Marque as instâncias de banco de dados do Amazon RDS	Abra o console do Amazon RDS e marque as instâncias de banco de dados do Amazon RDS que você deseja adicionar ao grupo de recursos. Uma tag é um metadado atribuído a um AWS recurso e consiste em um par de valores-chave. Recomendamos que você use Action como chave de tag e StartStopcomo valor. Para obter mais informações sobre isso, consulte Adicionar	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	, listar e remover tags na documentação do Amazon RDS.	
Crie um grupo de recursos para suas instâncias de banco de dados do Amazon RDS marcadas.	Abra o AWS Resource Groups console e crie um grupo de recursos com base na tag que você criou para suas instâncias de banco de dados Amazon RDS. Em Critérios de agrupamento, certifique-se de escolher AWS: :RDS:: DBInstance para o tipo de recurso e, em seguida, forneça o par de valores-chave da tag (por exemplo, “Ação- “). StartStop Isso garante que o serviço verifique apenas as instâncias de banco de dados do Amazon RDS e não outros recursos que tenham essa tag. Certifique-se de registrar o nome do grupo de recursos. Para obter mais informações e etapas detalhadas, consulte Criar uma consulta baseada em tags e criar um grupo na AWS Resource Groups documentação.	Administrador da AWS

Configure uma janela de manutenção para interromper as instâncias de banco de dados do Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Criar uma janela de manutenção.	1. Abra o console do Systems Manager, escolha Janelas de manutenção e, em seguida, escolha Criar uma janela de manutenção. Forneça um nome para sua janela de manutenção (por exemplo, "StopRdsInstance“), insira uma descrição e, em seguida, desmarque Permitir destinos não registrados. 2. Escolha expressão rate/de CRON e forneça uma expressão de programação para definir quando as instâncias de banco de dados do Amazon RDS devem ser interrompidas. Insira 1 para Duração e 0 para Parar de iniciar tarefas. Por padrão, o fuso horário mostra UTC. Você pode alterar o fuso horário para iniciar a janela de manutenção com base no timestamp definido na sua expressão cron. 3. Escolha Create maintenance window (Criar janela de manutenção). O sistema	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	retorna você para a página da janela de manutenção e o estado da janela de manutenção é Ativado. **Important** A tarefa de interromper a instância de banco de dados é executada quase instantaneamente quando iniciada e não abrange toda a duração da janela de manutenção. Esse padrão fornece os valores mínimos para a Duração e Parar inicialização de tarefas, pois são os parâmetros necessários para uma janela de manutenção. Para obter mais informações e etapas detalhadas, consulte Criar uma janela de manutenção (console) na documentação do Systems Manager.	

Tarefa	Descrição	Habilidades necessárias
Atribuir um destino a uma janela de manutenção.	1. No console do Systems Manager, escolha Maintenance Windows, escolha Actions e, em seguida, escolha Register targets. 2. Na área Destinos , especifiq ue Escolher um grupo de recurso e então escolha o nome de um grupo de recursos existente em sua conta. 3. Para Tipos de recursos, escolha AWS: :RDS:: DBInstance e, em seguida, escolha Registrar destino. Para obter mais informações e etapas detalhadas, consulte Atribuir destinos a uma janela de manutenção (console) na documentação do Systems Manager.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Atribuir uma tarefa a uma janela de manutenção.	1. No console do Systems Manager, escolha Maintenance Windows e, em seguida, escolha sua janela de manutenção. Escolha Ações e, em seguida, escolha Registrar tarefa de Automação. 2. Em Documento, escolha AWS- StopRdsInstance. 3. Na seção Metas, escolha Selecionar grupos-alvo registrados e, em seguida, escolha o alvo da janela de manutenção que você registrou na janela de manutenção atual. 4. Para Controle de taxa, especifique 100 por cento para Concurrency e Limite de erro. Você pode alterar os valores do Controle de taxa de acordo com as suas exigências para a concurrency da tarefa e limite de erro. Para obter mais informações sobre isso, consulte Sobre limites de simultaneidade e erro na documentação do Systems Manager. 5. Na seção Função de serviço do IAM, em Função de serviço, deixe essa caixa	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	em branco ou crie sua própria função personalizada. Se você deixar a caixa em branco, o Systems Manager criará automaticamente a função AWSServiceRoleForAmazonSSM vinculada ao serviço e, em seguida, associará a função à tarefa. Para criar sua própria função personalizada, consulte Criar uma função de serviço personalizada para janelas de manutenção (console) e associe essa função personalizada à tarefa. 6. Na seção Input parameters, especifique os parâmetros a seguir: para o runbook: • InstanceId: `{{RESOURCE_ID}}` **Note** Para InstanceId, um pseudoparâmetro é usado para extrair o ID do recurso de banco de dados Amazon RDS do ARN. Para saber mais	

Tarefa	Descrição	Habilidades necessárias
	sobre pseudopar âmetros, consulte Sobre pseudopar âmetros na documentação do Systems Manager. • AutomationAssumeRole: forneça o ARN da função de serviço que você criou para o Systems Manager Automation. 7. Escolha Register Automatio n task (Registrar tarefa de Automação). **Important** A opção Função de serviço define a função de serviço necessária para que a janela de manutençã o execute tarefas. No entanto, essa função não é idêntica ao perfil de serviço que você criou anteriorm ente para o Systems Manager Automation.	

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações e etapas detalhadas, consulte Atribuir tarefas a uma janela de manutenção (console) na documentação do Systems Manager.	

Configure uma janela de manutenção para iniciar as instâncias de banco de dados do Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Configure uma janela de manutenção para iniciar as instâncias de banco de dados do Amazon RDS.	Repita as etapas de Configurar uma manutenção para interromper o épico de instâncias do banco de dados do Amazon RDS para configurar outra janela de manutenção para iniciar as instâncias de banco de dados do Amazon RDS em um horário programado. **Important** Você deve fazer as seguintes alterações ao configurar a janela de manutenção para iniciar as instâncias de banco de dados: • Use um novo nome para a janela de manutenção (por	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	exemplo, "StartRdsInstance“). • Substitua a expressão cron pela expressão cron que você deseja usar para iniciar as instâncias de banco de dados. • Substitua o runbook `AWS-StopRdsInstance` por `AWS-StartRdsInstance` em Tarefa.	

Recursos relacionados

- Use documentos do Systems Manager Automation para gerenciar instâncias e cortar custos fora do horário de expediente (postagem AWS no blog)

Centralize a distribuição de pacotes de software no AWS Organizations usando o Terraform

Criado por Pradip kumar Pandey (AWS), Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Mayuri Shinde (AWS) e Pratap Kumar Nanda (AWS)

Resumo

As empresas geralmente mantêm várias Contas da AWS que estão espalhadas por várias Regiões da AWS para criar uma forte barreira de isolamento entre as cargas de trabalho. Para se manterem seguras e em conformidade, suas equipes de administração instalam ferramentas baseadas em agentes CrowdStrike, como SentinelOne, ou TrendMicroferramentas para verificação de segurança, e o _CloudWatch agente Amazon, o Datadog Agent ou agentes para monitoramento. AppDynamics Essas equipes geralmente enfrentam desafios quando querem automatizar centralmente o gerenciamento e a distribuição de pacotes de software em todo esse grande cenário.

O Distributor, um recurso da AWS Systems Manager, automatiza o processo de empacotamento e publicação de software em instâncias gerenciadas do Microsoft Windows e Linux na nuvem e em servidores locais por meio de uma única interface simplificada. Esse padrão demonstra como você pode usar o Terraform para simplificar ainda mais o processo de gerenciamento da instalação do software e executar scripts em um grande número de instâncias e contas de membros AWS Organizations com o mínimo esforço.

Essa solução funciona para instâncias Amazon, Linux e Windows que são gerenciadas pelo Systems Manager.

Pré-requisitos e limitações

- Um pacote do Distribuidor que tem o software a ser instalado
- Terraform versão 0.15.0 ou posterior
- Instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que são gerenciadas pelo Systems Manager e têm permissões básicas para acessar o Amazon Simple Storage Service (Amazon S3) na conta de destino
- Uma landing zone para sua organização que é configurada usando AWS Control Tower
- (Opcional) Account Factory for Terraform (AFT)

Arquitetura

Detalhes do recurso

Esse padrão usa o Account Factory for Terraform (AFT) para criar todos os AWS recursos necessários e o pipeline de código para implantar os recursos em uma conta de implantação. O pipeline de código é executado em dois repositórios:

- A personalização global contém o código do Terraform que será executado em todas as contas registradas na AFT.
- As personalizações da conta contêm o código do Terraform que será executado na conta de implantação.

Você também pode implantar essa solução sem usar o AFT, executando os comandos do Terraform na pasta de personalizações da conta.

O código do Terraform implanta os seguintes recursos:

- AWS Identity and Access Management Papel e políticas (IAM)
  - SystemsManager- AutomationExecutionRole concede ao usuário permissões para executar automações nas contas de destino.
  - SystemsManager- AutomationAdministrationRole concede ao usuário permissões para executar automações em várias contas e unidades organizacionais (OUs).
- Arquivos compactados e manifest.json para o pacote
  - No Systems Manager, um pacote inclui pelo menos um arquivo.zip de software ou ativos instaláveis.
  - O manifesto JSON inclui ponteiros para os arquivos de código do pacote.
- Bucket do S3
  - O pacote distribuído que é compartilhado em toda a organização é armazenado com segurança em um bucket do Amazon S3.
- AWS Systems Manager documentos (documentos SSM)
  - `DistributeSoftwarePackage`contém a lógica para distribuir o pacote de software para cada instância de destino nas contas dos membros.
  - `AddSoftwarePackageToDistributor`contém a lógica para empacotar os ativos de software instaláveis e adicioná-los à automação, um recurso de AWS Systems Manager.
- Systems Manager (Gerenciador de sistemas)Associação

- Uma associação do Systems Manager é usada para implantar a solução.

Arquitetura e fluxo de trabalho

O diagrama ilustra as seguintes etapas:

1. Para executar a solução a partir de uma conta centralizada, você carrega seus pacotes ou software junto com as etapas de implantação em um bucket do S3.
2. Seu pacote personalizado fica disponível na seção Documentos do console do Systems Manager, na guia Owned by me.
3. O State Manager, um recurso do Systems Manager, cria, agenda e executa uma associação para o pacote em toda a organização. A associação especifica que o pacote de software deve ser instalado e executado em um nó gerenciado antes de poder ser instalado no nó de destino.
4. A associação instrui o Systems Manager a instalar o pacote no nó de destino.
5. Para quaisquer instalações ou alterações subsequentes, os usuários podem executar a mesma associação periodicamente ou manualmente em um único local para realizar implantações em várias contas.
6. Nas contas dos membros, a automação envia comandos de implantação para o Distribuidor.
7. O distribuidor distribui pacotes de software entre instâncias.

Essa solução usa a conta de gerenciamento interna AWS Organizations, mas você também pode designar uma conta (administrador delegado) para gerenciá-la em nome da organização.

Ferramentas

Serviços da AWS

- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados. Esse padrão usa o Amazon S3 para centralizar e armazenar com segurança o pacote distribuído.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala. Esse padrão usa os seguintes recursos do Systems Manager:

  - O Distributor ajuda você a empacotar e publicar software nas instâncias gerenciadas do Systems Manager.
  - A automação simplifica as tarefas comuns de manutenção, implantação e remediação de muitos AWS serviços.
  - O Documents executa ações em suas instâncias gerenciadas do Systems Manager em toda a sua organização e contas.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias AWS contas em uma organização que você cria e gerencia centralmente.

Outras ferramentas

- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Repositório de código

As instruções e o código desse padrão estão disponíveis no repositório GitHub centralizado de distribuição de pacotes.

Práticas recomendadas

- Para atribuir tags a uma associação, use o AWS Command Line Interface (AWS CLI) ou Ferramentas da AWS para PowerShello. Não há suporte à adição de tags a uma associação usando o console do Systems Manager. Para obter mais informações, consulte Como marcar recursos do Systems Manager na documentação do Systems Manager.
- Para executar uma associação usando uma nova versão de um documento compartilhado de outra conta, defina a versão do documento como`default`.
- Para marcar somente o nó de destino, use uma chave de tag. Se você quiser direcionar seus nós usando várias chaves de tag, use a opção de grupo de recursos.

Épicos

Configurar arquivos e contas de origem

Tarefa	Descrição	Habilidades necessárias

Clonar o repositório.	1. Clone o repositório GitHub centralizado de distribuição de pacotes:
	`git clone https://github.com/aws-samples/aws-organization-centralised-package-distribution`
	2. O repositório de código do Terraform requer duas pastas de personalização gerenciadas pela AFT. Confirme se sua cópia local do repositório contém as seguintes pastas:
	`$ cd centralised-package-distribution`
	`$ ls`
	`global-customization account-customization`
		DevOps engenheiro

Atualize as variáveis globais.	Atualize os seguintes parâmetros de entrada no `global-customization/variables.tf` arquivo. Essas variáveis se aplicam a todas as contas criadas e gerenciadas pela AFT.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• `account_id` : o ID da conta em que a solução do distribuidor será implantada. • `aws_region` : O Região da AWS local onde a associação será implantada.	
Atualize as variáveis da conta.	Atualize os seguintes parâmetros de entrada no `account-customization/variables.tf` arquivo. Essas variáveis se aplicam somente a contas específicas criadas e gerenciadas pela AFT. • `package_bucket_name` : o nome do bucket do S3 que contém o arquivo de distribuição do pacote. • `package_name` : o nome do arquivo de distribuição do pacote. • `package_version` : A versão do pacote do instalador.	DevOps engenheiro

Personalize parâmetros e arquivos de implantação

Tarefa	Descrição	Habilidades necessárias
Atualize os parâmetros de entrada para a associação State Manager.	Atualize os seguintes parâmetros de entrada no `account-customizat`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`ion/association.tf` arquivo para definir o estado que você deseja manter em suas instâncias. Você pode usar os valores de parâmetro s padrão se eles oferecerem suporte ao seu caso de uso.
	• `targetAccounts` : a unidade organizacional (OU) IDs dentro do AWS Organizations que represent a contas com as instâncias de destino para distribuição. OU IDs começa com “você”.
	• `targetRegions` : o Regiões da AWS (por exemplo, “us-east-1″ ou” ap-southeast-2”) em que as instâncias de destino estão sendo executadas.
	• `action`: especifique se deseja instalar ou desinstal ar o pacote.
	• `installationType` : Um dos seguintes tipos de instalação:
	  • `uninstall` : O pacote está desinstalado.
	  • `reinstall` : o aplicativ o é colocado off-line até que o processo de reinstalação seja concluído.	

Tarefa	Descrição	Habilidades necessárias
	• `In-place update`: o aplicativo está disponível enquanto arquivos novos ou atualizados são adicionados à instalação. • `name`: o nome do pacote a ser instalado ou desinstalado. • `version`: a versão do pacote a ser instalada ou desinstalada. Se nenhuma versão do pacote estiver instalada, o sistema retornará um erro. • `bucketName` : o nome do bucket do S3 no qual o pacote foi implantado. Esse bucket deve consistir somente nos pacotes e no arquivo de manifesto. • `bucketPrefix` : o prefixo S3 em que os ativos do pacote são armazenados. • `AutomationAssumeRole` : O nome de recurso da Amazon (ARN) de. `SystemsManager-AutomationAdministrationRole`	

Tarefa	Descrição	Habilidades necessárias
Prepare os arquivos compactados e o `manifest.json` arquivo para o pacote.	Esse padrão fornece exemplos de arquivos PowerShell instaláveis (.msi para Windows e .rpm para Linux) com scripts de instalação e desinstalação na pasta `account-customization/package` 1. Substitua os arquivos PowerShell instaláveis pelos seus próprios arquivos ou forneça seu arquivo instalável, scripts de instalação e desinstalação e arquivo de manifesto para criar um pacote na `account-customization` pasta da sua conta. 2. Personalize o `manifest.json` arquivo padrão que o Terraform gera na `account-customization` pasta de acordo com seus requisitos.	DevOps engenheiro

Execute comandos do Terraform para provisionar recursos

Tarefa	Descrição	Habilidades necessárias
Inicialize a configuração do Terraform.	Para implantar a solução automaticamente com o AFT,	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	envie o código para AWS CodeCommit:
	
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
	
	Você também pode implantar essa solução sem usar o AFT executando um comando do Terraform na `account-customization` pasta. Para inicializar o diretório de trabalho que contém os arquivos do Terraform, execute:
	
	`$ terraform init`	

Tarefa	Descrição	Habilidades necessárias
Pré-visualize as alterações.	Para visualizar as alterações que o Terraform fará na infraestrutura, execute o comando: `$ terraform plan` Esse comando avalia a configuração do Terraform para determinar o estado desejado dos recursos que foram declarados. Ele também compara o estado desejado com a infraestrutura real a ser provisionada no espaço de trabalho.	DevOps engenheiro
Aplique as alterações.	Execute o comando a seguir para implementar as alterações feitas nos `variables.tf` arquivos: `$ terraform apply`	DevOps engenheiro

Validar recursos

Tarefa	Descrição	Habilidades necessárias
Valide a criação de documentos SSM.	1. No console do Systems Manager, no painel de navegação esquerdo, escolha Documents. 2. Escolha a guia De minha propriedade.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Você deve ver `DistributeSoftwarePackage` os `AddSoftwarePackageToDistributor` pacotes e.	
Valide a implantação bem-sucedida das automações.	1. No console do Systems Manager, no painel de navegação esquerdo, escolha Automação. 2. Na lista de execuções de automação, você deve ver as mais recentes `DistributeSoftwarePackage` e as `AddSoftwarePackageToDistributor` implantações. 3. Escolha ID de execução para validar se eles foram concluídos com êxito.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Valide se o pacote foi implantado nas instâncias da conta do membro de destino.	1. No console do Systems Manager, no painel de navegação, escolha Executar comando. 2. No histórico de comandos, você verá cada invocação e seu status. 3. Escolha qualquer ID de comando para ver o histórico de implantação de cada instância de destino. 4. Escolha o ID da instância e verifique a seção Saída da distribuição.	DevOps engenheiro

Solução de problemas

Problema	Solução
A associação do State Manager falhou ou está presa no status pendente.	Consulte as informações de solução de problemas no Centro de AWS Conhecimento.
Falha na execução de uma associação agendada.	Sua especificação de agendamento pode ser inválida. Atualmente, o State Manager não suporta a especificação de meses em expressões cron para associações. Use expressões cron ou rate para confirmar a programação.

Recursos relacionados

- Distribuição centralizada de pacotes (GitHub repositório)
- Account Factory for Terraform (AFT)

- Casos de uso e melhores práticas (AWS Systems Manager documentação)

Configure o registro em log para aplicativos.NET no Amazon CloudWatch Logs usando NLog

Criado por Bibhuti Sahu (AWS) e Rob Hill (AWS)

Resumo

Esse padrão descreve como usar a estrutura de registro de NLog código aberto para registrar o uso e os eventos do aplicativo.NET no Amazon CloudWatch Logs. No CloudWatch console, você pode ver as mensagens de log do aplicativo quase em tempo real. Você também pode configurar métricas e configurar alarmes para notificá-lo se um limite métrico for excedido. Usando o CloudWatch Application Insights, você pode visualizar painéis automatizados ou personalizados que mostram possíveis problemas para os aplicativos monitorados. CloudWatch O Application Insights foi projetado para ajudá-lo a isolar rapidamente os problemas contínuos com seus aplicativos e infraestrutura.

Para gravar mensagens de log em CloudWatch Logs, você adiciona o `AWS.Logger.NLog` NuGet pacote ao projeto.NET. Em seguida, você atualiza o `NLog.config` arquivo para usar o CloudWatch Logs como destino.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um aplicativo web ou de console do.NET que:
  - Usa as versões compatíveis da .NET Framework ou do .NET Core. Para obter mais informações, consulte Versões de produto.
  - Usa NLog para enviar dados de log para o Application Insights.
- Permissões para criar um perfil do IAM para um serviço da AWS. Para obter mais informações, consulte Permissões de perfil de serviço.
- Permissões para transmitir um perfil para um serviço da AWS. Para obter mais informações, consulte Conceder a um usuário permissões para transmitir uma função a um produto da AWS.

Versões do produto

- .NET Framework versão 3.5 ou superior.

- .NET Core versões 1.0.1, 2.0.0 ou superior

Arquitetura

Pilha de tecnologias de destino

- NLog
- CloudWatch Registros da Amazon

Arquitetura de destino

1. O aplicativo.NET grava dados de NLog log na estrutura de registro.
2. NLog grava os dados de registro em CloudWatch Logs.
3. Você usa CloudWatch alarmes e painéis personalizados para monitorar o aplicativo.NET.

Ferramentas

Serviços da AWS

- O Amazon CloudWatch Application Insights ajuda você a observar a saúde de seus aplicativos e dos recursos subjacentes da AWS.
- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas, aplicativos e serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- As ferramentas da AWS para PowerShell são um conjunto de PowerShell módulos que ajudam você a criar scripts de operações em seus recursos da AWS a partir da linha de PowerShell comando.

Outras ferramentas

- Lenhador. NLogé um NLog destino que registra dados de registro no CloudWatch Logs.
- NLogé uma estrutura de registro de código aberto para plataformas do.NET que ajuda você a gravar dados de log em destinos, como bancos de dados, arquivos de log ou consoles.

- PowerShellé um programa de gerenciamento de automação e configuração da Microsoft executado em Windows, Linux e macOS.
- O Visual Studio é um ambiente de desenvolvimento integrado (IDE) que inclui compiladores, ferramentas de preenchimento de código, designers gráficos e outros atributos compatíveis com o desenvolvimento de software.

Práticas recomendadas

- Defina uma política de retenção para o grupo de logs de destino. Isso deve ser feito fora da NLog configuração. Por padrão, os dados de registro são armazenados em CloudWatch Registros indefinidamente.
- Siga as Práticas recomendadas de gerenciamento de chaves de acesso da AWS.

Épicos

Configurar o acesso e ferramentas

Tarefa	Descrição	Habilidades necessárias
Crie uma política do IAM.	Siga as instruções em Como criar políticas usando o editor JSON na documentação do IAM. Insira a política JSON a seguir, que tem as permissões de privilégios mínimos necessárias para permitir que os registros leiam e gravem CloudWatch registros. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [`	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	<pre>"logs:CreateLogGroup",
	"logs:CreateLogStream",
	"logs:GetLogEvents",
	"logs:PutLogEvents",
	"logs:DescribeLogGroups",
	"logs:DescribeLogStreams",
	"logs:PutRetentionPolicy"
	],
	"Resource":
	[
	"*"
	]
	}
	]
	}</pre>	

Criar um perfil do IAM.	Para obter instruções, consulte Criar um perfil para delegar permissões a um serviço da AWS na documentação do IAM. Selecione a política que você criou anteriormente. Essa é a função que CloudWatch Logs assume para realizar ações de registro.	Administrador da AWS, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Configure o AWS Tools para PowerShell.	1. Siga as instruções do seu sistema operacional em Instalando as ferramentas da AWS para PowerShell. 2. Use as ferramentas da AWS para PowerShell cmdlets para armazenar sua chave de acesso e chave secreta em um perfil. Para obter instruções, consulte Gerenciamento de perfis nas ferrament as da AWS para obter a PowerShell documentação.	AWS geral

Configure NLog

Tarefa	Descrição	Habilidades necessárias
Instale o NuGet pacote.	1. No Visual Studio, escolha Arquivo e, em seguida, escolha Abrir um projeto ou solução. 2. Escolha o projeto em que você deseja instalar NLog. 3. No Visual Studio, escolha Tools, NuGet Package Manager, Package Manager Console. 4. Instale o `AWS.Logge r.NLog` NuGet pacote digitando o comando a seguir.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
	`Install-Package AWS.Logger.NLog -Version 3.1.0`	

Tarefa	Descrição	Habilidades necessárias
Configurar o destino de registro em log.	1. Abra o arquivo `NLog.config` . 2. Para o alvo `type`, digite `AWSTarget` . 3. Para o destino `logGroup`, insira o nome do grupo de logs que você deseja usar. Se o grupo de logs ainda não existir, um novo grupo de logs com o nome fornecido será criado automaticamente. 4. Para o destino`region`, insira a região da AWS em que o CloudWatch Logs está configurado. 5. Para o destino `profile`, insira o nome do perfil que você criou anteriormente para armazenar a chave de acesso e a chave secreta. 6. Salve e feche o arquivo `NLog.config` . Para obter um exemplo de arquivo de configuração, consulte a seção Informações adicionais deste padrão. Quando você executar seu aplicativo, NLog gravará as mensagens de log e as enviará para o CloudWatch Logs.	Desenvolvedor de aplicativos

Validar e monitorar logs

Tarefa	Descrição	Habilidades necessárias
Validar o registro em log.	Siga as instruções em Exibir dados de registro enviados para CloudWatch Registros na documentação de CloudWatch Registros. Valide se os eventos de logs estão sendo registrados para o aplicativo.NET. Se os eventos de log não estiverem sendo registrados, consulte a seção Solução de problemas nesse padrão.	AWS geral
Monitore a pilha de aplicativos .NET.	Configure o monitoramento CloudWatch conforme necessário para seu caso de uso. Você pode usar o CloudWatch Logs Insights, o CloudWatch Metrics Insights e o CloudWatch Application Insights para monitorar sua carga de trabalho.NET. Você também pode configurar alarmes para receber alertas e criar um painel personalizado para monitorar a workload a partir de uma única visualização.	AWS geral

Solução de problemas

Problema	Solução
Os dados do registro não aparecem nos CloudWatch registros.	Certifique-se de que a política do IAM esteja vinculada à função do IAM que o CloudWatch Logs assume. Para obter instruções, consulte a seção Configurar acesso e ferramentas na seção Épicos.

Recursos relacionados

- Trabalhando com grupos de registros e fluxos de CloudWatch registros (documentação de registros)
- Amazon CloudWatch Logs e .NET Logging Frameworks (publicação no blog da AWS)

Mais informações

Veja a seguir um exemplo de arquivo `NLog.config`.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <section name="nlog" type="NLog.Config.ConfigSectionHandler, NLog" />
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
  </startup>
  <nlog>
    <extensions>
      <add assembly="NLog.AWS.Logger" />
    </extensions>
    <targets>
      <target name="aws" type="AWSTarget" logGroup="NLog.TestGroup" region="us-east-1"
 profile="demo"/>
    </targets>
    <rules>
      <logger name="*" minlevel="Info" writeTo="aws" />
    </rules>
```

```
  </nlog>
</configuration>
```

Copie os produtos do AWS Service Catalog em diferentes contas e regiões da AWS

Criado por Sachin Vighe (AWS) e Santosh Kale (AWS)

Resumo

O AWS Service Catalog é um serviço regional e isso significa que os portfólios e produtos do AWS Service Catalog só são visíveis na região da AWS em que foram criados. Se você configurar um hub do AWS Service Catalog em uma nova região, deverá recriar seus produtos existentes e isso pode ser um processo demorado.

A abordagem desse padrão ajuda a simplificar esse processo, descrevendo como copiar produtos de um hub do AWS Service Catalog em uma conta ou região da AWS de origem para um novo hub em uma conta ou região de destino. Para obter mais informações sobre o modelo hub e spoke do AWS Service Catalog, consulte o modelo hub and spoke do AWS Service Catalog: Como automatizar a implantação e o gerenciamento do AWS Service Catalog em várias contas no blog de gerenciamento e governança da AWS.

O padrão também fornece os pacotes de códigos separados necessários para copiar os produtos do AWS Service Catalog entre contas ou para outras regiões. Ao usar esse padrão, sua organização pode economizar tempo, disponibilizar versões de produtos existentes e anteriores em um novo hub do AWS Service Catalog, minimizar o risco de erros manuais e escalar a abordagem em várias contas ou regiões.

> **Note**
>
> A seção Epics desse padrão oferece duas opções para copiar produtos. Você pode usar a Opção 1 para copiar produtos entre contas ou escolher a Opção 2 para copiar produtos entre regiões.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Produtos existentes do AWS Service Catalog em uma conta ou região de origem.
- Um hub existente do AWS Service Catalog em uma conta ou região de destino.

- Se quiser copiar produtos entre contas, você deve compartilhar e depois importar o portfólio do AWS Service Catalog contendo os produtos em sua conta de destino. Para obter mais informações sobre isso, consulte Compartilhamento e importação de portfólios na documentação do AWS Service Catalog.

Limitações

- Os produtos do AWS Service Catalog que você deseja copiar entre regiões ou contas não podem pertencer a mais de um portfólio.

Arquitetura

O diagrama a seguir mostra a cópia dos produtos do AWS Service Catalog de uma conta de origem para uma conta de destino.

O diagrama a seguir mostra a cópia dos produtos do AWS Service Catalog de uma região de origem para uma região de destino.

Pilha de tecnologia

- Amazon CloudWatch
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS Service Catalog

Automação e escala

Você pode escalar a abordagem desse padrão usando uma função do Lambda que pode ser escalada dependendo do número de solicitações recebidas ou de quantos produtos do AWS Service Catalog você precisa copiar. Para obter mais informações sobre isso, consulte Escalabilidade da função do Lambda na documentação do AWS Lambda.

Ferramentas

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.

- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Service Catalog ajuda você a gerenciar de modo centralizado os catálogos de serviços de TI aprovados para a AWS. Os usuários finais podem implantar rapidamente somente os serviços de TI aprovados de que precisam, seguindo as restrições definidas pela organização.

Código

Você pode usar o pacote `cross-account-copy` (anexado) para copiar produtos do AWS Service Catalog entre contas ou o pacote `cross-region-copy` (anexado) para copiar produtos entre regiões.

O pacote `cross-account-copy` contém os seguintes arquivos:

- `copyconf.properties`: o arquivo de configuração que contém os parâmetros de ID de conta da região e da AWS para copiar produtos entre contas.
- `scProductCopyLambda.py`: a função Python para copiar produtos entre contas.
- `createDestAccountRole.sh`: o script para criar um perfil do IAM na conta de destino.
- `createSrcAccountRole.sh`: o script para criar um perfil do IAM na conta de origem.
- `copyProduct.sh`: o script para criar e invocar a função do Lambda para copiar produtos entre contas.

O pacote `cross-region-copy` contém os seguintes arquivos:

- `copyconf.properties`: o arquivo de configuração que contém os parâmetros de ID de conta da região e da AWS para copiar produtos entre regiões.
- `scProductCopyLambda.py`: a função Python para copiar produtos entre regiões.
- `copyProduct.sh`: o script para criar um perfil do IAM e criar e invocar a função do Lambda para copiar produtos entre regiões.

Épicos

Opção 1 – Copiar os produtos do AWS Service Catalog entre contas

Tarefa	Descrição	Habilidades necessárias
Atualizar o arquivo de configuração.	1. Faça download do pacote `cross-account-copy` (anexado) na sua máquina local. 2. Atualize o arquivo de configuração `copyconf.properties` com os valores a seguir: • `srcRegion` : forneça a região de origem que contém os produtos. • `destRegion` : forneça a região de destino dos produtos. • `sourceAccountId` : forneça a ID da conta da AWS da AWS da sua conta de origem. • `destAccountId` : forneça a ID da conta da AWS da AWS da sua conta de destino.	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem
Configure suas credenciais para a AWS CLI na conta de destino.	Configure suas credencia is para acessar a AWS CLI em sua conta de destino executando o comando `aws configure` e fornecendo os seguintes valores:	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias

	`$aws configure`
	`AWS Access Key ID`
	` [None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	` [None]: <your_sec`
	`ret_access_key>`
	`Default region name`
	` [None]: Region`
	`Default output format`
	` [None]:`
	
	Para obter mais informações sobre isso, consulte Princípios básicos da configuração na documentação da interface da linha de comando da AWS.	

Tarefa	Descrição	Habilidades necessárias

Configure suas credenciais para a AWS CLI na conta de origem.	Configure suas credencia is para acessar a AWS CLI em sua conta de origem executando o comando `aws configure` e fornecendo os seguintes valores:
	`$aws configure`
	`AWS Access Key ID`
	`[None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	`[None]: <your_sec`
	`ret_access_key>`
	`Default region name`
	`[None]: Region`
	`Default output format`
	`[None]:`
	Para obter mais informações sobre isso, consulte Princípio s básicos da configuração na documentação da interface da linha de comando da AWS.
		Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
Crie uma função de execução do Lambda na sua conta de destino.	Execute o script `createDestAccountRole.sh` na sua conta de destino. O script implementa as seguintes ações: • Cria uma função de execução do Lambda na sua conta de destino • Cria e anexa a política do IAM para a função de execução do Lambda	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem
Crie o perfil do IAM entre contas na sua conta de origem.	Execute o script `createSrcAccountRole.sh` na sua conta de origem. O script implementa as seguintes ações: • Cria um perfil do IAM entre contas em sua conta de origem que é assumida pela função de execução do Lambda na conta de destino para copiar produtos • Cria e anexa uma política do IAM para a função entre contas em sua conta de origem	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
Execute o script copyProduct na sua conta de destino.	Execute o script `copyProduct.sh` na sua conta de destino. O script implementa as seguintes ações: • Cria e invoca a função do Lambda para copiar produtos da conta de origem para a conta de destino	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Opção 2 – Copiar produtos do AWS Service Catalog de uma região de origem para uma região de destino

Tarefa	Descrição	Habilidades necessárias
Atualizar o arquivo de configuração.	1. Faça download do pacote `cross-region-copy` (anexado) na sua máquina local. 2. Atualize o arquivo de configuração `copyconf.properties` com os valores a seguir: • `srcRegion` : forneça a região de origem que contém os produtos. • `destRegion` : forneça a região de destino dos produtos. • `accountId` : forneça o ID da sua conta da AWS.	Administrador de sistemas da AWS, administrador da nuvem, administrador da AWS

Tarefa	Descrição	Habilidades necessárias

Configurar as suas credencia is para a CLI da AWS	Configure suas credenciais para acessar a CLI da AWS em seu ambiente executando o comando `aws configure` e fornecendo os seguintes valores:
	
	`$aws configure`
	`AWS Access Key ID`
	`[None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	`[None]: <your_sec`
	`ret_access_key>`
	`Default region name`
	`[None]: Region`
	`Default output format`
	`[None]:`
	
	Para obter mais informações sobre isso, consulte Princípio s básicos da configuração na documentação da interface da linha de comando da AWS.
		Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
Execute o script CopyProduct.	Execute o script `copyProduct.sh` na sua região de destino. O script implementa as seguintes ações: • Cria uma função de execução do Lambda • Cria e anexa a política do IAM para a função de execução do Lambda • Cria e invoca a função do Lambda para copiar produtos da região de origem para a região de destino	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Recursos relacionados

- Criar uma função de execução do Lambda (documentação do AWS Lambda)
- Criar uma função do Lambda (documentação do AWS Lambda)
- Referência da API do AWS Service Catalog
- Documentação do AWS Service Catalog

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie uma matriz RACI ou RASCI para um modelo operacional em nuvem

Criado por Teddy Germade (AWS), Jerome Descreux (AWS), Josselin LE MINEUR (AWS) e Florian Leroux (AWS)

Resumo

O Cloud Center of Excellence (CCoE) ou CEE (Cloud Enablement Engine) é uma equipe capacitada e responsável, focada na prontidão operacional para a nuvem. Seu foco principal é transformar a organização de TI da informação de um modelo operacional on-premises para um modelo operacional em nuvem. O CCo E deve ser uma equipe multifuncional que inclua representação de infraestrutura, aplicativos, operações e segurança.

Um dos principais componentes de um modelo operacional em nuvem é uma matriz RACI ou matrix RASCI. Isso é usado para definir as funções e responsabilidades de todas as partes envolvidas nas atividades de migração e nas operações de nuvem. O nome da matriz é derivado dos tipos de responsabilidade definidos na matriz: responsável (R), responsável (A), suporte (S), consultado (C) e informado (I). O tipo de suporte é opcional. Se você a incluir, ela é chamada de matriz RASCI e, se você a excluir, é chamada de matriz RACI.

Começando com o modelo em anexo, sua equipe CCo E pode criar uma matriz RACI ou RASCI para sua organização. O modelo contém equipes, funções e tarefas que são comuns nos modelos operacionais de nuvem. A base dessa matriz são as tarefas relacionadas à integração de operações e aos recursos CCo E. No entanto, você pode personalizar esse modelo para atender às necessidades da estrutura e do caso de uso da sua organização.

Não há limites para a implementação de uma matriz RACI. Essa abordagem funciona para grandes organizações, startups e tudo mais. Para organizações pequenas, o mesmo recurso pode preencher várias funções.

Épicos

Crie a matriz

Tarefa	Descrição	Habilidades necessárias
Identifique as principais partes interessadas.	Identifique os principais gerentes de serviço e equipe vinculados aos objetivos	Gerente de projetos

Tarefa	Descrição	Habilidades necessárias
	estratégicos do seu modelo operacional de nuvem.	

Tarefa	Descrição	Habilidades necessárias

Personalize o modelo de matriz.	Faça o download do modelo na seção Anexos e, em seguida, atualize a matriz RACI ou RASCI da seguinte forma:
	• Na planilha do Cloud Teams, CCo atualize os nomes do stream E, os nomes das equipes e as descrições das equipes conforme necessário para sua organização.
	• Na planilha Cloud Roles, atualize as funções, os nomes das equipes e as descrições das funções conforme necessário para sua organização.
	• Na planilha RASCI, atualize o seguinte conforme necessário para sua organização:
	  • Na linha 1 e na coluna A, CCo atualize os fluxos E.
	  • Na linha 2, atualize os nomes das equipes.
	  • Na linha 3, atualize os nomes das funções.
	  • Nas colunas D e E, atualize os campos gerais e as atividades que você
		Gerente de projetos

Tarefa	Descrição	Habilidades necessárias
	deseja incluir no gráfico RASCI.	
Planeje reuniões.	1. Comunique os objetivos do RASCI a todas as partes interessadas. 2. Planeje uma ou mais reuniões para que um representante capacitado de cada equipe possa participar.	Gerente de projetos

Tarefa	Descrição	Habilidades necessárias
Conclua a matriz.	Na reunião com todas as partes interessadas, faça o seguinte: 1. Confirme se um represent ante de cada equipe está presente. A participação da equipe é obrigatória para que você possa atribuir com precisão os tipos de responsabilidade para cada tarefa. 2. Revise o que é uma matriz RASCI e os objetivos com os participantes. 3. Revise o modelo de responsabilidade compartil hada com os participantes para que eles entendam o escopo das responsab ilidades de sua organização pela segurança na nuvem. 4. Na planilha RASCI, para cada tarefa ou atividade , preencha as colunas F a AN para atribuir os seguintes tipos de responsabilidade: • Responsável (R): essa função é responsável por realizar o trabalho para concluir a tarefa. • Responsável (A): essa função é responsável por	Gerente de projetos

Tarefa	Descrição	Habilidades necessárias
	garantir que a tarefa seja concluída. Essa função também é responsáv el por garantir que os pré-requisitos sejam atendidos e delegar a tarefa aos responsáveis. • Suporte (S): essa função ajuda os responsáveis a concluir a tarefa. Esse tipo de responsabilidade é opcional e você pode optar por excluí-lo para criar uma matriz RACI mais tradicional. • Consultado (C): essa função deve ser consultada para obter opiniões ou conhecime ntos sobre a tarefa. Dependendo da tarefa, esse tipo de responsab ilidade pode não ser necessário. • Informado (I): essa função deve ser mantida atualizada sobre o progresso da tarefa e notificada quando a tarefa for concluída. • Em branco : essa função não está envolvida na atividade ou tarefa.	

Tarefa	Descrição	Habilidades necessárias
Compartilhe a matriz RASCI.	Quando a matriz RACI ou RASCI estiver completa, faça com que ela seja aprovada pela liderança. Salve-a em um repositório compartilhado ou em um local central onde todas as partes interessadas possam acessá-la. Recomendamos que você use processos padrão de controle de documentos para registrar e aprovar revisões na matriz.	Gerente de projetos

Recursos relacionados

- Modelo de Responsabilidade Compartilhada da AWS

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie alarmes para métricas personalizadas usando a detecção de CloudWatch anomalias da Amazon

Criado por Ram Kandaswamy (AWS) e Raheem Jiwani (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), você pode usar CloudWatch a Amazon para criar alarmes que monitoram métricas e enviam notificações ou fazem alterações automaticamente se um limite for violado.

Para evitar ser limitado por limites estáticos, você pode criar alarmes com base em padrões anteriores e notificá-lo se métricas específicas estiverem fora da janela operacional normal. Por exemplo, você pode monitorar os tempos de resposta da sua API a partir do Amazon API Gateway e receber notificações sobre anomalias que impedem que você cumpra um Acordo de Serviço (SLA).

Esse padrão descreve como usar a detecção de CloudWatch anomalias para métricas personalizadas. O padrão mostra como criar uma métrica personalizada no Amazon CloudWatch Logs Insights ou publicar uma métrica personalizada com uma função do AWS Lambda e, em seguida, configurar a detecção de anomalias e criar notificações usando o Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um tópico do SNS existente, configurado para enviar notificações por e-mail. Para obter mais informações sobre isso, consulte Conceitos básicos do Amazon SNS na documentação do Amazon SNS.
- Um aplicativo existente, configurado com o CloudWatch Logs.

Limitações

- CloudWatch as métricas não oferecem suporte a intervalos de tempo de milissegundos. Para obter mais informações sobre a granularidade de métricas regulares e personalizadas, consulte a Amazon. CloudWatch FAQs

Arquitetura

O diagrama mostra o seguinte fluxo de trabalho:

1. Os registros que usam métricas criadas e atualizadas pelo CloudWatch Logs são transmitidos para CloudWatch.
2. Um alarme é iniciado com base nos limites e envia um alerta para um tópico do SNS.
3. O Amazon SNS lhe enviará uma notificação por e-mail.

Pilha de tecnologia

- CloudWatch
- AWS Lambda
- Amazon SNS

Ferramentas

- CloudWatchA Amazon fornece uma solução de monitoramento confiável, escalável e flexível.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem provisionar ou gerenciar servidores.
- O Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens de publicadores para assinantes.

Épicos

Configurar detecção de anomalias para uma métrica personalizada

Tarefa	Descrição	Habilidades necessárias
Opção 1 - Crie uma métrica personalizada com uma função do Lambda.	Faça o download do `lambda_function.py` arquivo (anexado) e, em seguida, substitua o `lambda_function.py` arquivo de amostra	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	no aws-lambda-developer-guiderepositório na documentação GitHub da AWS. Isso fornece um exemplo de função Lambda que envia métricas personalizadas para CloudWatch o Logs. A função Lambda usa a API Boto3 para integração com o. CloudWatch Depois de executar a função Lambda, você pode entrar no AWS Management Console, abrir o CloudWatch console e a métrica publicada estará disponível em seu namespace publicado.	

Tarefa	Descrição	Habilidades necessárias
Opção 2 — Crie métricas personalizadas a partir de grupos de CloudWatch registros.	Faça login no AWS Management Console, abra o CloudWatch console e escolha Log groups. Escolha o grupo de logs para o qual você deseja criar uma métrica. Escolha Actions (Ações) e escolha Create metric filter (Criar filtro de métrica). Em Filter pattern (Padrão de filtro), insira o padrão de filtro que deseja usar. Para obter mais informações, consulte Sintaxe de filtros e padrões na CloudWatch documentação. Para testar seu padrão de filtro, insira um ou mais eventos de logs em Test Pattern (Testar padrão). Cada evento de log deve estar dentro de uma linha, porque as quebras de linha são usadas para separar eventos de log na caixa Log event messages (Mensagens do evento de log). Depois de testar o padrão, você pode inserir um nome e um valor para sua métrica em Detalhes da métrica.	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações e etapas para criar uma métrica personalizada, consulte Criar um filtro de métrica para um grupo de registros na CloudWatch documentação.	

Tarefa	Descrição	Habilidades necessárias
Crie um alarme para sua métrica personalizada.	No CloudWatch console, escolha Alarmes e, em seguida, escolha Criar alarme. Escolha Selecionar métrica e insira o nome da métrica que você criou anteriormente na caixa de pesquisa. Escolha a guia Métricas em gráficos e configure as opções de acordo com seus requisitos. Em Condições, escolha Detecção de anomalias em vez de Limites estáticos. Isso mostra uma banda com base em dois desvios padrão. É possível definir limites e ajustá-los de acordo com seus requisitos. Escolha Próximo. **Note** A banda é dinâmica e depende da qualidade dos pontos de dados. Quando você começa a agregar mais dados, a faixa e os limites são atualizados automatic amente.	DevOps engenheiro, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Configure notificações do SNS.	Em Notification (Notificação), escolha um tópico do SNS para notificar quando o alarme estiver no estado `ALARM`, `OK` ou `INSUFFICIENT_DATA` . Para que o alarme envie várias notificações para o mesmo estado de alarme ou para diferentes estados de alarme, escolha Add notificat ion (Adicionar notificação). Escolha Próximo. Digite um nome e uma descrição para o alarme. O nome deve conter somente caracteres ASCII. Escolha Próximo. Em Preview and create (Previsualizar e criar), confirme se as informações e condições estão corretas e escolha Create alarm (Criar alarme).	DevOps engenheiro, AWS DevOps

Recursos relacionados

- Publicação de métricas personalizadas em CloudWatch
- Usando a detecção de CloudWatch anomalias
- Eventos de alarme e Amazon EventBridge
- Quais são as práticas recomendadas a serem seguidas ao enviar métricas personalizadas para o Cloud Watch? (vídeo)
- Introdução ao CloudWatch Application Insights (vídeo)
- Detecte anomalias com CloudWatch (vídeo)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Crie um AWS Cloud9 IDE que usa volumes do Amazon EBS com criptografia padrão

Criado por Janardhan Malyala (AWS) e Dhrubajyoti Mukherjee (AWS)

Resumo

Aviso: não AWS Cloud9 está mais disponível para novos clientes. Os clientes existentes do AWS Cloud9 podem continuar usando o serviço normalmente. Saiba mais

É possível usar criptografia por padrão para aplicar a criptografia de seus volumes e cópias de snapshots do Amazon Elastic Block Store (Amazon EBS) na Nuvem Amazon Web Services (AWS).

Você pode criar um ambiente de desenvolvimento integrado (IDE) do AWS Cloud9 que usa volumes do EBS criptografados por padrão. No entanto, a função vinculada ao serviço do AWS Identity and Access Management (IAM) para o AWS Cloud9 exige acesso à chave do AWS Key Management Service (AWS KMS) para esses volumes do EBS. Se o acesso não for fornecido, o IDE do AWS Cloud9 pode falhar ao iniciar e a depuração poderá ser difícil.

Esse padrão fornece as etapas para adicionar a função vinculada ao serviço para AWS Cloud9 e para a chave do AWS KMS usada pelos volumes do EBS. A configuração descrita por esse padrão ajuda você a criar e iniciar com êxito um IDE que usa volumes do EBS com criptografia por padrão.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Criptografia padrão ativada para volumes do EBS. Para obter mais informações sobre criptografia por padrão, consulte a criptografia do Amazon EBS na documentação do Amazon Elastic Compute Cloud EC2 (Amazon).
- Uma chave KMS existente gerenciada pelo cliente para criptografar seus volumes do EBS.

> **Note**
>
> Você não precisa criar a função vinculada ao serviço para o AWS Cloud9. Quando você cria um ambiente de desenvolvimento do AWS Cloud9, o AWS Cloud9 cria uma função vinculada ao serviço para você.

Arquitetura

Pilha de tecnologia

- AWS Cloud9
- IAM
- AWS KMS

Ferramentas

- O AWS Cloud9 é um ambiente de desenvolvimento integrado (IDE) que ajuda você a codificar, criar, executar, testar e depurar software. Ele também ajuda você a lançar software na Nuvem AWS.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon Elastic Compute Cloud (Amazon). EC2
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.

Épicos

Encontre o valor da chave de criptografia padrão

Tarefa	Descrição	Habilidades necessárias
Registre o valor da chave de criptografia padrão para os volumes do EBS.	Faça login no AWS Management Console e abra o EC2 console da Amazon. Escolha EC2 painel e, em seguida, escolha Proteção e segurança de dados em Atributos da conta. Na seção Criptografia do EBS, copie e	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	registre o valor na Chave de criptografia padrão.	

Forneça acesso à chave do AWS KMS

Tarefa	Descrição	Habilidades necessárias
Forneça ao AWS Cloud9 acesso à chave KMS para volumes do EBS.	1. Abra o console do AWS KMS e escolha Chaves gerenciadas pelo cliente. Selecione a chave do AWS KMS usada para a criptografia do Amazon EBS e, em seguida, escolha Exibir chave. 2. Na guia Política de chaves, confirme se você pode ver o formato de texto da política de chaves. Se você não conseguir ver o formulário de texto, escolha Mudar para visualização da política. 3. Escolha Editar. Adicione o código na seção Informações adicionais à política e escolha Salvar alterações. As mudanças na política permitem que a função vinculada ao serviço do AWS Cloud9 e `AWSServiceRoleForAWSCloud9` , acesse a chave.	Arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações sobre a atualização de uma política de chaves, consulte Como alterar uma política de chaves (documentação do AWS KMS). **Important** A função vinculada ao serviço para o AWS Cloud9 é criada automaticamente quando você inicia seu primeiro IDE. Para obter mais informaçõ es, consulte Criar uma função vinculada ao serviço na documenta ção do AWS Cloud9.	

Crie e inicie o IDE

Tarefa	Descrição	Habilidades necessárias
Crie e inicie o IDE do AWS Cloud9.	Abra o console do AWS Cloud9 e escolha Criar ambiente. Configure o IDE de acordo com seus requisito s seguindo as etapas de Criação de um EC2 ambiente na documentação do AWS Cloud9.	Arquiteto de nuvem, DevOps engenheiro

Recursos relacionados

- Criptografe volumes do EBS usados pelo AWS Cloud9
- Criar um perfil vinculado a serviço para o AWS Cloud9
- Crie um EC2 ambiente no AWS Cloud9

Mais informações

Atualizações da política de chave do AWS KMS

Substitua <aws_accountid> pelo seu ID de conta da AWS.

```
{
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
```

Usando uma chave entre contas

Se quiser usar uma chave KMS entre contas, você deve usar uma concessão em combinação com a política de chaves KMS. Isso permite o acesso entre contas à chave. Na mesma conta que você usou para criar o ambiente Cloud9, execute o comando a seguir no terminal.

```
aws kms create-grant \
 --region <Region where Cloud9 environment is created> \
 --key-id <The cross-account KMS key ARN> \
 --grantee-principal arn:aws:iam::<The account where Cloud9 environment is
 created>:role/aws-service-role/cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9 \
 --operations "Encrypt" "Decrypt" "ReEncryptFrom" "ReEncryptTo" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "DescribeKey" "CreateGrant"
```

Depois de executar esse comando, você pode criar ambientes Cloud9 usando a criptografia do EBS com uma chave em uma conta diferente.

Crie CloudWatch painéis da Amazon baseados em tags automaticamente

Criado por Janak Vadaria (AWS), RAJNEESH TYAGI (AWS) e Vinodkumar Mandalapu (AWS)

Resumo

Criar diferentes CloudWatch painéis da Amazon manualmente pode ser demorado, especialmente quando você precisa criar e atualizar vários recursos para escalar automaticamente seu ambiente. Uma solução que cria e atualiza seus CloudWatch painéis automaticamente pode economizar seu tempo. Esse padrão ajuda você a implantar um AWS Cloud Development Kit (AWS CDK) pipeline totalmente automatizado que cria e atualiza CloudWatch painéis para seus AWS recursos com base em eventos de alteração de tag, para exibir as métricas do Golden Signals.

Na engenharia de confiabilidade de sites (SRE), Golden Signals se refere a um conjunto abrangente de métricas que oferecem uma visão ampla de um serviço do ponto de vista do usuário ou do consumidor. Essas métricas consistem em latência, tráfego, erros e saturação. Para obter mais informações, consulte O que é engenharia de confiabilidade do site (SRE)? no AWS site.

A solução fornecida por esse padrão é orientada por eventos. Depois de implantado, ele monitora continuamente os eventos de alteração da tag e atualiza automaticamente os CloudWatch painéis e os alarmes.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- AWS Command Line Interface (AWS CLI), instalado e configurado
- Pré-requisitos para a v2 AWS CDK
- Um ambiente inicializado em AWS
- Python versão 3
- AWS SDK para Python (Boto3), instalado
- Node.js versão 18 ou posterior
- Gerenciador de pacotes Node (npm), instalado e configurado para o AWS CDK
- Familiaridade moderada (nível 200) com e AWS CDK AWS CodePipeline

Limitações

Atualmente, essa solução cria painéis automatizados somente para os seguintes serviços da AWS:

- Amazon Relational Database Service (Amazon RDS)
- AWS Auto Scaling
- Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB
- AWS Lambda

Arquitetura

Pilha de tecnologias de destino

- CloudWatch painéis
- CloudWatch alarmes

Arquitetura de destino

1. Um evento de alteração de AWS tag para as tags de aplicativo configuradas ou alterações de código inicia um pipeline AWS CodePipeline para criar e implantar CloudWatch painéis atualizados.
2. AWS CodeBuild executa um script Python para encontrar os recursos que têm tags configuradas e armazena o recurso IDs em um arquivo local em um CodeBuild ambiente.
3. CodeBuild executa o cdk synth para gerar AWS CloudFormation modelos que implantam CloudWatch painéis e alarmes.
4. CodePipeline implanta os AWS CloudFormation modelos na região especificada Conta da AWS .
5. Quando a AWS CloudFormation pilha for implantada com sucesso, você poderá visualizar os CloudWatch painéis e os alarmes.

Automação e escala

Essa solução foi automatizada usando AWS CDK o. Você pode encontrar o código nos painéis GitHub Golden Signals no CloudWatch repositório da Amazon. Para escalonamento adicional e para criar painéis personalizados, você pode configurar várias chaves e valores de tag.

Ferramentas

Serviço da Amazon

- EventBridgeA Amazon é um serviço de barramento de eventos sem servidor que ajuda você a conectar seus aplicativos a dados em tempo real de várias fontes, incluindo AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras. Contas da AWS
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir com os serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Práticas recomendadas

Como prática recomendada de segurança, você pode usar criptografia e autenticação para os repositórios de origem que se conectam aos seus pipelines. Para obter mais práticas recomendadas, consulte as CodePipeline melhores práticas e os casos de uso na CodePipeline documentação.

Épicos

Configurar e implantar o aplicativo de amostra

Tarefa	Descrição	Habilidades necessárias
Configure e implante o aplicativo de amostra.	1. Clone o repositório de código de GitHub amostra usando o comando:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/aws-samples/golden-signals-dashboards-sample-app` 2. Navegue até o repositório clonado em seu computador e abra o `src/project-settings.ts` arquivo com o editor de sua preferência. 3. Altere o valor `projectSettings` constante de acordo com suas tags AWS de recursos e mapeamentos de aplicativos. 4. Defina `AWS_ACCOUNT` as variáveis de `GS_DASHBOARD_INSTANCE` ambiente`AWS_REGION` , e: • `AWS_ACCOUNT` Defina o ID da conta da sua AWS conta. • `AWS_REGION` Defina a região em que você deseja implantar o aplicativo de amostra. • `GS_DASHBOARD_INSTANCE` Defina como `devtest`, ou`prod`, dependendo do seu ambiente de desenvolvimento. (Recomendamos	

Tarefa	Descrição	Habilidades necessárias
	`test` o procedimento de teste descrito neste padrão.) 5. Configure o AWS CLI com suas AWS credenciais. Para obter mais informaçõ es, consulte Definir e visualizar as configurações usando comandos na AWS CLI documentação. 6. Execute o comando a seguir para implantar o aplicativo de amostra do painel Golden Signals: `sh deploy.sh`	

Tarefa	Descrição	Habilidades necessárias
Crie painéis e alarmes automaticamente.	Depois de implantar o aplicativo de amostra, você pode criar qualquer um dos recursos suportados por essa solução com os valores de tag esperados, o que criará automaticamente os painéis e alarmes especificados. Para testar essa solução, crie uma AWS Lambda função: 1. Faça login no local AWS Management Console em Região da AWS que você implantou o aplicativo de amostra. 2. Abra o console Lambda em. https://console.aws.amazon.com/lambda/ 3. Escolha Criar uma função e, em seguida, insira o nome da função. 4. No painel Configurações avançadas, selecione Ativar tags e escolha Adicionar nova tag. Insira a chave e o valor a seguir: • Chave: `AutoDashboard` • Valor: `True` 5. Escolha a opção Criar função.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	A função Lambda inicia imediatamente um pipeline de código, que cria automaticamente os painéis e alarmes para essa função específica do Lambda. 6. Para ver os painéis e alarmes automatizados, abra o CloudWatch console em. https://console.aws.amazon.com/cloudwatch/ Você pode visualizar os painéis e alarmes personalizados para a função especificada na `projectSettings` constante (APP1-lambda por padrão). 7. Selecione o painel da função Lambda para visualizar painéis automatizados adicionais que foram criados como parte dessa solução. 8. Repita essas etapas para outros serviços, como Amazon RDS, Amazon SNS e DynamoDB AWS Auto Scaling, para gerar os painéis associados. Para obter um exemplo para o Amazon RDS,	

Tarefa	Descrição	Habilidades necessárias
	consulte a seção Informaçõ es adicionais.	

Remova o aplicativo de amostra

Tarefa	Descrição	Habilidades necessárias
Remova a `golden-signals-dashboard` construção.	1. Para remover todas as AWS CloudFormation pilhas criadas pelo aplicativo de amostra, você precisa reconfigurar as variáveis de `GS_DASHBOARD_INSTANCE` ambiente `AWS_ACCOUNT` `AWS_REGION` , e. O `destroy.sh` comando exige essas configurações. • `AWS_ACCOUNT` é o ID da sua AWS conta. • `AWS_REGION` é a região em que você implantou seu aplicativo de amostra. • `GS_DASHBOARD_INSTANCE` é `dev`, `test`, ou `prod`, com base em suas configurações anteriores. 2. Configure AWS CLI com suas AWS credenciais. 3. Execute o comando a seguir para remover o aplicativo de amostra e	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	todas as AWS CloudForm ation pilhas associadas: `sh destroy.sh`	

Solução de problemas

Problema	Solução
Comando Python não encontrado (referindo-se à `findresources.sh` linha 8).	Verifique a versão da sua instalação do Python. Se você instalou o Python versão 3, `python` `python3` substitua pela linha 8 do `resources .sh` arquivo e execute o `sh deploy.sh` comando novamente para implantar a solução.

Recursos relacionados

- Bootstrapping (documentação)AWS CDK
- Usando perfis nomeados (AWS CLI documentação)
- AWS CDK Workshop

Mais informações

A ilustração a seguir mostra um painel de exemplo para o Amazon RDS criado como parte dessa solução.

Documente seu projeto de landing zone na AWS

Criado por Michael Daehnert (AWS), Florian Langer (AWS) e Michael Lodemann (AWS)

Resumo

Uma landing zone é um ambiente multicontas bem arquitetado, baseado nas melhores práticas de segurança e conformidade. É o contêiner corporativo que contém todas as suas unidades organizacionais (OUs) Contas da AWS, usuários e outros recursos. Uma landing zone pode ser dimensionada para atender às necessidades de uma empresa de qualquer tamanho. AWS tem duas opções para criar sua zona de pouso: uma zona de pouso baseada em serviços AWS Control Towerou uma zona de pouso personalizada que você constrói. Cada opção requer um nível de AWS conhecimento diferente.

AWS criado AWS Control Tower para ajudar você a economizar tempo automatizando a configuração de um landing zone. AWS Control Tower é gerenciado AWS e usa as melhores práticas e diretrizes para ajudá-lo a criar seu ambiente básico. AWS Control Tower usa serviços integrados, como AWS Service Catalogue AWS Organizations, para provisionar contas em sua landing zone e gerenciar o acesso a essas contas.

AWS os projetos de landing zone variam em requisitos, detalhes de implementação e itens de ação operacional. Há aspectos de personalização que precisam ser tratados em cada implementação de landing zone. Isso inclui (mas não se limita a) como o gerenciamento de acesso é tratado, qual pilha de tecnologia é usada e quais são os requisitos de monitoramento para a excelência operacional. Esse padrão fornece um modelo que ajuda você a documentar seu projeto de landing zone. Ao usar o modelo, você pode documentar seu projeto com mais rapidez e ajudar suas equipes de desenvolvimento e operações a entender sua landing zone.

Pré-requisitos e limitações

Limitações

Esse padrão não descreve o que é um landing zone ou como implementá-lo. Para obter mais informações sobre esses tópicos, consulte a seção Recursos relacionados.

Épicos

Crie o documento de design

Tarefa	Descrição	Habilidades necessárias
Identifique as principais partes interessadas.	Identifique os principais gerentes de serviço e equipe vinculados à sua landing zone.	Gerente de projetos
Personalize o modelo.	Faça o download do modelo na seção Anexos e atualize o modelo da seguinte forma: 1. Remova todas as seções que não se aplicam à landing zone ou aos processos da sua organizaç ão. 2. Adicione qualquer seção que seja exclusiva da sua organização.	Gerente de projetos
Preencha o modelo.	Em reuniões com as partes interessadas ou usando um write-and-review processo, preencha o modelo da seguinte forma: 1. Use as orientações e as informações nas caixas azuis para concluir cada seção. 2. Substitua ou remova todos os campos amarelos por valores personalizados para sua organização.	Gerente de projetos

Tarefa	Descrição	Habilidades necessárias
	3. Substitua ou remova qualquer campo de imagem com sua arquitetura personalizada ou diagramas de fluxo. 4. Preencha a seção Histórico de revisões e Colaboradores do modelo.	
Compartilhe o documento de design.	Quando a documentação do projeto do landing zone estiver completa, salve-a em um repositório compartilhado ou em um local central onde todas as partes interessadas possam acessá-la. Recomendamos que você use processos padrão de controle de documentos para registrar e aprovar revisões no documento de design.	Gerente de projetos

Recursos relacionados

- AWS Control Tower documentação
  - Planeje sua AWS Control Tower landing zone
  - AWS estratégia de várias contas para sua AWS Control Tower landing zone
  - Dicas administrativas para configuração da landing zone
  - Expectativas para a configuração da landing zone
- Personalizações para AWS Control Tower(Biblioteca deAWS soluções)
- Configurando um ambiente seguro e escalável com várias contas (AWS orientaçãoAWS prescritiva)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Melhore o desempenho operacional habilitando o Amazon DevOps Guru em várias regiões e contas da AWS e OUs com o AWS CDK

Criado pelo Dr. Rahul Sharad Gaikwad (AWS)

Resumo

Esse padrão demonstra as etapas para habilitar o serviço Amazon DevOps Guru em várias regiões, contas e unidades organizacionais () da Amazon Web Services (AWSOUs) usando o AWS Cloud Development Kit (AWS CDK) em. TypeScript Você pode usar pilhas de CDK da AWS para implantar a AWS a CloudFormation StackSets partir da conta administrativa (primária) da AWS para habilitar o Amazon DevOps Guru em várias contas, em vez de fazer login em cada conta e ativar o DevOps Guru individualmente para cada conta.

O Amazon DevOps Guru fornece recursos de operações de inteligência artificial (AIOps) para ajudá-lo a melhorar a disponibilidade de seus aplicativos e resolver problemas operacionais com mais rapidez. DevOps O Guru reduz seu esforço manual aplicando recomendações baseadas em aprendizado de máquina (ML), sem exigir nenhum conhecimento de ML. DevOps O Guru analisa seus recursos e dados operacionais. Se detectar alguma anomalia, ele fornece métricas, eventos e recomendações para ajudar a resolver o problema.

Esse padrão descreve três opções de implantação para habilitar o Amazon DevOps Guru:

- Para todos os recursos de pilha em várias contas e regiões
- Para todos os recursos de pilha OUs
- Para recursos de pilha específicos em várias contas e regiões

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI), instalada e configurada. (Consulte Instalar, atualizar e desinstalar a AWS CLI na documentação da AWS CLI.)
- AWS CDK Toolkit, instalado e configurado. (Consulte o AWS CDK Toolkit na documentação do AWS CDK.)
- Node Package Manager (npm), instalado e configurado para o AWS CDK em. TypeScript (Consulte Como baixar e instalar o Node.js e o npm na documentação do npm.)

- Python3 instalado e configurado, para executar um script Python para injetar tráfego no aplicativo de amostra com tecnologia sem servidor. (Consulte Configuração e uso do Python na documentação do Python.)
- Pip, instalado e configurado para instalar a biblioteca de solicitações do Python. (Consulte as instruções de instalação do pip no PyPI site.)

Versões do produto

- AWS CDK Toolkit versão 1.107.0 ou superior
- npm versão 7.9.0 ou superior
- Node.js versão 15.3.0 ou superior

Arquitetura

Tecnologias

A arquitetura para esse padrão inclui os seguintes serviços:

- DevOps Guru da Amazon
- AWS CloudFormation
- Amazon API Gateway
- AWS Lambda
- Amazon DynamoDB
- Amazon CloudWatch
- AWS CloudTrail

Pilhas do AWS CDK

O padrão usa as seguintes pilhas do AWS CDK:

- `CdkStackSetAdminRole`: cria uma função de administrador do AWS Identity and Access Management (IAM) para estabelecer uma relação de confiança entre as contas de administrador e de destino.
- `CdkStackSetExecRole`: cria um perfil do IAM para confiar na conta do administrador.

- `CdkDevopsGuruStackMultiAccReg`— Ativa o DevOps Guru em várias regiões e contas da AWS para todas as pilhas e configura as notificações do Amazon Simple Notification Service (Amazon SNS).
- `CdkDevopsGuruStackMultiAccRegSpecStacks`— Habilita o DevOps Guru em várias regiões e contas da AWS para pilhas específicas e configura notificações do Amazon SNS.
- `CdkDevopsguruStackOrgUnit`— Habilita o DevOps Guru OUs e configura as notificações do Amazon SNS.
- `CdkInfrastructureStack`: implanta amostras de componentes de aplicativos com tecnologia sem servidor, como API Gateway, Lambda e DynamoDB, na conta do administrador para demonstrar a injeção de falhas e a geração de insights.

Arquitetura de aplicativo de exemplo

O diagrama a seguir mostra a arquitetura de um aplicativo de exemplo com tecnologia sem servidor que foi implantado em várias contas e regiões. O padrão usa a conta do administrador para implantar todas as pilhas do AWS CDK. Ele também usa a conta de administrador como uma das contas de destino para configurar o DevOps Guru.

1. Quando o DevOps Guru está ativado, ele primeiro define o comportamento de cada recurso e, em seguida, ingere dados operacionais das métricas fornecidas. CloudWatch
2. Se ele detecta uma anomalia, ela a correlaciona com os eventos e gera uma CloudTrail visão.
3. O insight fornece uma sequência correlacionada de eventos junto com as recomendações prescritas para permitir que o operador identifique o recurso culpado.
4. O Amazon SNS envia mensagens de notificação para o operador.

Automação e escala

O GitHub repositório fornecido com esse padrão usa o AWS CDK como uma ferramenta de infraestrutura como código (IaC) para criar a configuração dessa arquitetura. O AWS CDK ajuda você a orquestrar recursos e habilitar o DevOps Guru em várias contas, regiões e. OUs

Ferramentas

Serviços da AWS

- AWS CDK — O AWS Cloud Development Kit (AWS CDK) ajuda você a definir sua infraestrutura de nuvem como código em uma das cinco linguagens de programação compatíveis: TypeScript,, JavaScript Python, Java e C#.
- AWS CLI: a AWS Command Line Interface (AWS CLI) é uma ferramenta unificada que fornece uma interface de linha de comando consistente para interagir com os serviços e os recursos da AWS.

Código

O código-fonte desse padrão está disponível no GitHub repositório Amazon DevOps Guru CDK Samples. O código do AWS CDK está escrito em TypeScript. Para clonar e usar o repositório, siga as instruções na próxima seção.

> **Important**
>
> Algumas das histórias desse padrão incluem exemplos de comandos do AWS CDK e da AWS CLI formatados para Unix, Linux e macOS. Para Windows, substitua o caractere de continuação Unix de barra invertida (\) no final de cada linha por um circunflexo (^).

Épicos

Prepare os recursos da AWS para implantação

Tarefa	Descrição	Habilidades necessárias

Configure perfis nomeados da AWS.	Configure seus perfis nomeados da AWS da seguinte forma para implantar pilhas em um ambiente de várias contas.
	
	Para a conta de administrador:
	
	`$aws configure --profile administrator`
	`AWS Access Key ID [****]: <your-adm`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	inistrator-access-key-ID> AWS Secret Access Key [****]: <your-administrator-secret-access-key> Default region name [None]: <your-administrator-region> Default output format [None]: json Para a conta de destino: $aws configure --profile target AWS Access Key ID [****: <your-target-access-key-ID> AWS Secret Access Key [****]: <your-target-secret-access-key> Default region name [None]: <your-target-region> Default output format [None]: json Para obter mais informações, consulte Uso de perfis nomeados na documentação da AWS CLI.	

Tarefa	Descrição	Habilidades necessárias
Verifique as configurações do perfil da AWS.	(Opcional) Você pode verificar suas configurações de perfil da AWS nos arquivos `credentials` e `config` seguindo as instruções em Definir e visualizar configurações na documentação da AWS CLI.	DevOps engenheiro
Verifique a versão do AWS CDK.	Verifique a versão do AWS CDK Toolkit executando o seguinte comando: `$cdk --version` Este padrão requer a versão 1.107.0 ou superior. Se você tiver uma versão anterior do AWS CDK, siga as instruções na documentação do AWS CDK para atualizá-la.	DevOps engenheiro
Clone o código do projeto.	Clone o GitHub repositório desse padrão usando o comando: `$git clone https://github.com/aws-samples/amazon-devopsguru-cdk-samples.git`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Instale as dependências do pacote e compile os TypeScript arquivos.	Instale as dependências do pacote e compile os TypeScript arquivos executando os seguintes comandos:
	`$cd amazon-devopsguru-cdk-samples`
	`$npm install`
	`$npm fund`
	Esses comandos instalam todos os pacotes do repositório de exemplo.
	Important
	Se você receber algum erro sobre pacotes ausentes, use um dos seguintes comandos:
	`$npm ci`
	—ou—
	`$npm install -g @aws-cdk/<package-name>`
	Você pode encontrar a lista de nomes e versões de pacotes na seção `Dependencies` do arquivo `/amazon-devopsguru-cdk-samp`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`les/package.json` . Para obter mais informações, consulte npm ci e npm install na documentação do npm.	

Crie (sintetize) as pilhas do AWS CDK

Tarefa	Descrição	Habilidades necessárias
Configure um endereço de e-mail para notificações do Amazon SNS.	Siga estas etapas para fornecer um endereço de e-mail para notificações do Amazon SNS: 1. Edite os arquivos `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-stack.ts` e `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-org-uni-stack.ts` . 2. No `DevOpsGuruTopic` , seção `Subscription` , atualize o parâmetro `Endpoint` com seu endereço de e-mail. 3. Salve e feche os arquivos.	DevOps engenheiro
Crie o código do projeto.	Crie o código do projeto e sintetize as pilhas executando o comando:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`npm run build && cdk synth`
	
	Você deve ver uma saída semelhante a:
	
	`$npm run build && cdk synth`
	`> cdk-devopsguru@0.1.0 build`
	`> tsc`
	`Successfully synthesized to ~/amazon-devopsguru-cdk-samples/cdk.out`
	`Supply a stack id (CdkDevopsGuruStackMultiAccReg,CdkDevopsGuruStackMultiAccRegSpecStacks, CdkDevopsguruStackOrgUnit, CdkInfrastructureStack, CdkStackSetAdminRole, CdkStackSetExecRole) to display its template.`
	
	Para obter mais informações e etapas, consulte Seu primeiro aplicativo do AWS CDK na documentação do AWS CDK.	

Tarefa	Descrição	Habilidades necessárias

Liste as pilhas do AWS CDK.	Execute o comando a seguir para listar todas as pilhas do AWS CDK:
	`$cdk list`
	O comando exibe a seguinte lista:
	`CdkDevopsGuruStack`
	`MultiAccReg`
	`CdkDevopsGuruSt`
	`ackMultiAccRegSpec`
	`Stacks`
	`CdkDevopsguruStackOr`
	`gUnit`
	`CdkInfrastructureStac`
	`k`
	`CdkStackSetAdminRole`
	`CdkStackSetExecRole`
		DevOps engenheiro

Opção 1 - Habilite o DevOps Guru para empilhar todos os recursos em várias contas

Tarefa	Descrição	Habilidades necessárias
Implante as pilhas do AWS CDK para criar perfis do IAM.	Esse padrão usa CloudFormation StackSets a AWS para realizar operações de pilha em várias contas. Se você estiver criando seu primeiro conjunto de pilhas, deverá criar os seguintes perfis do IAM para obter as permissões necessárias configuradas em suas contas da AWS:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	• `AWSCloudFormationStackSetAdministrationRole` • `AWSCloudFormationStackSetExecutionRole` **Note** As funções devem ter esses nomes exatos. 1. Crie o perfil `AWSCloudFormationStackSetAdministrationRole` do IAM na conta do administrador (principal) executando o seguinte comando da CLI: `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Crie o perfil `AWSCloudFormationStackSetExecutionRole` do IAM em todas as contas de destino nas quais você deseja executar as instâncias da pilha. Para criar esse perfil, execute estes comandos da CLI:	

Tarefa	Descrição	Habilidades necessárias

	`$cdk deploy CdkStackSetExecRole \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --profile administrator`
	
	`$cdk deploy CdkStackSetExecRole \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --profile target`
	
	Para obter mais informações, consulte Conceder permissões autogerenciadas na CloudFormation documentação da AWS.	

Tarefa	Descrição	Habilidades necessárias
Implante a pilha de CDK da AWS para habilitar o DevOps Guru em várias contas.	A pilha `CdkDevopsGuruStackMultiAccReg` do AWS CDK cria conjuntos de pilhas para implantar instâncias de pilha em várias contas e regiões. Para implantar a pilha, execute o seguinte comando da CLI com os parâmetros especificados: `$cdk deploy CdkDevopsGuruStackMultiAccReg \ --profile administrator \ --parameters AdministratorAccountId=<administrator-account-ID> \ --parameters TargetAccountId=<target-account-ID> \ --parameters RegionIds="<region-1>,<region-2>"` Atualmente, o Amazon DevOps Guru está disponível nas regiões da AWS listadas nas perguntas frequentes do DevOps Guru.	DevOps engenheiro

Opção 2 - Habilite o DevOps Guru para todos os recursos da pilha OUs

Tarefa	Descrição	Habilidades necessárias
Extraia OU IDs.	No console do AWS Organizations, identifique as IDs unidades organizacionais nas quais você deseja habilitar o DevOps Guru.	DevOps engenheiro
Ative as permissões gerenciadas pelo serviço para. OUs	Se você estiver usando o AWS Organizations para gerenciamento de contas, deverá conceder permissões gerenciadas por serviços para habilitar o DevOps Guru. Em vez de criar as funções do IAM manualmente, use acesso confiável baseado na organização e funções vinculadas a serviços (). SLRs	DevOps engenheiro
Implante a pilha de CDK da AWS para habilitar o DevOps Guru em todo lugar. OUs	A `CdkDevopsguruStack OrgUnit` pilha de CDK da AWS possibilita o serviço DevOps Guru em todo lugar. OUs Para implantar a pilha, execute o seguinte comando com os parâmetros especificados: `$cdk deploy CdkDevopsguruStackOrgUnit \ --profile administrator \ --parameters RegionIds="<region-1>,<region-2>" \`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`--parameters OrganizationalUnitIds="<OU-1>,<OU-2>"`	

Opção 3 - Habilite o DevOps Guru para acumular recursos específicos em várias contas

Tarefa	Descrição	Habilidades necessárias

Implante as pilhas do AWS CDK para criar perfis do IAM.	Se você ainda não criou os perfis do IAM necessários mostrados na primeira opção, faça isso primeiro:
	1. Crie o perfil `AWSCloudFormationStackSetAdministrationRole` do IAM na conta do administrador (principal) executando o seguinte comando da CLI:
	`$cdk deploy CdkStackSetAdminRole --profile administrator`
	2. Crie o perfil `AWSCloudFormationStackSetExecutionRole` do IAM em todas as contas de destino nas quais você deseja executar as instâncias da pilha. Para criar esse perfil, execute os comandos da CLI:
	`$cdk deploy CdkStackSetExecRole \`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	<pre>--parameters AdministratorAccountId=<administrator-account-ID> \
	--profile administrator
	
	$cdk deploy CdkStackSetExecRole \
	--parameters AdministratorAccountId=<administrator-account-ID> \
	--profile target</pre>
	Para obter mais informações, consulte Conceder permissões autogerenciadas na CloudFormation documentação da AWS.	

Tarefa	Descrição	Habilidades necessárias
Exclua as pilhas existentes.	Se você já usou a primeira opção para ativar o DevOps Guru para todos os recursos da pilha, você pode excluir a pilha antiga usando o seguinte comando: `$cdk destroy CdkDevopsGuruStackMultiAccReg --profile administrator` Ou você pode alterar o parâmetro `RegionIds` ao reimplantar a pilha para evitar um erro de As pilhas já existem.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Atualize a pilha do AWS CDK com uma lista de pilhas.	1. Edite o arquivo `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-spec-stack.ts` . 2. `EmResources` ,, `CloudFormation StackNames` , liste as pilhas para as quais você deseja habilitar o DevOps Guru. Para fins de demonstração, o parâmetro especifica a pilha `CdkInfrastructureStack` , mas você pode editar essa entrada com base em seus requisitos. 3. Salve e feche o arquivo. 4. Para sintetizar e atualizar o modelo de pilha, execute: `$cdk synth`	Engenheiro de dados

Tarefa	Descrição	Habilidades necessárias
Implante a pilha de CDK da AWS para habilitar o DevOps Guru a usar recursos de pilha específicos em várias contas.	A `CdkDevopsGuruStack MultiAccRegSpecSta cks` pilha de CDK da AWS permite que o DevOps Guru use recursos de pilha específicos em várias contas. Para implantar a pilha, execute o seguinte comando: `$cdk deploy CdkDevops GuruStackMultiAccR egSpecStacks \ --profile administr ator \ --parameters AdministratorAccou ntId=<administrator- account-ID> \ --parameters TargetAccountId=<t arget-account-ID> \ --parameters RegionIds="<region -1>,<region-2>"` **Note** Se você implantou essa pilha anteriorm ente para a opção 1, altere o `RegionIds` parâmetro (certific ando-se de escolher entre as regiões disponíveis) para	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	evitar um erro de pilhas já existentes.	

Implante a pilha de infraestrutura do AWS CDK

Tarefa	Descrição	Habilidades necessárias
Implante a pilha de infraestrutura de amostra com tecnologia sem servidor.	O AWS CDK `CdkInfrastructureStack` stack implanta componentes sem servidor, como API Gateway, Lambda e uma tabela do DynamoDB, para demonstrar os insights do Guru. DevOps Para implantar a pilha, execute o seguinte comando: `$cdk deploy CdkInfrastructureStack --profile administrator`	DevOps engenheiro

Insira registros de amostra no DynamoDB.	Execute o comando a seguir para preencher a tabela do DynamoDB com registros de amostra. Forneça o caminho correto para o script `populate-shops-dynamodb-table.json` .
	`$aws dynamodb batch-write-item \`
	`  --request-items file://scripts/populate-shops-dynamodb-table.json \`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`--profile administrator`
	
	O comando exibe a seguinte saída:
	
	`{ "UnprocessedItems": {} }`	

Tarefa	Descrição	Habilidades necessárias

Verifique os registros inseridos no DynamoDB.	Para verificar se a tabela do DynamoDB inclui os registros de amostra do arquivo `populate-shops-dynamodb-table.json`, acesse a URL da API `ListRestApiEndpointMonitorOperator`, que é publicada como uma saída da pilha do AWS CDK. Você também pode encontrar esse URL na guia Saídas do CloudFormation console da AWS para a `CdkInfrastructureStack` pilha. A saída do AWS CDK deverá ser semelhante ao seguinte:
	`CdkInfrastructureStack.CreateRestApiMonitorOperatorEndpointD1D00045 = https://oure17c5vob.execute-api.<your-region>.amazonaws.com/prod/`
	`CdkInfrastructureStack.ListRestApiMonitorOperatorEndpointABBDB8D8 = https://cdff8icfrn4.execute-api.<your-region>.amazonaws.com/prod/`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Aguarde até que os recursos concluam a linha de base.	Essa pilha com tecnologia sem servidor tem alguns recursos. Recomendamos que você espere 2 horas antes de realizar as próximas etapas. Se você implantou essa pilha em um ambiente de produção, pode levar até 24 horas para concluir a linha de base, dependendo do número de recursos selecionados para monitorar no Guru. DevOps	DevOps engenheiro

Gere insights do DevOps Guru

Tarefa	Descrição	Habilidades necessárias
Atualize a pilha de infraestrutura do AWS CDK.	Para experimentar o DevOps Guru Insights, você pode fazer algumas alterações na configuração para reproduzir um problema operacional típico. 1. Edite o arquivo `/amazon-devopsguru-cdk-samples/lib/infrastructure-stack.ts` . 2. Na seção `DDB Table`, altere a capacidade de leitura da tabela do DynamoDB de 5 para 1. 3. Salve e feche o arquivo.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	4. Execute os seguintes comandos para sintetizar e implantar a pilha de infraestrutura atualizada do AWS CDK:
	`$cdk synth`
	`$cdk deploy CdkInfrastructureStack --profile administrator`	

Tarefa	Descrição	Habilidades necessárias
Injete solicitações de HTTP na API.	Injete tráfego de entrada na forma de solicitações de HTTP na API `ListRestApiMonitorOperatorEndpointxxxx` : 1. Edite o script `/amazon-devopsguru-cdk-samples/scripts/sendAPIRequest.py` do Python. 2. Atualize a variável `url` com o link da API para `ListRestApiMonitorOperatorEndpointxxxx` . Você pode encontrar essa URL na saída do comando de implantação do AWS CDK ou no console do AWS Cloudformation, na guia Saídas da pilha. 3. Salve e feche o arquivo. 4. Execute o script do Python usando o comando: `$python sendAPIRequest.py` 5. Certifique-se de obter um código de status 200. 6. Talvez seja necessário executar o script em vários terminais (de preferênc	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ia quatro) para injetar o tráfego em alta velocidade. 7. Depois que o script for executado em um loop de aproximadamente 10 minutos, você poderá ver uma visão operacional no console do DevOps Guru.	
Analise os insights do DevOps Guru.	Sob condições padrão, o painel do DevOps Guru exibe zero no contador de insights em andamento. Ao detectar uma anomalia, ele emite um alerta na forma de um insight. No painel de navegação, escolha Insights para ver os detalhes da anomalia, incluindo uma visão geral, métricas agregadas, eventos relevantes e recomendações. Para obter mais informações sobre a análise de insights, consulte a postagem do blog Como obter informações operacionais AIOps usando o Amazon DevOps Guru.	DevOps engenheiro

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpe e exclua recursos.	Depois de percorrer esse padrão, você deve remover os	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	recursos criados para evitar cobranças adicionais. Execute estes comandos:
	
	`$cdk destroy CdkDevopsGuruStackMultiAccReg --profile administrator`
	`$cdk destroy CdkDevopsguruStackOrgUnit --profile administrator`
	`$cdk destroy CdkDevopsGuruStackMultiAccRegSpecStacks --profile administrator`
	`$cdk destroy CdkInfrastructureStack --profile administrator`
	`$cdk destroy CdkStackSetAdminRole --profile administrator`
	`$cdk destroy CdkStackSetExecRole --profile administrator`
	`$cdk destroy CdkStackSetExecRole --profile target`	

Recursos relacionados

- Obtendo insights operacionais com o AIOps uso do Amazon DevOps Guru
- Configure facilmente o Amazon DevOps Guru em várias contas e regiões usando a AWS CloudFormation StackSets
- DevOps Workshop do Guru

Implemente o Account Factory for Terraform (AFT) usando um pipeline de bootstrap

Criado por Vinicius Elias (AWS) e Edgar Costa Filho (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Esse padrão fornece um método simples e seguro para implantar o AWS Control Tower Account Factory for Terraform (AFT) a partir da conta de gerenciamento do. AWS Organizations O núcleo da solução é um AWS CloudFormation modelo que automatiza a configuração do AFT criando um pipeline do Terraform, que é estruturado para ser facilmente adaptável à implantação inicial ou às atualizações subsequentes.

A segurança e a integridade dos dados são as principais prioridades AWS, portanto, o arquivo de estado do Terraform, que é um componente essencial que rastreia o estado da infraestrutura e das configurações gerenciadas, é armazenado com segurança em um bucket do Amazon Simple Storage Service (Amazon S3). Esse bucket é configurado com várias medidas de segurança, incluindo criptografia do lado do servidor e políticas para bloquear o acesso público, para ajudar a garantir que seu estado do Terraform seja protegido contra acesso não autorizado e violações de dados.

A conta de gerenciamento organiza e supervisiona todo o ambiente, portanto, é um recurso essencial em. AWS Control Tower Esse padrão segue as AWS melhores práticas e garante que o processo de implantação não seja apenas eficiente, mas também esteja alinhado aos padrões de segurança e governança, para oferecer uma maneira abrangente, segura e eficiente de implantar o AFT em seu AWS ambiente.

Para obter mais informações sobre o AFT, consulte a AWS Control Tower documentação.

Pré-requisitos e limitações

Pré-requisitos

- Um ambiente básico de AWS várias contas com, no mínimo, as seguintes contas: conta de gerenciamento, conta de arquivamento de registros, conta de auditoria e uma conta adicional para gerenciamento de AFT.

- Um AWS Control Tower ambiente estabelecido. A conta de gerenciamento deve ser configurada adequadamente, pois o CloudFormation modelo será implantado nela.
- As permissões necessárias na conta AWS de gerenciamento. Você precisará de permissões suficientes para criar e gerenciar recursos, como buckets, AWS Lambda funções, funções AWS Identity and Access Management (IAM) e AWS CodePipeline projetos do S3.
- Familiaridade com o Terraform. Compreender os principais conceitos e o fluxo de trabalho do Terraform é importante porque a implantação envolve a geração e o gerenciamento das configurações do Terraform.

Limitações

- Esteja ciente das cotas AWS de recursos em sua conta. A implantação pode criar vários recursos, e encontrar cotas de serviço pode impedir o processo de implantação.
- O modelo foi desenvolvido para versões específicas do Terraform e. Serviços da AWS A atualização ou alteração de versões pode exigir modificações no modelo.
- O modelo não oferece suporte a serviços de sistema de controle de versão (VCS) autogerenciado, como GitHub o Enterprise.

Versões do produto

- Terraform versão 1.6.6 ou posterior
- AFT versão 1.11 ou posterior

Arquitetura

Pilha de tecnologias de destino

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- IAM
- AWS Lambda

- Amazon S3

Arquitetura de destino

O diagrama a seguir ilustra a implementação discutida nesse padrão.

O fluxo de trabalho consiste em três tarefas principais: criar os recursos, gerar o conteúdo e executar o pipeline.

Criando os recursos

O CloudFormation modelo fornecido com esse padrão cria e configura todos os recursos necessários, dependendo dos parâmetros selecionados ao implantar o modelo. No mínimo, o modelo cria os seguintes recursos:

- Um CodePipeline pipeline para implementar o AFT
- Um bucket S3 para armazenar o arquivo de estado do Terraform associado à implementação do AFT
- Dois CodeBuild projetos para implementar o plano do Terraform e aplicar comandos em diferentes estágios do pipeline
- Funções CodeBuild e CodePipeline serviços do IAM
- Um segundo bucket S3 para armazenar artefatos de tempo de execução do pipeline

Dependendo do provedor de VCS selecionado (CodeCommit ou do VCS externo), o modelo cria os seguintes recursos.

- Para CodeCommit:
  - Um CodeCommit repositório para armazenar o código de bootstrap do AFT Terraform
  - Uma EventBridge regra para capturar alterações no CodeCommit repositório na ramificação `main`
  - Outra função do IAM para a EventBridge regra
- Para qualquer outro provedor externo de VCS, como GitHub:
  - Uma Conexões de código da AWS conexão

Além disso, quando você seleciona CodeCommit como provedor de VCS, se você definir o `Generate AFT Files` parâmetro como`true`, o modelo cria esses recursos adicionais para gerar o conteúdo:

- Um bucket S3 para armazenar o conteúdo gerado e ser usado como fonte do CodeCommit repositório
- Uma função Lambda para processar os parâmetros fornecidos e gerar o conteúdo apropriado
- Uma função do IAM para executar a função Lambda
- Um recurso CloudFormation personalizado que executa a função Lambda quando o modelo é implantado

Gerando o conteúdo

Para gerar os arquivos de bootstrap AFT e seu conteúdo, a solução usa uma função Lambda e um bucket S3. A função cria uma pasta no bucket e, em seguida, cria dois arquivos dentro da pasta: `main.tf` `backend.tf` e. A função também processa os CloudFormation parâmetros fornecidos e preenche esses arquivos com código predefinido, substituindo os respectivos valores dos parâmetros.

Para visualizar o código usado como modelo para gerar os arquivos, consulte o GitHub repositório da solução. Basicamente, os arquivos são gerados da seguinte forma.

main.tf

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory?
ref=<aft_version>"

  # Required variables
  ct_management_account_id  = "<ct_management_account_id>"
  log_archive_account_id    = "<log_archive_account_id>"
  audit_account_id          = "<audit_account_id>"
  aft_management_account_id = "<aft_management_account_id>"
  ct_home_region            = "<ct_home_region>"

  # Optional variables
  tf_backend_secondary_region = "<tf_backend_secondary_region>"
  aft_metrics_reporting       = "<false|true>"
```

```
  # AFT Feature flags
  aft_feature_cloudtrail_data_events      = "<false|true>"
  aft_feature_enterprise_support          = "<false|true>"
  aft_feature_delete_default_vpcs_enabled = "<false|true>"

  # Terraform variables
  terraform_version      = "<terraform_version>"
  terraform_distribution = "<terraform_distribution>"

  # VCS variables (if you have chosen an external VCS)
  vcs_provider                                = "<github|githubenterprise|gitlab|
gitlabselfmanaged|bitbucket>"
  account_request_repo_name                   = "<org-name>/aft-account-request"
  account_customizations_repo_name            = "<org-name>/aft-account-
customizations"
  account_provisioning_customizations_repo_name = "<org-name>/aft-account-provisioning-
customizations"
  global_customizations_repo_name             = "<org-name>/aft-global-
customizations"

}
```

backend.tf

```
terraform {
  backend "s3" {
    region = "<aft-main-region>"
    bucket = "<s3-bucket-name>"
    key    = "aft-setup.tfstate"
  }
}
```

Durante a criação do CodeCommit repositório, se você definir o `Generate AFT Files` parâmetro como`true`, o modelo usará o bucket do S3 com o conteúdo gerado como a origem da `main` ramificação para preencher automaticamente o repositório.

Executando o pipeline

Depois que os recursos foram criados e os arquivos de bootstrap foram configurados, o pipeline é executado. O primeiro estágio (Fonte) busca o código-fonte da ramificação principal do repositório e o segundo estágio (Construção) executa o comando de plano do Terraform e gera os resultados a serem revisados. No terceiro estágio (Aprovação), o pipeline aguarda uma ação manual para aprovar

ou rejeitar o último estágio (Implantação). No último estágio, o pipeline executa o `apply` comando do Terraform usando o resultado do comando anterior do Terraform como `plan` entrada. Finalmente, uma função entre contas e as permissões na conta de gerenciamento são usadas para criar os recursos do AFT na conta de gerenciamento do AFT.

> **Note**
>
> Se você selecionar um provedor de VCS externo, precisará autorizar a conexão com suas credenciais de provedor de VCS. Para concluir a configuração, siga as etapas em Atualizar uma conexão pendente na documentação do console do AWS Developer Tools.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los em todo o seu ciclo de vida em todas Contas da AWS as regiões.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeCommité um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada sem precisar gerenciar seu próprio sistema de controle de código-fonte.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- Conexões de código da AWSpermite que AWS recursos e serviços, como CodePipeline, se conectem a repositórios de código externos, como GitHub.
- AWS Lambdaé um serviço de computação que executa seu código em resposta a eventos e gerencia automaticamente os recursos de computação, fornecendo uma maneira rápida de criar um aplicativo moderno e sem servidor para produção.
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS

Outras ferramentas

- O Terraform é uma ferramenta de infraestrutura como código (IaC) que permite criar, alterar e criar versões da infraestrutura com segurança e eficiência. Isso inclui componentes de baixo nível, como instâncias de computação, armazenamento e rede, e componentes de alto nível, como entradas de DNS e recursos SaaS.
- Python é uma linguagem de programação poderosa e fácil de aprender. Ele tem estruturas de dados eficientes de alto nível e fornece uma abordagem simples, mas eficaz, para a programação orientada a objetos.

Repositório de código

O código desse padrão está disponível no repositório do pipeline de bootstrap do GitHub AFT.

Para o repositório oficial do AFT, consulte AWS Control Tower Account Factory for Terraform em. GitHub

Práticas recomendadas

Ao implantar o AFT usando o CloudFormation modelo fornecido, recomendamos que você siga as melhores práticas para ajudar a garantir uma implementação segura, eficiente e bem-sucedida. As principais diretrizes e recomendações para implementar e operar o AFT incluem o seguinte.

- Revisão completa dos parâmetros: analise e compreenda cuidadosamente cada parâmetro no CloudFormation modelo. A configuração precisa dos parâmetros é crucial para a configuração e o funcionamento corretos do AFT.
- Atualizações regulares do modelo: mantenha o modelo atualizado com os AWS recursos mais recentes e as versões do Terraform. As atualizações regulares ajudam você a aproveitar as novas funcionalidades e manter a segurança.
- Controle de versão: fixe sua versão do módulo AFT e use uma implantação AFT separada para testar, se possível.
- Escopo: use o AFT somente para implantar proteções e personalizações de infraestrutura. Não o use para implantar seu aplicativo.
- Linting e validação: o pipeline AFT requer uma configuração do Terraform limitada e validada. Execute o lint, valide e teste antes de enviar a configuração para os repositórios AFT.
- Módulos do Terraform: crie código reutilizável do Terraform como módulos e sempre especifique as versões do Terraform e do AWS provedor de acordo com os requisitos da sua organização.

Épicos

Configurar e configurar o AWS ambiente

Tarefa	Descrição	Habilidades necessárias
Prepare o AWS Control Tower ambiente.	Instale e configure AWS Control Tower em seu AWS ambiente para garantir gerenciamento e governanç a centralizados para seu Contas da AWS. Para obter mais informações, consulte Introdução AWS Control Tower na AWS Control Tower documentação.	Administrador de nuvem
Inicie a conta de gerenciam ento do AFT.	Use o AWS Control Tower Account Factory para lançar uma nova Conta da AWS para servir como sua conta de gerenciamento da AFT. Para obter mais informações, consulte Provisionar contas com o AWS Service Catalog Account Factory na AWS Control Tower documentação.	Administrador de nuvem

Implante o CloudFormation modelo na conta de gerenciamento

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo.	Neste épico, você implanta o CloudFormation modelo fornecido com esta solução para configurar o pipeline de bootstrap do AFT em sua	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	conta AWS de gerenciamento. O pipeline implanta a solução AFT na conta de gerenciamento da AFT que você configurou no épico anterior. Etapa 1: abrir o AWS CloudFormation console • Faça login no AWS Management Console e abra o AWS CloudFormation console. Verifique se você está operando na região AWS Control Tower principal correta. Etapa 2: criar uma nova pilha 1. Escolha criar uma nova pilha. 2. Selecione a opção de carregar um arquivo de modelo e carregar o CloudFormation modelo fornecido com esse padrão. Etapa 3: configurar os parâmetros da pilha • `VCS Provider`: selecione o provedor do sistema de controle de versão (VCS) a ser usado. Você pode	

Tarefa	Descrição	Habilidades necessárias
	selecionar um VCS externo GitHub, como, ou usar CodeCommit se sua conta tiver permissão para usar o serviço. • `Repository Name` : especifique o nome do repositório para armazenar o módulo de bootstrap AFT. Para provedores externos de VCS, use o caminho completo, incluindo o nome da organização (por exemplo,`my-github-org/my-repo`). • `Branch Name`: especifique a ramificação do repositório de origem. • `CodeBuild Docker Image`: escolha o arquivo a ser usado como imagem base do CodeBuild Docker. • Se você definir o provedor VCS para uma opção diferente de CodeCommit, vá para a etapa 8.	
	Etapa 4: decidir sobre a geração de arquivos • Se você selecionou CodeCommit como seu provedor de VCS, você pode usar o `Generate`	

Tarefa	Descrição	Habilidades necessárias
	`AFT Files` parâmetro para controlar a geração de arquivos de implantação padrão do AFT. Defina esse parâmetro como: • `true`para criar e armazenar automatic amente arquivos de implantação do AFT no repositório especificado. • `false`se você quiser lidar manualmente com a criação do arquivo ou se já tiver os arquivos no lugar. • Se você selecionou`false`, vá para a etapa 8; caso contrário, siga primeiro as etapas 5 a 7. Etapa 5: preencher os AWS Control Tower detalhes da conta AFT • Se você definir o `Generate AFT Files` parâmetro como`true`, forneça as seguintes AWS Control Tower informações específicas da conta AFT. • `Log Archive Account ID`: O ID do ID da conta do Log Archive em AWS Control Tower.	

Tarefa	Descrição	Habilidades necessárias
	• `Audit Account ID`: O ID da conta de auditoria em AWS Control Tower. • `AFT Management Account ID`: O ID da conta de gerenciamento da AFT que você criou no primeiro épico. • `AFT Main RegioneAFT Secondary Region`: O principal e o secundári o Regiões da AWS para implantação do AFT. Etapa 6: Configurar as opções do AFT • Configure relatórios de métricas: • `AFT Enable Metrics Reporting` : Ative ou desative os relatórios de métricas do AFT. Para obter mais informaçõ es, consulte Métricas operacionais na AWS Control Tower documenta ção. • Defina as opções do recurso AFT: • `Enable AFT CloudTrail Data`	

Tarefa	Descrição	Habilidades necessárias
	`Events`: Habilite eventos CloudTrail de dados em todas as contas gerenciadas do AFT. Para obter mais informações, consulte eventos de AWS CloudTrail dados na AWS Control Tower documentação. • `Enable AFT Enterprise Support` : Habilite o Enterprise Support em todas as contas gerenciadas do AFT. Para obter mais informações, consulte o plano AWS Enterprise Support na AWS Control Tower documentação. • `Enable AFT Delete Default VPC`: Exclua tudo somente VPCs na conta de gerenciamento do AFT. Para obter mais informações, consulte Excluir a VPC AWS padrão na AWS Control Tower documentação. Etapa 7: especificar versões • `AFT Terraform Version`: Escolha a versão	

Tarefa	Descrição	Habilidades necessárias
	do Terraform para usar em pipelines AFT. • `AFT Version`: defina a versão do AFT para implantação. Mantenha a configuração padrão (`latest`) para usar a versão mais atual do AFT. Etapa 8: revisar e criar a pilha • Revise todos os parâmetros e configurações. Se tudo estiver em ordem, continue criando a pilha. Etapa 9: Monitorar a criação da pilha • AWS CloudFormation provisiona e configura os recursos que você definiu. Monitore o processo de criação da pilha no CloudFormation console. Esse processo pode levar alguns minutos. Etapa 10: Verificar a implantação • Quando o status da pilha mostrar CREATE_COMPLETE, verifique se todos	

Tarefa	Descrição	Habilidades necessárias
	os recursos foram criados corretamente. • Na seção Saídas, observe o `TerraformBackendBucketName` valor.	

Preencha e valide o repositório e o pipeline de bootstrap do AFT

Tarefa	Descrição	Habilidades necessárias
Opção 1: Preencher o repositório de bootstrap AFT para um VCS externo.	Se você definir o provedor de VCS como um VCS externo (não para CodeCommit), siga estas etapas. (Opcional) Depois de implantar o CloudFormation modelo, você pode preencher ou validar o conteúdo no repositório de bootstrap AFT recém-criado e testar se o pipeline foi executado com êxito. Etapa 1: atualizar a conexão 1. No CodePipeline console, no painel de navegação , escolha Configurações, Conexões. 2. Selecione a `aft-vcs-connection` conexão. Deveria estar em `Pending` status.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	3. Escolha Atualizar conexão pendente e siga as instruções em Atualizar uma conexão pendente na documentação do console do Developer Tools. 4. Quando a conexão estiver em `Available` status, vá para a próxima etapa. Etapa 2: preencher o repositório 1. Use suas credenciais externas do VCS para clonar o repositório que você especificou no modelo em sua máquina local. Se você manteve o nome padrão, o repositório será chamado`aft-setup` . 2. No repositório, crie uma pasta chamada `terraform` com dois arquivos vazios dentro dela: `backend.tf` e. `main.tf` 3. Abra o `backend.tf` arquivo e adicione este trecho de código: `terraform { backend "s3" { region = "<aft-main-region>"`	

Tarefa	Descrição	Habilidades necessárias

	<pre> bucket = "<s3-bucket-name>"
	    key = "aft-setup"
	  }
	}</pre>
	No arquivo:
	• `<aft-main-region>` Substitua pela região AFT principal. Isso deve corresponder à região AWS Control Tower principal.
	• `<s3-bucket-name>` Substitua pelo nome do bucket de back-end do Terraform. Você pode encontrar isso na `TerraformBackendBucketName` saída gerada pelo CloudFormation modelo que você implantou anteriormente.
	4. Abra o `main.tf` arquivo e use um dos exemplos disponíveis no repositório AFT para implantar o AFT. Por exemplo, você pode trabalhar com seu provedor de VCS preferido (CodeCommit GitHub, ou Bitbucket) ou personalizar o AFT VPC. Para obter mais opções de entrada	

Tarefa	Descrição	Habilidades necessárias
	AFT, consulte o arquivo README no repositório AFT. Etapa 2: confirme e promova suas alterações • Depois de criar e preencher a pasta e os arquivos, confirme suas alterações e faça o upload do código no repositório. O pipeline é iniciado automaticamente, percorre os estágios de origem e criação e, em seguida, aguarda uma ação de aprovação antes do estágio de implantação.	

Tarefa	Descrição	Habilidades necessárias
Opção 2: Preencher o repositório AFT bootstrap para. CodeCommit	Se você definir o provedor VCS como CodeCommit, siga estas etapas. (Opcional) Depois de implantar o CloudFormation modelo, você pode preencher ou validar o conteúdo no repositório de bootstrap AFT recém-criado e testar se o pipeline foi executado com êxito. Se você definir o `Generate AFT Files` parâmetro como`true`, vá para a próxima história (validando o pipeline). Etapa 1: preencher o repositór io 1. Abra o AWS CodeCommi t console e selecione o repositório recém-cri ado. Se você manteve o nome padrão, o nome do repositório deveria ser`aft-setup` . 2. Clone o repositório em sua máquina local usando SSH, HTTPS ou HTTPS (GRC) e abra-o em um editor. 3. Crie uma pasta chamada `terraform` e dois	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	arquivos vazios dentro dela: `backend.tf` `main.tf` e. 4. Abra o `backend.tf` arquivo e adicione este trecho de código: `terraform { backend "s3" { region = "<aft-main-region>" bucket = "<s3-bucket-name>" key = "aft-setup" } }` No arquivo: • `<aft-main-region>`Substitua pela região AFT principal. Isso deve corresponder à região AWS Control Tower principal. • `<s3-bucket-name>`Substitua pelo nome do bucket de back-end do Terraform. Você pode encontrar isso na `TerraformBackendBucketName` saída gerada pelo CloudFormation modelo que você implantou anteriormente.	

Tarefa	Descrição	Habilidades necessárias
	5. Abra o `main.tf` arquivo e use um dos exemplos disponíveis no repositório AFT para implantar o AFT. Por exemplo, você pode trabalhar com seu provedor de sistema de controle de versão (VCS) preferido (CodeCommit GitHub, ou Bitbucket) ou personalizar o AFT VPC. Para obter mais opções de entrada AFT, consulte o arquivo README no repositório AFT. Etapa 2: confirme e promova suas alterações • Depois de criar e preencher a pasta e os arquivos, confirme suas alterações e faça o upload do código no repositório. O pipeline é iniciado automaticamente, percorre os estágios de origem e criação e, em seguida, aguarda uma ação de aprovação antes do estágio de implantação.	

Tarefa	Descrição	Habilidades necessárias
Valide o pipeline de bootstrap do AFT.	Etapa 1: Visualizar o pipeline • Abra o CodePipeline console e verifique se o `aft-bootstrap-pipeline` pipeline foi iniciado com sucesso. Ele deve estar executando um plano do Terraform ou aguardando uma ação de aprovação manual. Etapa 2: Aprovar os resultados do plano Terraform • Você pode revisar os resultados do plano do Terraform examinando os registros de execução do estágio de construção e, em seguida, aprovar ou rejeitar a execução no estágio de aprovação. Se você aprovar, o pipeline começará a implantar recursos do AFT na conta de gerenciamento do AFT fornecida. Etapa 3: Aguarde a implantação • Aguarde até que o pipeline seja executado com sucesso. Isso deve levar	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	cerca de 30 minutos. Qualquer falha que você possa encontrar geralment e é causada por cotas de API. Nesses casos, você pode executar novamente o pipeline para continuar a implantação. Etapa 4: verificar os recursos criados • Acesse a conta de gerenciamento do AFT e confirme se os recursos foram criados.	

Solução de problemas

Problema	Solução
A função Lambda personalizada incluída no CloudFormation modelo falha durante a implantação.	Verifique os CloudWatch registros da Amazon para a função Lambda para identificar o erro. Os registros fornecem informações detalhada s e podem ajudar a identificar o problema específico. Confirme se a função Lambda tem as permissões necessárias e se as variáveis de ambiente foram definidas corretamente.
Você encontra falhas na criação ou no gerenciamento de recursos causadas por permissões inadequadas.	Analise as funções e políticas do IAM que estão associadas à função Lambda e outros serviços envolvidos na implantação. CodeBuild Confirme se eles têm as permissões necessári as. Se houver problemas de permissão, ajuste

Problema	Solução
	as políticas do IAM para conceder o acesso necessário.
Você está usando uma versão desatualizada do CloudFormation modelo com versões mais recentes Serviços da AWS ou do Terraform.	Atualize regularmente o CloudFormation modelo para ser compatível com as versões mais recentes AWS e do Terraform. Verifique as notas de lançamento ou a documenta ção para ver se há alterações ou requisitos específicos da versão.
Você atinge as AWS service (Serviço da AWS) cotas durante a implantação.	Antes de implantar o pipeline, verifique as AWS service (Serviço da AWS) cotas de recursos como buckets S3, funções do IAM e funções Lambda. A solicitação aumenta, se necessári o. Para obter mais informações, consulte AWS service (Serviço da AWS) as cotas no AWS site.
Você encontra erros devido a parâmetros de entrada incorretos no CloudFormation modelo.	Verifique novamente todos os parâmetros de entrada em busca de erros de digitação ou valores incorretos. Confirme se os identific adores de recursos, como nomes de conta IDs e região, estão corretos.

Recursos relacionados

Para implementar esse padrão com sucesso, revise os recursos a seguir. Esses recursos fornecem informações e orientações adicionais que podem ser inestimáveis na configuração e gerenciamento do AFT usando AWS CloudFormation.

AWSdocumentação:

- AWS Control Tower O Guia do usuário oferece informações detalhadas sobre configuração e gerenciamento AWS Control Tower.
- AWS CloudFormation a documentação fornece informações sobre CloudFormation modelos, pilhas e gerenciamento de recursos.

Políticas e melhores práticas do IAM:

- As melhores práticas de segurança no IAM explicam como ajudar a proteger AWS recursos usando funções e políticas do IAM.

Terraform em AWS:

- A documentação do Terraform AWS Provider fornece informações abrangentes sobre como usar o Terraform com. AWS

AWS service (Serviço da AWS) cotas:

- AWS service (Serviço da AWS) as cotas fornecem informações sobre como visualizar as AWS service (Serviço da AWS) cotas e como solicitar aumentos.

Gerencie produtos do AWS Service Catalog em várias contas e regiões da AWS

Criado por Ram Kandaswamy (AWS)

Resumo

O Amazon Web Services (AWS) Service Catalog simplifica e acelera a governança e a distribuição de modelos de infraestrutura como código (IaC) para empresas. Você usa CloudFormation modelos da AWS para definir uma coleção de recursos da AWS (pilhas) necessários para um produto. A AWS CloudFormation StackSets estende essa funcionalidade ao permitir que você crie, atualize ou exclua pilhas em várias contas e regiões da AWS com uma única operação.

Os administradores do AWS Service Catalog criam produtos usando CloudFormation modelos criados por desenvolvedores e os publicam. Esses produtos são então associados a um portfólio e as restrições são aplicadas à governança. Para disponibilizar seus produtos para usuários em outras contas ou unidades organizacionais da AWS (OUs), você normalmente compartilha seu portfólio com eles. Esse padrão descreve uma abordagem alternativa para gerenciar as ofertas de produtos do AWS Service Catalog com base na AWS CloudFormation StackSets. Em vez de compartilhar portfólios, você usa restrições de conjuntos de pilhas para definir regiões e contas da AWS nas quais seu produto pode ser implantado e usado. Ao usar essa abordagem, você pode provisionar seus produtos do AWS Service Catalog em várias contas e regiões da AWS e gerenciá-los a partir de um local central, ao mesmo tempo em que atende aos requisitos de governança. OUs

Benefícios dessa abordagem:

- O produto é provisionado e gerenciado a partir da conta primária e não é compartilhado com outras contas.
- Essa abordagem fornece uma visão consolidada de todos os produtos provisionados (pilhas) baseados em um produto específico.
- A configuração com o AWS Service Management Connector é mais fácil, pois ela tem como destino apenas uma conta.
- É mais fácil consultar e usar produtos do AWS Service Catalog.

Pré-requisitos e limitações

Pré-requisitos

- CloudFormation Modelos da AWS para IaC e controle de versão
- Configuração de várias contas e AWS Service Catalog para provisionamento e gerenciamento de recursos da AWS

Limitações

- Essa abordagem usa a AWS CloudFormation StackSets e as limitações da StackSets aplicação:
  - StackSets não oferece suporte à implantação CloudFormation de modelos por meio de macros. Se você estiver usando uma macro para pré-processar o modelo, não poderá usar uma implantação StackSets baseada.
  - StackSets fornece a capacidade de desassociar uma pilha do conjunto de pilhas, para que você possa direcionar uma pilha específica para corrigir um problema. No entanto, uma pilha desassociada não pode ser associada novamente ao conjunto de pilhas.
- O AWS Service Catalog gera StackSet nomes automaticamente. A personalização não é compatível no momento.

Arquitetura

Arquitetura de destino

1. O usuário cria um CloudFormation modelo da AWS para provisionar recursos da AWS, no formato JSON ou YAML.
2. O CloudFormation modelo cria um produto no AWS Service Catalog, que é adicionado a um portfólio.
3. O usuário cria um produto provisionado, que cria CloudFormation pilhas nas contas de destino.
4. Cada pilha provisiona os recursos especificados nos CloudFormation modelos.

Ferramentas

Serviços da AWS

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Service Catalog ajuda você a gerenciar de modo centralizado os catálogos de serviços de TI aprovados para a AWS. Os usuários finais podem implantar rapidamente somente os serviços de TI aprovados de que precisam, seguindo as restrições definidas pela organização.

Épicos

Provisione produtos entre contas

Tarefa	Descrição	Habilidades necessárias
Crie um portfólio.	Um portfólio é um contêiner que inclui um ou mais produtos agrupados com base em critérios específicos. Usar um portfólio para seus produtos ajuda você a aplicar restrições comuns em todo o seu conjunto de produtos. Para criar um portfólio, siga as instruções na documenta ção do AWS Service Catalog. Se você estiver usando a AWS CLI, veja um exemplo de comando: `aws servicecatalog create-portfolio --provider-name my-provider --display-name my-portfolio`	AWS Service Catalog, IAM

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte a documentação da AWS CLI.	
Crie um CloudFormation modelo.	Crie um CloudFormation modelo que descreva os recursos. Os valores das propriedades do recurso devem ser parametrizados quando aplicável.	AWS CloudFormation, JSON/YAML

Tarefa	Descrição	Habilidades necessárias
Crie um produto com informações sobre a versão.	O CloudFormation modelo se torna um produto quando você o publica no AWS Service Catalog. Forneça valores para os parâmetros opcionais de detalhes da versão, como título e descrição da versão; isso será útil para consultar o produto posteriormente. Para criar um produto, siga as instruções na documentação do AWS Service Catalog. Um exemplo de comando se você estiver usando a AWS CLI: `aws servicecatalog create-product --cli-input-json file://create-product-input.json` onde `create-product-input.json` está o arquivo que passa os parâmetros do produto. Para obter um exemplo desse arquivo, consulte a seção Informações adicionais. Para obter mais informações, consulte a documentação da AWS CLI.	AWS Service Catalog

Tarefa	Descrição	Habilidades necessárias
Aplique restrições.	Aplique restrições de conjunto de pilhas ao portfólio para configurar opções de implantação de produtos, como várias contas, regiões e permissões da AWS. Para obter instruções, consulte a documentação do AWS Service Catalog.	AWS Service Catalog
Adicione permissão.	Conceder permissões para usuários para que eles possam lançar os produtos no portfólio. Para obter as instruções do console, consulte a documentação do AWS Service Catalog. Se você estiver usando a AWS CLI, veja um exemplo de comando: `aws servicecatalog associate-principal-with-portfolio \ --portfolio-id port-2s6abcdefwdh4 \ --principal-arn arn:aws:iam::444455556666:role/Admin \ --principal-type IAM` Para obter mais informações, consulte a documentação da AWS CLI.	AWS Service Catalog, IAM

Tarefa	Descrição	Habilidades necessárias
Provisione o produto.	Um produto provisionado é uma instância de um produto com recursos. O provision amento de um produto com base em um CloudFormation modelo inicia uma CloudForm ation pilha e seus recursos subjacentes. Provisione o produto segmentando as regiões e contas aplicáveis da AWS, com base nas restrições do conjunto de pilhas. Na AWS CLI, veja um exemplo de comando: `aws servicecatalog provision-product \ --product-id prod-abcdfz3syn2rg \ --provisioning-artifact-id pa-abc347pcsccfm \ --provisioned-product-name "mytestppname3"` Para obter mais informações, consulte a documentação da AWS CLI.	AWS Service Catalog

Recursos relacionados

Referências

- Visão geral do AWS Service Catalog
- Usando a AWS CloudFormation StackSets

Tutoriais e vídeos

- AWS re:Invent 2019: automatize tudo: opções e melhores práticas (vídeo)

Mais informações

Quando você usa o `create-product` comando, o `cli-input-json` parâmetro aponta para um arquivo que especifica informações como proprietário do produto, e-mail de suporte e detalhes do CloudFormation modelo. Veja a seguir um exemplo desse arquivo:

```
{
   "Owner": "Test admin",
      "SupportDescription": "Testing",
         "Name": "SNS",
            "SupportEmail": "example@example.com",
            "ProductType": "CLOUD_FORMATION_TEMPLATE",
               "AcceptLanguage": "en",
                  "ProvisioningArtifactParameters": {
                     "Description": "SNS product",
                        "DisableTemplateValidation": true,
                           "Info": {
                              "LoadTemplateFromURL": "<url>"
                     },
                           "Name": "version 1"
}
```

Migre uma conta membro da AWS do AWS Organizations para o AWS Control Tower

Criado por Rodolfo Jr. Cerrada (AWS)

Resumo

Esse padrão descreve como migrar uma conta da Amazon Web Services (AWS) do AWS Organizations, onde é uma conta membro governada por uma conta de gerenciamento, para o AWS Control Tower. Ao cadastrar a conta no AWS Control Tower, você pode aproveitar as barreiras de proteção e os atributos preventivos e de detetive que simplificam a governança da sua conta. Talvez você também queira migrar a sua conta de membro, caso sua conta de gerenciamento do AWS Organizations tenha sido comprometida e queira transferir as contas dos membros para uma nova organização que seja governada pela AWS Control Tower.

O AWS Control Tower fornece uma estrutura que combina e integra os recursos de vários outros serviços da AWS, incluindo o AWS Organizations, e garante conformidade e governança consistentes em todo o seu ambiente de várias contas. Com o AWS Control Tower, você pode seguir um conjunto de regras e definições prescritas que ampliam as capacidades do AWS Organizations. Por exemplo, você pode usar barreiras de proteção para garantir que os registros de segurança e as permissões necessárias de acesso entre contas sejam criados e não alterados.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Configuração da AWS Control Tower em sua organização de destino no AWS Organizations (para obter instruções, consulte Configuração na documentação da AWS Control Tower)
- Credenciais de administrador do AWS Control Tower (membro do AWSControlTowerAdminsgrupo)
- Credenciais de administrador para a conta de origem da AWS

Limitações

- A conta de gerenciamento de origem no AWS Organizations deve ser diferente da conta de gerenciamento de destino no AWS Control Tower.

Versões do produto

- AWS Control Tower versão 2.3 (fevereiro de 2020) ou superior (veja as notas de lançamento)

Arquitetura

O diagrama a seguir ilustra o processo de migração e arquitetura de referência. Esse padrão migra a conta da AWS da organização de origem para uma organização de destino que é governada pela AWS Control Tower.

O processo de inscrição consiste em três etapas:

1. A conta deixa a organização de origem no AWS Organizations.
2. A conta se torna uma conta autônoma. Isso significa que ela não pertence a nenhuma organização, portanto, a governança e o faturamento são gerenciados de forma independente pelos administradores da conta.
3. A organização de destino envia um convite para que a conta participe da organização.
4. A conta independente aceita o convite e se torna membro da organização de destino.
5. A conta foi inscrita no AWS Control Tower e transferida para uma unidade organizacional (OU) registrada. (Recomendamos que você verifique o painel do AWS Control Tower para confirmar a inscrição.) Nesse ponto, todas as barreiras de proteção habilitadas na OU registrada entram em vigor.

Ferramentas

Serviços da AWS

- O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias contas da AWS em uma única entidade (uma organização), que você cria e gerencia centralmente.
- AWS Control Tower integra os recursos de outros serviços, incluindo AWS Organizations, Centro de Identidade do AWS IAM (sucessor do AWS Single Sign-On) e AWS Service Catalog, para ajudar você a aplicar e gerenciar regras de governança para segurança, operações e conformidade em grande escala em todas as suas organizações e contas na Nuvem AWS.

Épicos

Remova a conta membro da organização de origem

Tarefa	Descrição	Habilidades necessárias
Verifique se a conta do membro pode ser executada como uma conta independente.	Confirme se a conta membro que sairá da organização de origem tem as informações necessárias para operar como uma conta independente. Por exemplo, se a conta do membro não tiver informações de cobrança, ela não poderá operar como uma conta independente, porque a AWS usa as informações de pagamento para cobrar por qualquer atividade faturável da AWS que ocorra enquanto a conta não estiver vinculada a uma organização. Normalmente, se você criou a conta do membro usando o console do AWS Organizations, a API ou os comandos da interface de linha de comandos (CLI), as informações exigidas das contas independentes não são coletadas automaticamente. Para adicionar essas informações, faça login na conta e especifique um plano de suporte, informações	Administrador da conta

Tarefa	Descrição	Habilidades necessárias
	de contato e uma forma de pagamento. Para obter mais informaçõ es sobre o que você precisa saber antes de remover uma conta de uma organização, consulte Antes de remover uma conta da organização na documentação do AWS Organizations.	

Tarefa	Descrição	Habilidades necessárias
Remova a conta membro da sua organização de origem.	Siga as instruções na documentação do AWS Organizations para remover uma conta-membro de uma organização. Você pode entrar na conta de gerenciamento da organização e remover a conta do membro, ou entrar na conta do membro e sair da organização. Se não tiver credenciais de administrador para remover ou sair da conta, peça ajuda ao administrador da sua organização. Se a conta do membro não tiver um plano de suporte, informações de contato ou informações de pagamento, você será solicitado a fornecer e verificar essas informações. Quando você deixar a organização, será redirecionado para a página Getting Started (Conceitos básicos) do console do AWS Organizations, onde você pode visualizar convites pendentes para a sua conta para ingressar em outras organizações.	Administrador da conta de gerenciamento ou administrador da conta

Tarefa	Descrição	Habilidades necessárias
	Important Neste momento, sua conta é uma conta independente. Se estiver executando cargas de trabalho que não são cobertas pelo nível gratuito da AWS, você será cobrado de acordo com as informaçõ es de pagamento e faturamento fornecida s para a conta.	
Verifique se a conta-mem bro deixa de fazer parte da organização de origem.	No console do AWS Organizat ions, você não deve mais ver o botão Sair da organizaç ão. Em vez disso, você deve ver convites pendentes, se houver, de outras organizaç ões.	Administrador da conta

Tarefa	Descrição	Habilidades necessárias
Remova os perfis do IAM que concedem acesso à sua conta a partir da organização que você deixou.	Quando você remove a conta da organização de origem, as funções do AWS Identity and Access Management (IAM) criadas pelo AWS Organizations ou pelos administradores não são excluídas automaticamente. Para deseja terminar esse acesso a partir da conta de gerenciamento da organização de origem, exclua manualmente os perfis do IAM. Para obter mais informações, consulte Excluir funções ou perfis de instância na documentação do IAM. Quando uma conta-membro sai de uma organização, todas as tags anexadas à conta são excluídas. Contas autônomas não dão suporte para tags.	Administrador da conta

Convide a conta para se juntar à nova organização com o AWS Control Tower

Tarefa	Descrição	Habilidades necessárias
Faça login no AWS Control Tower.	Faça login no console do AWS Control Tower como administrador. Atualmente, não há uma forma direta de mover uma conta da AWS de uma organização de origem para	Administrador do AWS Control Tower

Tarefa	Descrição	Habilidades necessárias
	uma organização em uma OU que seja governada pela AWS Control Tower. No entanto, você pode estender a governança da AWS Control Tower para uma conta existente da AWS ao inscrevê-la em uma OU que já seja governada pela AWS Control Tower. É por isso que você precisa fazer login no AWS Control Tower para esta etapa.	

Tarefa	Descrição	Habilidades necessárias
Convidar a conta-membro.	1. Faça login no console do AWS Organizations e navegue até a página contas da AWS. 2. Na página Adicionar uma conta da AWS, escolha Convidar uma conta da AWS existente. 3. Preencha as informaçõ es da conta, incluindo o número da conta de 12 dígitos (sem traços) e a descrição e as tags opcionais, e escolha Enviar convite. **Important** Verifique se nenhum aplicativo ou conectivi dade de rede será afetado pela transferê ncia da conta. Essa ação envia um e-mail de convite com um link para a conta-membro. Quando o administrador da conta segue o link e aceita o convite, a conta do membro aparece na página de contas da AWS. Para obter mais informações, consulte Convidar uma conta	Administrador do AWS Control Tower

Tarefa	Descrição	Habilidades necessárias
	da AWS para participar de sua organização na documentação da AWS Organizations.	
Teste aplicativos e conectividade.	Quando a conta do membro é registrada na nova organização, ela aparece na OU dentro de uma raiz. Ele também aparece no console do AWS Control Tower, marcado como não inscrito em contas, porque ainda não foi inscrito na OU registrada no AWS Control Tower. Verifique o seguinte: • Verifique o painel do AWS Control Tower para ver se há alguma violação da barreira de proteção. • Verifique a conectividade da rede (VPN ou AWS Direct Connect) para garantir que ela não tenha sido afetada pela transferência. • (Proprietários do aplicativo) Teste os aplicativos associados a essa conta para verificar se eles são executados conforme o esperado e se as dependências não foram afetadas pela transferência da conta.	Administrador do AWS Control Tower, administrador da conta do membro, proprietários de aplicativos

Prepare a conta para inscrição

Tarefa	Descrição	Habilidades necessárias
Revise as barreiras de proteção e corrija quaisquer violações.	Revise as barreiras de proteção definidas na UO de destino, especialmente as grades de proteção preventiv as, e corrija quaisquer violações. Várias barreiras de proteção preventivas obrigatórias são habilitadas por padrão quando você configura sua zona de pouso do AWS Control Tower. Elas não podem ser desabilit adas. Você deve revisar essas barreiras de proteção obrigatórias e corrigir a conta do membro (manualmente ou usando um script) antes de cadastrar a conta. **Note** As proteções preventiv as mantêm as contas registradas do AWS Control Tower em conformidade e evitam violações de políticas. Qualquer violação das barreiras de proteção preventivas pode afetar a inscrição. Detetives que violam	Administrador do AWS Control Tower, administrador da conta do membro

Tarefa	Descrição	Habilidades necessárias
	a barreira de proteção aparecem no painel do AWS Control Tower, se detectadas, após o cadastro bem-suced ido. Eles não afetam o processo de inscrição . Para obter mais informações, consulte Barreiras de proteção no AWS Control Tower na documenta ção da AWS.	
Verifique se há problemas de conectividade depois de corrigir as violações da barreira de proteção.	Em alguns casos, você pode ter que fechar portas específic as ou desativar serviços para corrigir violações da barreira de proteção. Certifique-se de que os aplicativos que usam essas portas e serviços sejam corrigidos antes de registrar a conta.	Proprietário do aplicativo

Inscreva a conta no AWS Control Tower

Tarefa	Descrição	Habilidades necessárias
Faça login no console do AWS Control Tower.	Use credenciais de login que tenham permissões administrativas para o AWS Control Tower. Não use as credenciais do usuário raiz (conta de gerenciamento) para	Administrador do AWS Control Tower

Tarefa	Descrição	Habilidades necessárias
	cadastrar uma conta do AWS Organizations. Isso exibirá uma mensagem de erro.	
Registre a conta.	1. Na página Account Factory no AWS Control Tower, escolha Cadastrar conta. 2. Preencha os detalhes, incluindo o endereço de e-mail associado à conta que você deseja inscrever , o nome de exibição que aparecerá no AWS Control Tower, o endereço de e-mail do IAM Identity Center, o nome e o sobrenome do proprietário da conta e a OU na qual você gostaria de inscrever a conta. O endereço de e-mail do IAM Identity Center é o endereço de e-mail de seu usuário preferido. Você pode usar o mesmo endereço de e-mail do e-mail da conta. 3. Escolha Enroll account (Registrar conta). Para obter mais informações, consulte Inscrever uma conta existente na documentação do AWS Control Tower.	Administrador do AWS Control Tower

Verifique a conta após a inscrição

Tarefa	Descrição	Habilidades necessárias
Verifique a conta.	No AWS Control Tower, escolha Contas. A conta que você acabou de cadastrar tem um estado inicial de Inscrição. Quando a inscrição é concluída, seu estado muda para Inscrito.	Administrador do AWS Control Tower, administrador da conta do membro
Verifique se há violações da barreira de proteção.	As barreiras de proteção definidas na OU se aplicarão automaticamente à conta do membro inscrito. Monitore o painel do AWS Control Tower em busca de violações e corrija-as adequadamente. Para obter mais informações, consulte Barreiras de proteção no AWS Control Tower na documentação da AWS.	Administrador do AWS Control Tower, administrador da conta do membro

Solução de problemas

Problema	Solução
Você recebe a mensagem de erro: Ocorreu um erro desconhecido. Tente novamente mais tarde ou entre em contato com o AWS Support.	Esse erro ocorre quando você usa credencia is de usuário raiz (conta de gerenciamento) no AWS Control Tower para inscrever uma nova conta. O AWS Service Catalog não pode mapear o portfólio ou o produto Account Factory para o usuário raiz, o que resulta na mensagem de erro. Para corrigir esse erro, use as credenciais de usuário (administrador)

Problema	Solução
	não raiz e com acesso total para registrar a nova conta. Para obter mais informações sobre como atribuir acesso administrativo a um usuário administrativo, consulte os Conceitos básicos na documentação do Centro de Identidade do AWS IAM (sucessor do AWS Single Sign-On).
A página de atividades do AWS Control Tower exibe uma ação Obter desvios catastróficos.	Essa ação reflete uma verificação de desvio do serviço e não indica nenhum problema com a configuração do AWS Control Tower. Nenhuma ação é necessária.

Recursos relacionados

Documentação

- Terminologia e conceitos do AWS Organizations (documentação do AWS Organizations)
- O que é o AWS Control Tower? (Documentação do AWS Control Tower)
- Remover uma conta-membro da sua organização (documentação do AWS Organizations)
- Criação de uma conta de administrador na AWS Control Tower (documentação da AWS Control Tower)

Tutoriais e vídeos

- Workshop sobre a AWS Control Tower (workshop individualizado)
- O que é o AWS Control Tower? (vídeo)
- Provisionamento de usuários no AWS Control Tower (vídeo)
- Habilitar o AWS Control Tower para organizações existentes (vídeo)

Monitore clusters do SAP RHEL Pacemaker usando os serviços da AWS

Criado por Harsh Thoria (AWS), Randy Germann (AWS) e RAVEENDRA Voore (AWS)

Resumo

Esse padrão descreve as etapas para monitorar e configurar alertas para um cluster Red Hat Enterprise Linux (RHEL) Pacemaker para aplicativos SAP e serviços de banco de dados SAP HANA usando a Amazon e o Amazon Simple Notification Service (CloudWatch Amazon SNS).

A configuração permite monitorar recursos de cluster SAP SCS ou ASCS, Enqueue Replication Server (ERS) e SAP HANA quando eles estão em um estado “parado” com a ajuda de fluxos de CloudWatch log, filtros métricos e alarmes. O Amazon SNS envia um e-mail para a infraestrutura ou para a equipe do SAP Basis sobre o status do cluster interrompido.

Você pode criar os AWS recursos para esse padrão usando AWS CloudFormation scripts ou os consoles AWS de serviço. Esse padrão pressupõe que você esteja usando os consoles; ele não fornece CloudFormation scripts nem cobre a implantação de infraestrutura para CloudWatch o Amazon SNS. Os comandos do Pacemaker são usados para definir a configuração de alerta do cluster.

Pré-requisitos e limitações

Pré-requisitos

- Uma AWS conta ativa.
- Amazon SNS configurado para enviar notificações por e-mail ou dispositivos móveis.
- Um cluster SAP ASCS/ERS for ABAP or SCS/ERS para Java e SAP HANA Database RHEL Pacemaker. Para instruções, consulte:
  - Configuração do cluster SAP HANA
  - Configuração do cluster SAP Netweaver ABAP/Java

Limitações

- Atualmente, essa solução funciona para clusters baseados no RHEL versão 7.3 e posteriores baseados no Pacemaker. Ele não foi testado nos sistemas operacionais da SUSE.

Versões do produto

- RHEL 7.3 e versões posteriores

Arquitetura

Pilha de tecnologias de destino

- Agente orientado por eventos de alerta do RHEL Pacemaker
- Nuvem de computação elástica da Amazon (Amazon EC2)
- CloudWatch alarme
- CloudWatch grupo de registros e filtro métrico
- Amazon SNS

Arquitetura de destino

O diagrama a seguir ilustra os componentes e fluxos de trabalho dessa solução.

Automação e escala

- Você pode automatizar a criação de AWS recursos usando CloudFormation scripts. Você também pode usar filtros métricos adicionais para escalar e cobrir vários clusters.

Ferramentas

Serviços da AWS

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.

Ferramentas

- CloudWatch agent (unificado) é uma ferramenta que coleta métricas, registros e rastreamentos em nível de sistema de EC2 instâncias e recupera métricas personalizadas de seus aplicativos.

- O agente de alerta do Pacemaker (para RHEL 7.3 e versões posteriores) é uma ferramenta que inicia uma ação quando há uma alteração, como quando um recurso para ou reinicia, em um cluster do Pacemaker.

Práticas recomendadas

- Para obter as melhores práticas para usar cargas de trabalho SAP em AWS, consulte o SAP Lens for the AWS Well-Architected Framework.
- Considere os custos envolvidos na configuração do CloudWatch monitoramento de clusters SAP HANA. Para obter mais informações, consulte a documentação do CloudWatch .
- Considere usar um pager ou mecanismo de emissão de tíquetes para alertas do Amazon SNS.
- Sempre verifique as versões RHEL de alta disponibilidade (HA) do pacote RPM para PCs, Pacemaker e o AWS agente de vedação.

Épicos

Configuração do Amazon SNS

Tarefa	Descrição	Habilidades necessárias
Criar um tópico do SNS.	1. Faça login no AWS Management Console e abra o console do Amazon SNS em https://console.aws.amazon.com/sns/ v3/ home. 2. No painel do Amazon SNS, em Common actions (Ações comuns), escolha Create Topic (Criar tópico). 3. Na caixa de diálogo Criar novo tópico, em Tipo, escolha Padrão.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	4. Em Nome do tópico, insira um nome para o tópico (por exemplo,`my-topic`). 5. Escolha Criar tópico. Isso cria um tópico do SNS com uma política de recursos que permite publicar notificações. 6. Copie o ARN do tópico (por exemplo,`arn:aws:sns:us-east-1:111122223333:my-topic`). Você usará esse ARN em uma etapa posterior.	

Tarefa	Descrição	Habilidades necessárias
Modifique a política de acesso para o tópico do SNS.	1. No console do Amazon SNS, no painel de navegação, escolha Tópicos e, em seguida, escolha o tópico que você criou. 2. Escolha Editar e vá para a seção Política de acesso. 3. Certifique-se de que a política de acesso CloudWatch inclua um dos diretores de serviço que têm permissão para publicar neste tópico. Por exemplo: `{ "Sid": "Allow AWS CloudWatch to Publish to this SNS topic", "Effect": "Allow", "Principal": { "Service": [ "cloudwatch.amazonaws.com" ] }, "Action": "SNS:Publish", "Resource": "arn:aws:sns:us-east-1:111122223333:my-topic" }`	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	4. Escolha Salvar alterações.	
Inscreva-se no tópico do SNS.	1. No console do Amazon SNS, no painel de navegação, escolha Assinaturas, Criar assinatura. 2. Para ARN do tópico, cole o ARN que você criou na primeira tarefa. 3. Em Protocolo, escolha E-mail. 4. Para Endpoint, insira um endereço de e-mail da pessoa ou equipe responsável pelo cluster do SAP Pacemaker e deve receber notificações. Por exemplo, esse pode ser o endereço de e-mail da lista de distribuição do SAP Basis ou da equipe de infraestrutura. 5. Selecione Criar assinatura. 6. No seu aplicativo de e-mail, abra a mensagem em AWS Notificações e confirme sua assinatura. O navegador da Web exibe uma resposta de confirmação do Amazon SNS.	Administrador de sistemas AWS

Confirme a configuração do cluster

Tarefa	Descrição	Habilidades necessárias
Verifique o status do cluster.	Use o comando pcs status para confirmar se os recursos estão on-line.	Administrador do SAP Basis

Configurar alertas do Pacemaker

Tarefa	Descrição	Habilidades necessárias

Configure o agente de alerta do Pacemaker na instância primária do cluster.	Faça login na EC2 instância no cluster primário e execute os seguintes comandos:
	`install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample`
	`touch /var/lib/pacemaker/alert_file.sh`
	`touch /var/log/pcmk_alert_file.log`
	`chown hacluster:haclient /var/log/pcmk_alert_file.log`
	`chmod 600 /var/log/pcmk_alert_file.log`
	`pcs alert create id=alert_file description="Log events to a file." path=/var/lib/pacemaker/alert_file.sh`
	`pcs alert recipient add alert_file id=my-alert_logfile value=/va`
		Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	`r/log/pcmk_alert_f ile.log`	

Configure o agente de alerta do Pacemaker na instância secundária do cluster.	Faça login na EC2 instância secundária do cluster no cluster secundário e execute os seguintes comandos:
	`install --mode=0755 / usr/share/pacemak er/alerts/alert_fi le.sh.sample`
	`touch /var/lib/ pacemaker/alert_fi le.sh`
	`touch /var/log/ pcmk_alert_file.log`
	`chown hacluster :haclient /var/log/ pcmk_alert_file.log`
	`chmod 600 /var/log/ pcmk_alert_file.log`
		Administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias

Confirme se o recurso de alerta do RHEL foi criado.	Use o comando a seguir para confirmar que o recurso de alerta foi criado:
	`pcs alert`
	A saída do comando ficará assim:
	`[root@xxxxxxx ~]# pcs alert`
	`Alerts:`
	` Alert: alert_file (path=/var/lib/pacemaker/alert_file.sh)`
	`  Description: Log events to a file.`
	`  Recipients:`
	`   Recipient: my-alert_logfile (value=/var/log/pcmk_alert_file.log)`
		Administrador do SAP Basis

Configurar o CloudWatch agente

Tarefa	Descrição	Habilidades necessárias
Instale o CloudWatch agente.	Há várias maneiras de instalar o CloudWatch agente em uma EC2 instância. Para usar a linha de comando: 1. Baixe o pacote do CloudWatch agente:	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	`wget https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-region/redhat/amd64/latest/amazon-cloudwatch-agent.rpm`
	onde `<region>` é Região da AWS onde a EC2 instância está localizada (por exemplo,`us-west-2`).
	2. (Opcional) Verifique a assinatura do pacote. Para obter instruções, consulte Verificação da assinatura do pacote do CloudWatch agente na CloudWatch documentação.
	3. Instale o pacote na primeira instância:
	`sudo rpm -U ./amazon-cloudwatch-agent.rpm`
	4. Repita o procedimento para a instância secundária.
	
	Para obter mais informações, consulte a documentação do CloudWatch .	

Tarefa	Descrição	Habilidades necessárias
Anexe uma função do IAM à EC2 instância.	Para permitir que o CloudWatch agente envie dados das instâncias, você deve anexar a CloudWatchAgentServerRolefunção do IAM a cada instância. Ou você pode adicionar uma política para o CloudWatch agente à sua função atual do IAM. Para obter mais informações, consulte a documentação do CloudWatch .	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Configure o CloudWatch agente para monitorar o arquivo de log do agente de alerta do Pacemaker na instância primária do cluster.	1. Configure a instância primária do cluster executando o comando: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard` 2. Escolha 1 para Linux e, em seguida, selecione as opções para sua estratégia de monitoramento. 3. Para a pergunta “Deseja monitorar qualquer arquivo de log”, escolha Sim e forneça o caminho do arquivo de log do Pacemaker a partir do comando pcs alert. No nosso caso, é `var/log/pcmk_alert_file.log`. 4. Forneça o nome do grupo de registros e do fluxo de registros. Se você não especificar um stream de registros, o ID da AWS instância será usado como padrão. 5. Repita as etapas de 1 a 4 para a instância secundária do cluster.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudWatch agente nas instâncias primárias e secundárias do cluster.	Para iniciar o agente, execute o seguinte comando nas EC2 instâncias dos clusters primário e secundário: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json`	Administrador da AWS

Configurar CloudWatch recursos

Tarefa	Descrição	Habilidades necessárias
Configure grupos de CloudWatch registros.	1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/ 2. No painel de navegação, escolha Grupos de registros, Criar grupo de registros. 3. Insira um nome para o grupo de registros e escolha Criar grupo de registros. O CloudWatch agente transferirá o arquivo de alerta do Pacemaker para o grupo	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	de CloudWatch registros como um fluxo de registros.	

Tarefa	Descrição	Habilidades necessárias
Configure filtros CloudWatch métricos.	Os filtros métricos ajudam você a pesquisar um padrão, como `stop <cluster-resource-name>` nos fluxos de CloudWatch log. Quando esse padrão é identificado, o filtro métrico atualiza uma métrica personalizada. 1. No CloudWatch console, no painel de navegação, escolha Grupos de registros. 2. Escolha o nome do grupo de registros que você criou na tarefa anterior. 3. Escolha Ações, Criar filtro de métrica. 4. Em Padrão de filtro, insira o padrão de filtro a ser usado, como `stop ABC_scs`, para corresponder ao evento de parada de um recurso de cluster do SAP SCS chamado `ABC_scs`. Para obter mais informações, consulte Sintaxe do padrão de filtro na CloudWatch documentação. 5. (Opcional) Para testar seu padrão de filtro, em Test	Administrador da AWS, administrador do SAP Basis

Tarefa	Descrição	Habilidades necessárias
	Pattern (Testar padrão), insira um ou mais eventos de log a serem usados para testar o padrão. Cada evento de log deve ser especificado em uma linha separada, porque as quebras de linha são usadas para separar eventos de log na caixa Mensagens de eventos de log. 6. Escolha Next (Próximo) e digite um nome para o filtro. 7. Em Detalhes da métrica, em Namespace métrica, insira um nome para o CloudWatch namespace em que a métrica será publicada (por exemplo,). `sapcluster_monitoring` Se esse namespace ainda não existir, selecione Criar novo. 8. Em Nome da métrica, insira um nome para a nova métrica (por exemplo `sapcluster_<sid>` , onde `<sid>` está o nome de identificação do sistema SAP). 9. Em Valor métrico, insira 1.	

Tarefa	Descrição	Habilidades necessárias
	Como alternativa, você pode inserir um token como `$size`. Isso increment a a métrica pelo valor do número no campo `size` para cada evento de log que contém um campo `size`. 10 Em Valor padrão, insira 0. 11 Escolha Criar filtro de métrica. Quando o filtro métrico identifica o padrão na etapa 4, ele atualiza o valor da métrica CloudWatch personalizada `sapcluster_abc` para 1. O CloudWatch alarme `SAP-Cluster-QA1-ABC` monitora a métrica `sapcluster_abc` e envia uma notificação de SNS quando o valor da métrica muda para 1. Isso indica que o recurso do cluster foi interrompido e uma ação precisa ser tomada.	

Tarefa	Descrição	Habilidades necessárias
Configure um alarme CloudWatch métrico para a métrica SAP ASCS/SCS e ERS.	Para criar um alarme com base em uma única métrica: 1. No CloudWatch console, no painel de navegação, escolha Alarmes, Todos os alarmes. 2. Selecione Criar alarme. 3. Escolha Select metric (Selecionar métrica). 4. Pesquise a métrica personalizada `sapcluster_monitoring` que foi criada na tarefa anterior. 5. Escolha o nome da métrica para o SAP SCS (por exemplo,`sapcluster_<abc>`), que também foi criado na tarefa anterior. 6. Na guia Métricas representadas graficamente, defina o seguinte: • Em Statistic (Estatística), escolha Maximum (Máximo). • Em Período, escolha 1 minuto. • Em Tipo de limite, escolha Estático e defina o limite **`sapcluster_<sid>`** para um valor maior ou igual a 1. 7. Escolha Próximo.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	8. Para Notificação, selecione o tópico SNS que você criou no primeiro épico. 9. Em Nome e Descrição, forneça o nome do alarme e uma breve descrição e escolha Avançar. 10 Escolha Create Alarm.	
Configure um alarme CloudWatch métrico para a métrica do SAP HANA.	Repita as etapas para configurar um alarme CloudWatch métrico da tarefa anterior, com estas alterações: • Para a etapa 5, escolha o nome da métrica para SAP HANA (por exemplo, `sapcluster_db_<abc>`). • Para a etapa 6, defina o limite `sapcluster_<sid>` para um valor maior que 0.	Administrador da AWS

Recursos relacionados

- Scripts de acionamento para eventos de cluster (documentação do RHEL)
- Crie o arquivo de configuração do CloudWatch agente com o assistente (CloudWatch documentação)
- Instalando e executando o CloudWatch agente em seus servidores (CloudWatch documentação)
- Crie um CloudWatch alarme com base em um limite estático (CloudWatch documentação)
- Implantação manual do SAP HANA no AWS com clusters de alta disponibilidade (documentação da SAP AWS no site)

- NetWeaver Guias SAP (documentação da SAP no AWS site)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Monitore a atividade do aplicativo usando o CloudWatch Logs Insights

Criado por Ram Kandaswamy (AWS)

Resumo

Esse padrão fornece uma solução para detectar e alertar automaticamente sobre exceções de aplicativos usando o Amazon CloudWatch Logs Insights. Ao implementar análises e alertas automatizados de registros, você pode identificar e responder rapidamente aos problemas de aplicativos em seu ambiente de produção.

Os registros desempenham um papel crucial no monitoramento do comportamento do sistema, na identificação de problemas e na garantia de um desempenho ideal. Durante um processo de migração, os arquivos de log são inestimáveis para validar o funcionamento do sistema no novo ambiente, detectar problemas de compatibilidade e identificar comportamentos inesperados. Os problemas podem estar relacionados às operações ou à segurança. Para problemas relacionados à segurança, permitir a detecção precoce de tentativas de acesso não autorizado ou atividades suspeitas é essencial para manter a segurança e a conformidade regulatória. Esse recurso é especialmente importante ao lidar com dados confidenciais ou sistemas críticos.

Esse padrão é particularmente valioso para equipes que precisam manter a alta disponibilidade dos aplicativos e responder rapidamente aos problemas de produção. É relevante em vários setores e casos de uso. Por exemplo, em telecomunicações, ele permite a identificação rápida de configurações incorretas ou interrupções da rede e a detecção de caminhos de roteamento abaixo do ideal para identificar possíveis congestionamentos. No domínio da Internet das Coisas (IoT), os componentes do Greengrass podem publicar registros no CloudWatch, permitindo que essa técnica extraia detalhes relevantes do registro e os apresente em um painel abrangente.

Pré-requisitos e limitações

Pré-requisitos

- Um aplicativo de produção implantado no ativo Conta da AWS
- Compreensão básica do formato de registro e dos padrões de exceção do aplicativo de produção
- Logs de aplicativos configurados para serem transmitidos para o Amazon CloudWatch Logs

Limitações

- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para saber a disponibilidade da região, consulte AWS Serviços por região. Para endpoints específicos, consulte Endpoints e cotas de serviço e escolha o link para o serviço.

Arquitetura

O diagrama a seguir mostra como o CloudWatch Logs Insights avalia os registros de recursos e envia uma visualização de dados relevante para um CloudWatch painel.

O diagrama mostra o seguinte fluxo de trabalho:

1. Os recursos publicam registros no CloudWatch Logs. Os recursos podem incluir AWS recursos como instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou buckets do Amazon Simple Storage Service (Amazon S3). Outro exemplo inclui sistemas locais com o CloudWatch Agente instalado que podem publicar CloudWatch registros em.
2. CloudWatch O Logs Insights filtra a sequência de padrões relevante. Exemplos de cadeias de caracteres de padrões de pesquisa incluem “erro”, “exceção” ou uma expressão regular específica.
3. Normalmente, a equipe de suporte de produção ou os desenvolvedores adicionam a visualização do padrão ao CloudWatch painel.

Automação e escala

Os desenvolvedores podem automatizar a solução desse padrão usando o AWS Cloud Development Kit (AWS CDK) AWS CloudFormation, ou AWS SDKs para lidar com vários padrões de string. As equipes podem incorporar essa automação em seus processos de integração e implantação contínuas (CI/CD) DevOps .

Ferramentas

Serviços da AWS

- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas e aplicativos, Serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.

- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.

Práticas recomendadas

- Defina e configure grupos de registros para analisar dados de registro relevantes.
- Use exploradores de campo para entender a estrutura e os campos disponíveis em seus dados de registro.
- Escreva consultas eficientes usando a sintaxe de consulta do CloudWatch Logs Insights.
- Adapte as consultas de amostra aos seus requisitos específicos para uma análise mais rápida.
- Monitore as consultas para identificar possíveis problemas de desempenho ou gargalos.
- Defina limites de consulta para evitar custos excessivos ou consumo de recursos.
- Salve as consultas para uso futuro para economizar tempo e garantir análises consistentes.
- Aplique políticas apropriadas do IAM para controlar o acesso ao CloudWatch Logs Insights e aos grupos de registros. Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para realizar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e nas melhores práticas de segurança na documentação do IAM.
- Ative a criptografia de dados AWS KMS de log usando dados de log confidenciais.

Épicos

Crie um grupo de registros e configure os registros para visualização no painel.

Tarefa	Descrição	Habilidades necessárias
Configurar permissões do IAM	Para configurar as permissões do IAM, faça o seguinte: 1. Identifique as funções do IAM usadas pelo seu aplicativo para gravar registros e pelos usuários ou serviços que criarão painéis, consultas e alarmes.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administrador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	2. Para a função do aplicativo, adicione as seguintes ações e recursos de API a uma política:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents" ], "Resource": [ "arn:aws:logs:*:*:*" ] } ] }`
	
	3. Para gerenciar CloudWatch recursos, adicione o seguinte a uma política:
	
	`{`	

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"cloudwatch:PutDashboard",
	"cloudwatch:GetDashboard",
	"logs:StartQuery",
	"logs:StopQuery",
	"logs:GetQueryResults",
	"cloudwatch:PutMetricAlarm"
	],
	"Resource": "*"
	}
	]
	}</pre> Para obter informações sobre como criar políticas do IAM ou adicionar permissões às políticas existentes, consulte Definir permissões personalizadas do IAM com políticas gerenciadas pelo cliente e Editar políticas do IAM no	

Tarefa	Descrição	Habilidades necessárias
	Guia do usuário do IAM. Para obter mais informaçõ es, consulte Gerenciamento de identidade e acesso para Amazon CloudWatch Logs e referência de permissões de CloudWatch registros no Guia do usuário do Amazon CloudWatch Logs.	

Tarefa	Descrição	Habilidades necessárias

Criar um grupo de logs do	Para criar um grupo de registros, use qualquer uma das seguintes opções:
	• Crie ou abra um arquivo CloudFormation de modelo (formato YAML ou JSON) com uma extensão `.yaml` ou `.json`. (O código a seguir usa o formato YAML.) Adicione a seguinte definição de recurso à seção Recursos do seu modelo:
	`MyLogGroup:`
	`  Type: AWS::Logs`
	`::LogGroup`
	`  Properties:`
	`  LogGroupName: my-log-group`
	Para obter mais informações, consulte Início rápido: use AWS CloudFormation para começar a usar CloudWatch os registros no Guia do usuário do Amazon CloudWatch Logs.
	• Use o CloudWatch console, conforme descrito em Criar um grupo de CloudWatch registros em Logs no
		Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administrador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Guia do usuário do Amazon CloudWatch Logs. • Use a CreateLog Groupoperação na API CloudWatch Logs.	

Tarefa	Descrição	Habilidades necessárias
Gere uma consulta do CloudWatch Logs Insights.	Para criar e salvar uma consulta do CloudWatch Logs Insights: 1. Abra o CloudWatch console. 2. Navegue até Logs Insights. 3. Crie sua consulta usando um dos seguintes métodos: • Comece com um exemplo de consulta na seção Consultas. • Escreva uma consulta personalizada. • Modifique o seguinte exemplo de consulta: `fields @timestamp, @message | filter @message like /(?i)exception/|stats count() by bin(30s)` Essa consulta verifica o arquivo de log, extrai o registro de data e hora e o conteúdo da mensagem, filtra a palavra “exceção” (sem distinção entre maiúsculas e minúsculas) e conta as ocorrências em intervalos de 30 segundos.	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administrador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Crie uma visualização em um CloudWatch painel.	Para usar um CloudWatch painel para criar uma visualização, faça o seguinte: 1. Abra o CloudWatch console e crie um CloudWatch painel (se você ainda não tiver um) ou abra um painel existente. 2. Adicione sua visualização de monitoramento de exceções. Gráficos de barras, linhas e setores estão disponíveis, dependendo da necessidade da sua empresa. Para obter mais informações, consulte Uso de widgets em CloudWatch painéis no Guia do usuário do Amazon CloudWatch Logs. Para visualizações de dados em tempo real, você pode personalizar um widget para atender às suas necessidades. Para obter mais informações sobre as opções e recursos do painel, consulte Uso de CloudWatch painéis da Amazon e Criação de CloudWatch painéis flexíveis com variáveis de painel no	Administrador da AWS, AWS DevOps, administrador de sistemas da AWS, administrador de nuvem, arquiteto de nuvem, DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Guia do usuário do Amazon CloudWatch Logs.	

Solução de problemas

Problema	Solução
Não é possível ver os resultados da consulta ou a consulta parece estar quebrada	Comece com uma consulta funcional que foi modificada a partir de uma consulta de amostra. Faça pequenas alterações incrementais em partes da consulta (como um filtro ou campo) e aproveite o recurso gerador de consultas de CloudWatch registros.
Grupos de registros que não criam fluxos de registros	Na política do IAM, certifique-se de que o recurso para as CreateLogGroupoperações CreateLogStreame as seja fornecido com um `(*)` valor de caractere curinga. A `create` operação não será bem-sucedida sem essa permissão curinga.

Recursos relacionados

- Análise de dados de registro com o CloudWatch Logs Insights
- Amazon CloudWatch FAQs
- Criação de CloudWatch painéis flexíveis com variáveis de painel
- Comece a usar o Logs Insights QL: tutoriais de consulta
- Use linguagem natural para gerar e atualizar consultas do CloudWatch Logs Insights
- Use PutDashboard com um AWS SDK ou CLI
- Trabalhando com grupos e fluxos de registros

Monitore o uso de uma Amazon Machine Image compartilhada em várias Contas da AWS

Criado por Naveen Suthar (AWS) e Sandeep Gawande (AWS)

Resumo

As Amazon Machine Images (AMIs) são usadas para criar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em seu ambiente Amazon Web Services (AWS). Você pode criar AMIs em uma conta separada e centralizada da AWS, que é chamada de conta de criador nesse padrão. Em seguida, você pode compartilhar a AMI entre várias Contas da AWS que estão na mesma Região da AWS, chamadas de contas de consumidores nesse padrão. O gerenciamento AMIs a partir de uma única conta fornece escalabilidade e simplifica a governança. Nas contas de consumidores, você pode fazer referência à AMI compartilhada nos modelos de lançamento do Amazon EC2 Auto Scaling e nos grupos de nós do Amazon Elastic Kubernetes Service (Amazon EKS).

Quando uma AMI compartilhada é preterida, cancelada ou não compartilhada, as que Serviços da AWS se referem à AMI nas contas de consumidores não podem usar essa AMI para iniciar novas instâncias. Qualquer evento de ajuste de escala automático ou re-execução da mesma instância falha. Isso pode acarretar problemas no ambiente de produção, como tempo de inatividade do aplicativo ou comprometimento do desempenho. Quando os eventos de compartilhamento e uso da AMI ocorrem em vários Contas da AWS, pode ser difícil monitorar essa atividade.

Esse padrão ajuda você a monitorar o uso e o status compartilhados da AMI em contas na mesma região. Ele usa serviços sem servidor Serviços da AWS, como Amazon EventBridge, Amazon AWS Lambda DynamoDB e Amazon Simple Email Service (Amazon SES). Você provisiona a infraestrutura como código (IaC) usando o HashiCorp Terraform. Essa solução fornece alertas quando um serviço em uma conta de consumidor faz referência a uma AMI com registro cancelado ou não compartilhada.

Pré-requisitos e limitações

Pré-requisitos

- Duas ou mais contas ativas Contas da AWS: uma conta de criador e uma ou mais contas de consumidor
- Um ou mais AMIs que são compartilhados da conta do criador para uma conta de consumidor
- CLI do Terraform, instalada (documentação do Terraform)

- Terraform AWS Provider, configurado (documentação do Terraform)
- (Opcional, mas recomendado) Backend do Terraform, configurado (documentação do Terraform)
- Git, instalado

Limitações

- Esse padrão monitora o AMIs que foi compartilhado com contas específicas usando o ID da conta. Esse padrão não monitora AMIs o que foi compartilhado com uma organização usando o ID da organização.
- AMIs só podem ser compartilhadas com contas que estejam dentro da mesma Região da AWS. Esse padrão monitora AMIs dentro de uma única região alvo. Para monitorar o uso AMIs em várias regiões, você implanta essa solução em cada região.
- Esse padrão não monitora nenhum AMIs que tenha sido compartilhado antes da implantação dessa solução. Se você quiser monitorar o compartilhamento anterior AMIs, você pode cancelar o compartilhamento da AMI e depois compartilhá-la novamente com as contas do consumidor.

Versões do produto

- Terraform versão 1.2.0 ou superior
- Terraform AWS Provider versão 4.20 ou posterior

Arquitetura

Pilha de tecnologias de destino

Os seguintes recursos são provisionados como IaC por meio do Terraform:

- Tabelas do Amazon DynamoDB
- EventBridge Regras da Amazon
- AWS Identity and Access Management Função (IAM)
- AWS Lambda funções
- Amazon SES

Arquitetura de destino

O diagrama mostra o seguinte fluxo de trabalho:

1. Uma AMI na conta do criador é compartilhada com uma conta de consumidor na mesma Região da AWS.
2. Quando a AMI é compartilhada, uma EventBridge regra na conta do criador captura o `ModifyImageAttribute` evento e inicia uma função Lambda na conta do criador.
3. A função do Lambda armazena dados relacionados à AMI em uma tabela do DynamoDB na conta de criador.
4. Quando uma AWS service (Serviço da AWS) conta do consumidor usa a AMI compartilhada para iniciar uma EC2 instância da Amazon ou quando a AMI compartilhada é associada a um modelo de execução, uma EventBridge regra na conta do consumidor captura o uso da AMI compartilhada.
5. A EventBridge regra inicia uma função Lambda na conta do consumidor. A função do Lambda faz o seguinte:
   a. A função do Lambda atualiza os dados relacionados à AMI em uma tabela do DynamoDB na conta de consumidor.
   b. A função Lambda assume uma função do IAM na conta do criador e atualiza a tabela Lambda na conta do criador. Na tabela `Mapping`, ela cria um item que mapeia o ID da instância ou o ID do modelo de execução para o ID de sua respectiva AMI.
6. A AMI gerenciada centralmente na conta de criador foi descontinuada, teve seu registro cancelado ou não é compartilhada.
7. A EventBridge regra na conta do criador captura o `DeregisterImage` evento `ModifyImageAttribute` or com a `remove` ação e inicia a função Lambda.
8. A função do Lambda verifica a tabela do DynamoDB para determinar se a AMI é usada em alguma das contas de consumidor. Se não houver instância IDs ou modelo de execução IDs associado à AMI na `Mapping` tabela, o processo estará concluído.
9. Se alguma instância IDs ou modelo de execução IDs estiver associado à AMI na `Mapping` tabela, a função Lambda usa o Amazon SES para enviar uma notificação por e-mail aos assinantes configurados.

Ferramentas

Serviços da AWS

- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- Amazon Simple Email Service (Amazon SES): ajuda você a enviar e receber e-mails usando seus próprios endereços de e-mail e domínios.

Outras ferramentas

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub cross-account-ami-monitoring-terraform-samples.

Práticas recomendadas

- Siga as melhores práticas para trabalhar com AWS Lambda funções.
- Siga as melhores práticas de construção AMIs.
- Ao criar o perfil do IAM, siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte Concessão de privilégio mínimo e nas melhores práticas de segurança na documentação do IAM.
- Configure o monitoramento e o alerta para as AWS Lambda funções. Para obter mais informações, consulte Monitorar e solucionar problemas de funções do Lambda.

Épicos

Personalize os arquivos de configuração do Terraform

Tarefa	Descrição	Habilidades necessárias
Crie os perfis AWS CLI nomeados.	Para a conta do criador e a conta de cada consumidor, crie um perfil chamado AWS Command Line Interface (AWS CLI). Para obter instruções, consulte Configurar o AWS CLI no Centro de recursos de AWS introdução.	DevOps engenheiro
Clonar o repositório.	Insira o comando da a seguir. Isso clona o repositório cross-account-ami-monitoring-terraform-samples usando SSH. GitHub `git clone git@github.com:aws-samples/cross-account-ami-monitoring-terraform-samples.git`	DevOps engenheiro
Atualize o arquivo provider.tf.	1. Insira comando a seguir para navegar para a pasta `terraform` no repositório clonado. `cd cross-account-ami-monitoring/terraform` 2. Abra o arquivo `provider.tf` .	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	3. Atualize as configurações do Terraform AWS Provider para a conta do criador e a conta do consumidor da seguinte forma: • Em `alias`, insira um nome para a configuração de provedor. • Para `region`, insira o destino Região da AWS em que você deseja implantar essa solução. • Para `profile`, insira o perfil AWS CLI nomeado para acessar a conta. 4. Se você estiver configurando mais de uma conta de consumidor, crie um perfil para cada conta adicional de consumidor. 5. Salve e feche o arquivo `provider.tf` . Para obter mais informações sobre como configurar os provedores, consulte Configurações de vários provedores na documentação do Terraform.	

Tarefa	Descrição	Habilidades necessárias
Atualize o arquivo terraform .tfvars.	1. Abra o arquivo `terraform.tfvars` . 2. No parâmetro `account_email_mapping` , configure alertas para a conta de criador e a conta de consumidor da seguinte forma: • Em `account`, insira o ID da conta. • Em `email`, informe o endereço de e-mail para o qual você deseja enviar alertas. Você pode inserir somente um endereço de e-mail para cada conta. 3. Se você estiver configurando mais de uma conta de consumidor, insira uma conta e um endereço de e-mail para cada conta de consumidor adicional. 4. Salve e feche o arquivo `terraform.tfvars` .	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Atualize o arquivo main.tf.	Conclua essas etapas somente se você estiver implantando essa solução em mais de uma conta de consumidor. Se você estiver implantando essa solução em apenas uma conta de consumidor, nenhuma modificação desse arquivo será necessária. 1. Abra o arquivo `main.tf`. 2. Para cada conta de consumidor adicional , crie um novo módulo baseado no módulo `consumer_account_A` do modelo. Para cada conta de consumidor, para `provider`, o valor deve corresponder ao alias que você inseriu no arquivo `provider.tf` . 3. Salve e feche o arquivo `main.tf`.	DevOps engenheiro

Implemente a solução usando o Terraform

Tarefa	Descrição	Habilidades necessárias
Implante a solução.	Na CLI do Terraform, insira os seguintes comandos para implantar os recursos	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	AWS nas contas de criador e consumidor:
	1. Insira o seguinte comando para inicializar o Terraform.
	`terraform init`
	2. Insira o seguinte comando para validar as configura ções do Terraform.
	`terraform validate`
	3. Insira o seguinte comando para criar um plano de execução do Terraform.
	`terraform plan`
	4. Revise as alterações de configuração no plano do Terraform e confirme que você deseja implementar essas alterações.
	5. Execute o seguinte comando para implementar os recursos.
	`terraform apply`	

Tarefa	Descrição	Habilidades necessárias
Verifique a identidade do endereço de e-mail.	Quando você implantou o plano Terraform, o Terraform criou uma identidade de endereço de e-mail para cada conta de consumidor no Amazon SES. Antes de enviar notificações para esse endereço de e-mail, você deve verificá-lo. Para obter instruções, consulte Verificação da identidade de um endereço de e-mail na documentação do Amazon SES.	AWS geral

Validar a implantação de recursos

Tarefa	Descrição	Habilidades necessárias
Valide a implantação na conta de criador.	1. Faça login na conta do criador. 2. Na barra de navegação, confirme se você está visualizando o alvo Região da AWS. Se você estiver em outra região, escolha o nome da região exibida atualmente e escolha a região de destino. 3. Abra o console do DynamoDB. 4. No painel de navegação, selecione Tabelas.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	5. Na lista de tabelas, valide se a tabela `AmiShare` está presente. 6. Abra o console do lambda. 7. Selecione Funções no painel de navegação. 8. Na lista de funções, valide se a função `ami-share` está presente. 9. Abra o console do IAM. 10. No painel de navegação, selecione Perfis. 11. Na lista de funções, valide se a função `external-ddb-role` está presente. 12. Abra o console de EventBridge . 13. No painel de navegação, escolha Regras. 14. Na lista de regras, valide se a regra `modify_image_attribute_event` está presente. 15. Abra o console do Amazon SES. 16. No painel de navegação , escolha Identidades verificadas. 17. Na lista de identidades, valide se uma identidade de endereço de e-mail foi	

Tarefa	Descrição	Habilidades necessárias
	registrada e verificada para cada conta de consumidor.	

Tarefa	Descrição	Habilidades necessárias
Valide a implantação na conta de consumidor.	1. Faça login na conta de consumidor. 2. Na barra de navegação, confirme se você está visualizando o alvo Região da AWS. Se você estiver em outra região, escolha o nome da região exibida atualmente e escolha a região de destino. 3. Abra o console do DynamoDB. 4. No painel de navegação, selecione Tabelas. 5. Na lista de tabelas, valide se a tabela `Mapping` está presente. 6. Abra o console do lambda. 7. Selecione Funções no painel de navegação. 8. Na lista de funções, valide se as funções `ami-usage-function` e `ami-deregister-function` estão presentes. 9. Abra o console de EventBridge . 10. No painel de navegação, escolha Regras. 11. Na lista de regras, valide se as regras `ami_usage_events` e `ami_dereg`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`ister_events` estão presentes.	

Validar o monitoramento

Tarefa	Descrição	Habilidades necessárias
Crie uma AMI na conta de criador.	1. Na conta de criador, crie uma AMI privada. Para obter instruções, consulte Criar uma AMI a partir de uma EC2 instância da Amazon. 2. Compartilhe a nova AMI com uma das contas de consumidor. Para obter instruções, consulte Compartilhar uma AMI com informações específicas Contas da AWS.	DevOps engenheiro
Use a AMI na conta de consumidor.	Na conta do consumidor, use a AMI compartilhada para criar uma EC2 instância da Amazon ou um modelo de execução. Para obter instruções, consulte Como faço para iniciar uma EC2 instância da Amazon a partir de uma AMI personalizada (AWS re:POST Knowledge Center) ou Criar um modelo de lançamento para um grupo do Auto Scaling (document	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ação do Amazon Auto EC2 Scaling).	
Valide o monitoramento e os alertas.	1. Faça login na conta do criador. 2. Abra o EC2 console da Amazon. 3. No painel de navegação, escolha AMIs. 4. Selecione sua AMI na lista e, em seguida, escolha Ações, Editar permissões de AMI. 5. Na seção Contas compartilhadas, selecione a conta de consumidor e escolha Remover selecionada. 6. Escolha Salvar alterações. 7. Valide se o endereço de e-mail de destino que você definiu para a conta de consumidor recebe uma notificação de que o compartilhamento foi cancelado para a AMI.	DevOps engenheiro

(Opcional) Interromper o monitoramento compartilhado AMIs

Tarefa	Descrição	Habilidades necessárias
Excluir os recursos.	1. Digite o comando a seguir para remover os recursos implantados por esse	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	padrão e interromper o monitoramento compartil hado AMIs. `terraform destroy` 2. Confirme o comando `destroy` inserindo `yes`.	

Solução de problemas

Problema	Solução
Não recebi um alerta por e-mail.	Pode haver vários motivos pelos quais o e-mail do Amazon SES não foi enviado. Verifique o seguinte: 1. Na seção Epics, use o épico Validar a implantação de recursos para confirmar se a infraestrutura foi provisionada adequadam ente em todos eles. Contas da AWS 2. Valide os eventos da função Lambda no Amazon CloudWatch Logs. Para obter instruções, consulte Como usar o CloudWatc h console na documentação do Lambda. Confirme se não há problemas de permissõe s, como uma negação explícita em qualquer política baseada em identidade ou em recursos. Para obter mais informações, consulte Lógica de avaliação de políticas na documentação do IAM. 3. No Amazon SES, valide se o status da identidade do endereço de e-mail é Verificad o. Para obter mais informações, consulte

Problema	Solução
	Verificar identidades de um endereço de e-mail.

Recursos relacionados

AWS documentação

- Criar funções do Lambda com Python (documentação do Lambda)
- Crie uma AMI (EC2 documentação da Amazon)
- Compartilhe uma AMI com uma AMI específica Contas da AWS (EC2 documentação da Amazon)
- Cancele o registro da sua AMI (documentação da Amazon EC2)

Documentação do Terraform

- Instalar o Terraform
- Configuração de backend do Terraform
- Provedor Terraform do AWS
- Download binário do Terraform

Configure alertas para encerramentos programáticos de contas no AWS Organizations

Criado por Richard Milner-Watts (AWS), Debojit Bhadra (AWS) e Manav Yadav (AWS)

Resumo

A CloseAccount API para AWS Organizations permite que você feche contas de membros dentro de uma organização de forma programática, sem precisar fazer login na conta com credenciais raiz. A RemoveAccountFromOrganization API extrai uma conta de uma organização no AWS Organizations, então ela se torna uma conta independente.

Isso aumenta APIs potencialmente o número de operadores que podem fechar ou remover uma conta da AWS. Todos os usuários que têm acesso à organização por meio do AWS Identity and Access Management (IAM) na conta de gerenciamento do AWS Organizations podem ligar para eles APIs, portanto, o acesso não se limita ao proprietário do e-mail raiz da conta com qualquer dispositivo de autenticação multifator (MFA) associado.

Esse padrão implementa alertas quando o `CloseAccount` e `RemoveAccountFromOrganization` APIs é chamado, para que você possa monitorar essas atividades. Para alertas, ele usa um tópico do Amazon Simple Notification Service (Amazon SNS). Também é possível configurar as notificações do Slack usando um webhook.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma organização no AWS Organizations
- Acesso à conta de gerenciamento da organização, sob a raiz da organização, para criar os recursos necessários

Limitações

- Conforme descrito na referência da API do AWS Organizations, a API `CloseAccount` permite que apenas 10% das contas ativas dos membros sejam fechadas em um período contínuo de 30 dias.

- Quando uma conta da AWS é fechada, seu status é alterado para SUSPENSO. Por 90 dias após essa transição de status, o AWS Support pode reabrir a conta. A conta é excluída permanentemente após 90 dias.
- Usuários que têm acesso à conta de gerenciamento do AWS Organizations e também APIs podem ter permissões para desativar esses alertas. Se a principal preocupação for comportamento malicioso em vez de exclusão acidental, considere proteger os recursos criados por esse padrão com um limite de permissões do IAM.
- A API chama por `CloseAccount` e `RemoveAccountFromOrganization` é processado na região Leste dos EUA (Norte da Virgínia) (`us-east-1`). Portanto, você deve implantar essa solução em `us-east-1` para observar os eventos.

Arquitetura

Pilha de tecnologias de destino

- AWS Organizations
- AWS CloudTrail
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Arquitetura de destino

O diagrama a seguir mostra a arquitetura da solução desse padrão.

1. O AWS Organizations processa uma solicitação `CloseAccount` ou `RemoveAccountFromOrganization`.
2. A Amazon EventBridge está integrada à AWS CloudTrail para entregar esses eventos ao barramento de eventos padrão.
3. Uma EventBridge regra personalizada da Amazon corresponde às solicitações do AWS Organizations e chama uma função do AWS Lambda.
4. A função do Lambda entrega uma mensagem para um tópico do SNS, na qual os usuários podem se inscrever para receber alertas por e-mail ou processamento adicional.

5. Se as notificações do Slack estiverem ativadas, a função do Lambda enviará uma mensagem para um webhook do Slack.

Ferramentas

Serviços da AWS

- CloudFormationA AWS fornece uma forma de modelar uma coleção de recursos relacionados da AWS e de terceiros, provisioná-los de forma rápida e consistente e gerenciá-los ao longo de seus ciclos de vida, tratando a infraestrutura como código.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que você pode usar para conectar seus aplicativos a dados de várias fontes. EventBridge recebe um evento, um indicador de uma mudança no ambiente, e aplica uma regra para rotear o evento até um alvo. As regras fazem a correspondência entre os eventos e os destinos com base na estrutura do evento, chamada padrão do evento ou em um schedule.
- O AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia a milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando seu código não estiver em execução.
- O AWS Organizations ajuda a gerenciar e governar centralmente seu ambiente à medida que você expande e escala seus recursos da AWS da. Usando o AWS Organizations, você pode criar programaticamente novas contas da AWS e alocar recursos, agrupar contas para organizar seus fluxos de trabalho, aplicar políticas a contas ou grupos para fins de governança e simplificar o faturamento usando um único método de pagamento para todas as suas contas.
- A AWS CloudTrail monitora e registra a atividade da conta em toda a sua infraestrutura da AWS e oferece controle sobre ações de armazenamento, análise e remediação.
- O Amazon Simple Notification Service (Amazon SNS) é um serviço de mensagens totalmente gerenciado para comunicação (A2A) application-to-application e (A2P) application-to-person.

Outras ferramentas

- A biblioteca AWS Lambda Powertools for Python é um conjunto de utilitários que fornece recursos de rastreamento, registro em log, métricas e tratamento de eventos para funções do Lambda.

Código

O código desse padrão está localizado no repositório do GitHub AWS Account Closer Notifier.

A solução inclui um CloudFormation modelo que implanta a arquitetura desse padrão. Ele usa a biblioteca AWS Lambda Powertools for Python para fornecer registro e rastreamento.

Épicos

Implantar a arquitetura

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo para a pilha de soluções.	O CloudFormation modelo para esse padrão está na ramificação principal do GitHub repositório. Ele implanta as funções, EventBridge as regras, as funções do Lambda e o tópico do SNS do IAM. Para iniciar o modelo: 1. Clone o GitHub repositório para obter uma cópia do código da solução. 2. Abra o Console de Gerenciamento da AWS para a conta de gerenciamento do AWS Organizations. 3. Escolha a região Leste dos EUA (Norte da Virgínia`us-east-1`) () e abra o CloudFormation console. 4. Crie a pilha usando o modelo `account-c`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`losure-notifier.yml` e especificando os seguintes valores: • Nome da pilha: `aws-account-closure-notifier-stack` • `ResourcePrefix` parâmetro:`aws-account-closure-notifier` • `SlackNotification` parâmetro : se as notificações do Slack forem necessárias, altere essa configuração para `true`. • Parâmetro `SlackWebhookEndpoint` : se as notificações do Slack forem necessárias, especifique o URL do webhook. Para obter mais informações sobre o lançamento de uma CloudFormation pilha, consulte a documentação da AWS.	

Tarefa	Descrição	Habilidades necessárias
Verifique se a solução foi iniciada com sucesso.	1. Aguarde até que a CloudFormation pilha alcance o status CREATE_COMPLETE. 2. Abra o EventBridge console em `us-east-1` . 3. Verifique se uma nova regra foi criada com o nome `aws-account-closure-notifier-event-rule` .	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Inscreva-se no tópico do SNS.	(Opcional) Se você quiser se inscrever no tópico do SNS: 1. Abra o console do Amazon SNS em `us-east-1` e encontre o tópico chamado `aws-account-closure-notifier-sns-topic`. 2. Escolha o nome do tópico e, em seguida, escolha Criar inscrição. 3. Em Protocolo, escolha E-mail. 4. Em Endpoint, especifique um endereço de e-mail para receber a notificação e, em seguida, escolha Criar assinatura. 5. Verifique sua caixa de entrada de e-mail para ver uma mensagem do AWS Notifications. Use o link no e-mail para confirmar a assinatura. Para obter mais informações sobre como configurar as notificações do SNS, consulte a documentação do Amazon SNS.	Administrador da AWS

Verifique a solução

Tarefa	Descrição	Habilidades necessárias
Envie um evento de teste ao barramento de eventos padrão.	O GitHub repositório fornece um evento de amostra que você pode enviar para o barramento de eventos EventBridge padrão para teste. A EventBridge regra também reage aos eventos que usam a fonte `account.closure.notifier` de eventos personalizada. **Note** Você não pode usar a fonte do CloudTrail evento para enviar esse evento, porque não é possível enviar um evento como um serviço da AWS. Para enviar um evento de teste: 1. Abra o EventBridge console em `us-east-1` . 2. No painel de navegação, em Barramentos, escolha Barramentos de eventos e selecione o barramento de eventos padrão. 3. Escolha Enviar eventos.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	4. Em Origem do evento, insira `account.closure.notifier` . 5. Em Tipo de detalhe, insira `AWS API Call via CloudTrail` . 6. Para detalhes do evento, copie e cole o conteúdo `tests/dummy-event.json` do GitHub repositório na caixa de texto. 7. Escolha Enviar para iniciar o fluxo de trabalho de notificação.	
Verifique se a notificação por e-mail foi recebida.	Verifique se há notificações na caixa de correio que se inscreveu no tópico do SNS. Você deve receber um e-mail com detalhes da conta que foi fechada e da entidade principal que realizou a chamada de API.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Verifique se a notificação do Slack foi recebida.	(Opcional) Se você especificou uma URL de webhook para o `SlackWebhookEndpoint` parâmetro ao implantar o CloudFormation modelo, verifique o canal do Slack que está mapeado para o webhook. Ele deve exibir uma mensagem com detalhes da conta que foi fechada e da entidade principal que realizou a chamada de API.	Administrador da AWS

Recursos relacionados

- CloseAccount ação (referência da API do AWS Organizations)
- RemoveAccountFromOrganization ação (referência da API do AWS Organizations)
- Powertools do AWS Lambda para Python

Ver os detalhes do snapshot do EBS para sua conta ou organização da AWS

Criado por Arun Chandapillai (AWS) e Parag Nagwekar (AWS)

Resumo

Este padrão descreve como você pode gerar automaticamente um relatório sob demanda de todos os snapshots do Amazon Elastic Block Store (Amazon EBS) na sua conta da Amazon Web Services (AWS) ou unidade organizacional (OU) no AWS Organizations.

O Amazon EBS é um easy-to-use serviço de armazenamento em bloco escalável e de alto desempenho projetado para o Amazon Elastic Compute Cloud (Amazon). EC2 Um volume do EBS fornece armazenamento durável e persistente que você pode anexar às suas EC2 instâncias. Você pode usar volumes do EBS como armazenamento primário para seus dados e fazer um point-in-time backup dos volumes do EBS criando um snapshot. É possível usar o Console de Gerenciamento da AWS ou a AWS Command Line Interface (AWS CLI) para visualizar detalhes de snapshots específicos do EBS. Este padrão fornece uma forma programática de recuperar informações sobre todos os snapshots do EBS em sua conta ou OU da AWS.

Você pode usar o script fornecido por esse padrão para gerar um arquivo com valores separados por vírgula (CSV) que tenha as seguintes informações sobre cada snapshot: ID da conta, ID do snapshot, ID e tamanho do volume, data em que o snapshot foi obtido, ID da instância e descrição. Se seus snapshot do EBS estiverem marcados, o relatório também incluirá os atributos do proprietário e da equipe.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS CLI versão 2 instalada e configurada
- Perfil do AWS Identity and Access Management (IAM) com as permissões apropriadas (permissões de acesso para uma conta específica ou para todas as contas em uma OU, se você estiver planejando executar o script a partir do AWS Organizations)

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho do script que gera um relatório sob demanda de snapshots do EBS distribuídos por várias contas da AWS em uma OU.

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O Amazon Elastic Block Store (Amazon EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias. EC2
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias contas AWS em uma organização que você cria e gerencia de maneira centralizada.

Código

O código do aplicativo de amostra usado nesse padrão está disponível em GitHub, no aws-ebs-snapshots-awsorganizationsrepositório. Siga as instruções da próxima seção para usar os arquivos de amostra.

Épicos

Faça download do script

Tarefa	Descrição	Habilidades necessárias
Baixe o script Python.	Baixe o script GetSnapshotDetailsAllAccountsOU.py do GitHub repositório.	AWS geral

Obtenha detalhes do snapshot do EBS para uma conta da AWS

Tarefa	Descrição	Habilidades necessárias

Execute o script do Python.	Execute o comando :
	`python3 getsnapsh otinfo.py --file <output-file>.csv --region <region-name>`
	em que `<output-file>` se refere ao arquivo CSV resultante no qual você deseja que as informações sobre os snapshots do EBS sejam inseridas e `<region-name>` é a região da AWS em que os snapshots são armazenados. Por exemplo:
	`python3 getsnapsh otinfo.py --file snapshots.csv --region us-east-1`
		AWS geral

Obtenha detalhes do snapshot do EBS para uma organização

Tarefa	Descrição	Habilidades necessárias
Execute o script do Python.	Execute o comando : `python3 getsnapsh otinfo.py --file <output-file>.csv --role <IAM-role> --region <region-name>`	AWS geral

Tarefa	Descrição	Habilidades necessárias
	em que `<output-file>` se refere ao arquivo CSV resultante no qual você deseja que as informaçõ es sobre os snapshots do EBS sejam inseridas, `<IAM-role>` é o perfil que fornece as permissões para acesso à AWS Organizat ions e `<region-name>` é a região da AWS em que os snapshots são armazenados. Por exemplo: `python3 getsnapsh otinfo.py --file snapshots.csv --role <IAM role> --region us-west-2`	

Recursos relacionados

- Documentação do Amazon EBS
- Ações do Amazon EBS
- Referência da API do Amazon EBS
- Aprimoramento do desempenho do Amazon EBS
- Recursos do Amazon EBS
- Definição de preço de snapshot EBS

Mais informações

Tipos de snapshots do EBS

O Amazon EBS fornece três tipos de snapshots, com base na propriedade e no acesso:

- Pertencente a você: por padrão, só é possível criar volumes a partir dos snapshots que você possui.
- Snapshots públicos: você pode compartilhar snapshots publicamente com todas as outras contas da AWS. Para criar um snapshot público, você modifica as permissões de um snapshot para compartilhá-lo com as contas da AWS que você especificar. Os usuários autorizados podem usar os snapshots que você compartilhar para criar os próprios volumes do EBS, ao passo que seu snapshot original não será afetado. Se você desejar, poderá disponibilizar os snapshots não criptografados publicamente para todos os usuários da AWS. No entanto, você não pode disponibilizar publicamente seus snapshots criptografados por motivos de segurança. Os snapshots públicos representam um risco de segurança considerável devido à possibilidade de exposição de dados pessoais e confidenciais. É altamente recomendável não compartilhar seus snapshots do EBS com todas as contas da AWS. Para obter informações sobre a cópia de um DB snapshot, consulte a documentação do AWS.
- Snapshots privados: você pode compartilhar snapshots de forma privada com contas individuais da AWS que você especificar. Para compartilhar o snapshot de forma privada com contas específicas da AWS, siga as instruções na documentação da AWS e escolha Privado para a configuração de permissões. Os usuários autorizados podem usar os snapshots que você compartilhar para criar os próprios volumes do EBS, ao passo que seu snapshot original não será afetado.

Visões gerais e procedimentos

A tabela a seguir fornece links para obter mais informações sobre snapshots do EBS, incluindo como reduzir os custos de volume do EBS ao descobrir e excluir snapshots não utilizados, além de arquivar snapshots raramente acessados que não exigem recuperação frequente ou rápida.

Para obter mais informações sobre	Consulte
Snapshots, seus atributos e suas limitações	Criar snapshots de Amazon EBS
Para criar um snapshot	Console: criar um snapshot AWS CLI: comando delete-snapshot Por exemplo:

```
aws ec2 create-snapshot --volume-id
 vol-1234567890abcdef0 --description
 " volume snapshot"
```

Arquivamento de snapshots (informações gerais)	Excluir um snapshot do Amazon EBS
Para excluir um snapshot	Console: excluir um snapshot AWS CLI: comando delete-snapshot Por exemplo:

```
aws ec2 delete-snapshot --snapshot-id
 snap-1234567890abcdef0
```

Arquivamento de snapshots (informações gerais)	Arquivar snapshots do Amazon EBS Arquivo de snapshots do Amazon EBS (publicação no blog)
Para arquivar um snapshot	Console: arquivar um snapshot AWS CLI: comando modify-snapshot-tier
Como recuperar um snapshot arquivado	Console: Restaurar um snapshot arquivado AWS CLI: comando restore-snapshot-tier
Definição de preço de snapshot	Preços do Amazon EBS

PERGUNTAS FREQUENTES

Qual o período mínimo de arquivamento?

O período de arquivamento mínimo é de 90 dias.

Quanto tempo seria necessário para restaurar um snapshot arquivado?

Pode levar até 72 horas para restaurar um snapshot arquivado da camada de arquivo para a camada padrão, dependendo do tamanho do snapshot.

Os snapshots arquivados são snapshots completos?

Os snapshots arquivados são sempre snapshots completos.

Quais snapshots um usuário pode arquivar?

Só é possível arquivar os snapshots que você possui na sua conta.

Você pode arquivar um snapshot do volume de um dispositivo raiz de uma imagem de máquina da Amazon (AMI) registrada?

Não, você não pode arquivar um snapshot do volume do dispositivo raiz de uma AMI registrada.

Quais são as considerações de segurança para compartilhar um snapshot?

Ao compartilhar um snapshot, você está oferecendo a outras pessoas o acesso a todos os dados no snapshot. Compartilhe snapshots somente com as pessoas de sua confiança.

Como você compartilha um snapshot com outra região da AWS?

Os snapshots são restritos à região na qual foram criados. Para compartilhar um snapshot com outra região, copie o snapshot nessa região e, em seguida, compartilhe a cópia.

Você pode compartilhar snapshots criptografados?

Não é possível compartilhar snapshots criptografados com a chave gerenciada pela AWS padrão. Você só pode compartilhar snapshots criptografados com uma chave gerenciada pelo cliente. Ao compartilhar um snapshot criptografado, também é necessário compartilhar a chave gerenciada pelo cliente usada para criptografar o snapshot.

E quanto aos snapshots não criptografados?

É possível compartilhar apenas snapshots não criptografados publicamente.

Mais padrões

- Automatize a criação de contas usando o Landing Zone Accelerator em AWS
- Automatize as operações de AWS infraestrutura usando o Amazon Bedrock
- Automatize a avaliação de recursos da AWS
- Faça o inventário automático de AWS recursos em várias contas e regiões
- Automatize o portfólio e a implantação de produtos do AWS Service Catalog usando o AWS CDK
- Automatize o gerenciamento dinâmico de pipelines para implantar soluções de hotfix em ambientes Gitflow usando e AWS Service CatalogAWS CodePipeline
- Automatize a ingestão e a visualização de métricas personalizadas do Amazon MWAA no Amazon Managed Grafana usando o Terraform
- Automatize as verificações de segurança para cargas de trabalho entre contas usando o Amazon Inspector e AWS Security Hub
- Anexe automaticamente uma política gerenciada da AWS para Systems Manager aos perfis de EC2 instância usando o Cloud Custodian e o AWS CDK
- Criptografe automaticamente volumes novos e existentes do Amazon EBS
- Centralize o monitoramento usando o Amazon CloudWatch Observability Access Manager
- Verifique as EC2 instâncias para ver as tags obrigatórias no lançamento
- Limpe os recursos AWS do Account Factory for Terraform (AFT) com segurança após a perda do arquivo de estado
- Configure o registro e o monitoramento de eventos de segurança em seu AWS IoT ambiente
- Crie uma definição de tarefa do Amazon ECS e monte um sistema de arquivos em EC2 instâncias usando o Amazon EFS
- Crie regras AWS Config personalizadas usando AWS CloudFormation Guard políticas
- Personalize os nomes das funções padrão usando AWS CDK aspectos e escotilhas de escape
- Exclua volumes não utilizados do Amazon EBS usando e AWS ConfigAWS Systems Manager
- Implemente e gerencie AWS Control Tower controles usando AWS CDK e CloudFormation
- Implemente e gerencie AWS Control Tower controles usando o Terraform
- Implante código em várias regiões da AWS usando AWS CodePipeline CodeCommit, AWS e AWS CodeBuild
- Habilite a Amazon GuardDuty condicionalmente usando modelos AWS CloudFormation

- Exporte um relatório das identidades do AWS IAM Identity Center e suas atribuições usando PowerShell
- Gere um CloudFormation modelo da AWS contendo regras gerenciadas do AWS Config usando o Troposphere
- Conceda às instâncias do SageMaker notebook acesso temporário a um CodeCommit repositório em outra conta da AWS
- Integre o controlador universal Stonebranch com o AWS Mainframe Modernization
- Lance um CodeBuild projeto em várias contas da AWS usando Step Functions e uma função de proxy Lambda
- Migrar certificados SSL do Windows para um Application Load Balancer usando o ACM
- Monitorar a atividade do usuário raiz do IAM
- Otimize implantações sem servidor de várias contas usando os fluxos de trabalho e Actions AWS CDK GitHub
- Execute ações personalizadas a partir de CodeCommit eventos da AWS
- Preserve o espaço IP roteável em projetos de VPC com várias contas para sub-redes sem workload
- Provisione funções do IAM com privilégios mínimos implantando uma solução de máquina de venda automática de funções
- Registrar várias contas da AWS com um único endereço de e-mail usando o Amazon SES
- Remova EC2 as entradas Contas da AWS da Amazon em frente AWS Managed Microsoft AD usando a AWS Lambda automação
- Remova EC2 as entradas da Amazon na mesma forma Conta da AWSAWS Managed Microsoft AD usando a AWS Lambda automação
- Alternar as credenciais do banco de dados sem reiniciar os contêineres
- Executar workloads agendadas e orientadas por eventos em grande escala com o AWS Fargate
- Envie notificações para uma instância de banco de dados Amazon RDS para SQL Server usando um servidor SMTP on-premises e o Database Mail
- Configure um painel de monitoramento da Grafana para a AWS ParallelCluster
- Configure o registro centralizado em escala corporativa usando o Terraform
- Marque anexo do gateway de trânsito automaticamente usando o AWS Organizations
- Use as consultas do BMC Discovery para extrair dados de migração para o planejamento da migração

- Verifique as melhores práticas operacionais para o PCI DSS 4.0 usando AWS Config
- Visualize relatórios de credenciais do IAM para todas as contas da AWS usando a Amazon QuickSight

Mensagens e comunicações

Tópicos

- Automatize a configuração RabbitMQ no Amazon MQ
- Melhore a qualidade das chamadas nas estações de trabalho dos atendentes nas centrais de atendimento do Amazon Connect
- Mais padrões

Automatize a configuração RabbitMQ no Amazon MQ

Criado por Yogesh Bhatia (AWS) e Afroz Khan (AWS)

Resumo

O Amazon MQ é um serviço de agente de mensagens gerenciado, que fornece compatibilidade com muitos agentes de mensagens populares. O uso do Amazon MQ com o RabbitMQ fornece um cluster RabbitMQ robusto gerenciado na nuvem da Amazon Web Services (AWS) com vários agentes e opções de configuração. O Amazon MQ fornece uma infraestrutura altamente disponível, segura e escalável e pode processar um grande número de mensagens por segundo com facilidade. Vários aplicativos podem usar a infraestrutura com diferentes hosts virtuais, filas e trocas. No entanto, gerenciar essas opções de configuração ou criar a infraestrutura manualmente pode exigir tempo e esforço. Esse padrão descreve uma forma de gerenciar as configurações do RabbitMQ em uma única etapa, por meio de um único arquivo. Você pode incorporar o código fornecido com esse padrão em qualquer ferramenta de integração contínua (CI), como Jenkins ou Bamboo.

Você pode usar esse padrão para configurar qualquer cluster do RabbitMQ. Tudo o que é necessário é conectividade com o cluster. Embora existam muitas outras maneiras de gerenciar as configurações do RabbitMQ, essa solução cria configurações completas do aplicativo em uma única etapa, para que você possa gerenciar filas e outros detalhes com facilidade.

Pré-requisitos e limitações

Pré-requisitos

- AWS Command Line Interface (AWS CLI) instalada e configurada para apontar para sua conta AWS (para obter instruções, consulte a documentação da AWS CLIhttps://docs.aws.amazon.com/cli/latest/userguide/install-cliv2-linux.html)
- Ansible instalado, para que você possa executar playbooks para criar a configuração
- rabbitmqadmin instalado (para obter instruções, consulte a documentação do RabbitMQ)
- Um cluster RabbitMQ no Amazon MQ, criado com métricas saudáveis da Amazon CloudWatch

Requisitos adicionais

- Certifique-se de criar as configurações para hosts virtuais e usuários separadamente e não como parte do JSON.
- Certifique-se de a configuração JSON faça parte do repositório e tenha controle de versão.

- A versão da CLI do rabbitmqadmin deve ser a mesma do servidor RabbitMQ, então a melhor opção é baixar a CLI do console do RabbitMQ.
- Como parte do pipeline, certifique-se que a sintaxe JSON seja validada antes de cada execução.

Versões do produto

- AWS CLI versão 2.0
- Ansible versão 2.9.13
- rabbitmqadmin versão 3.9.13 (deve ser igual à versão do servidor RabbitMQ)

Arquitetura

Pilha de tecnologia de origem

- Um cluster RabbitMQ executado em uma máquina virtual (VM) on-premises existente ou em um cluster Kubernetes (no local ou na nuvem)

Pilha de tecnologias de destino

- Configurações automatizadas do Automated RabbitMQ no Amazon MQ para RabbitMQ

Arquitetura de destino

Há muitas formas de configurar o RabbitMQ. Esse padrão usa a funcionalidade de configuração de importação, em que um único arquivo JSON contém todas as configurações. Esse arquivo aplica todas as configurações e pode ser gerenciado por um sistema de controle de versão, como o Bitbucket ou o Git. Esse padrão usa o Ansible para implementar a configuração por meio da CLI rabbitmqadmin.

Ferramentas

Ferramentas

- rabbitmqadmin é uma ferramenta de linha de comando para a API baseada em HTTP do RabbitMQ. Ele é usado para gerenciar e monitorar nós e clusters do RabbitMQ.
- O Ansible é uma ferramenta de código aberto para automatizar aplicativos e infraestrutura de TI.

- A AWS CLI permite interagir com serviços da AWS usando comandos no shell da linha de comando.

Serviços da AWS

- O Amazon MQ é um serviço gerenciado de agente de mensagens que facilita a configuração e operação de agentes de mensagem na nuvem.
- CloudFormationA AWS ajuda você a configurar sua infraestrutura da AWS e acelerar o provisionamento na nuvem com a infraestrutura como código.

Código

O arquivo de configuração JSON usado nesse padrão e um exemplo de manual do Ansible são fornecidos no anexo.

Épicos

Crie sua infraestrutura AWS

Tarefa	Descrição	Habilidades necessárias
Crie um cluster RabbitMQ na AWS.	Se você ainda não tem um cluster RabbitMQ, você pode usar a AWS CloudFormation para criar a pilha na AWS. Ou você pode usar o módulo Cloudformation no Ansible para criar a pilha. Com a última abordagem, você pode usar o Ansible para as duas tarefas: criar a infraestrutura do RabbitMQ e gerenciar configurações.	AWS CloudFormation, Ansible

Criar as configurações do Amazon MQ para RabbitMQ

Tarefa	Descrição	Habilidades necessárias
Crie um arquivo de propriedades.	Faça o download do arquivo de configuração JSON (`rabbitmqconfig.json`) no anexo ou exporte-o do console do RabbitMQ. Modifique-o para configurar filas, trocas e vinculações. Este arquivo de configuração demonstra o seguinte: - Cria duas filas: `sample-queue1` e `sample-queue2` - Cria duas trocas: `sample-exchange1` e `sample-exchange2` - Implementa a ligação entre as filas e as trocas Essas configurações são realizadas no host virtual root (/), conforme exigido pelo rabbitmqadmin.	JSON
Recupere os detalhes da infraestrutura do Amazon MQ para RabbitMQ.	Recupere os seguintes detalhes da infraestrutura do RabbitMQ na AWS: • Nome do agente • RabbitMQ host • Nome de usuário do RabbitMQ (o usuário	AWS CLI, Amazon MQ

Tarefa	Descrição	Habilidades necessárias
	administrador criado durante a criação do cluster) • Senha RabbitMQ É possível usar o Console de Gerenciamento da AWS ou a AWS CLI para recuperar essas informações. Esses detalhes permitem que o manual do Ansible se conecte à sua conta AWS e use o cluster RabbitMQ para executar comandos. **Important** O computador que executa o manual do Ansible deve ser capaz de acessar sua conta da AWS, e a CLI da AWS já deve estar configurada, conforme descrito na seção Pré-requisitos.	

Tarefa	Descrição	Habilidades necessárias

Crie o arquivo hosts_var.	Crie o arquivo `hosts_var` para o Ansible e certifique-se de que todas as variáveis estejam definidas no arquivo. Considere usar o Ansible Vault para armazenar a senha. Você pode configurar o arquivo `hosts_var` da seguinte forma (substitua os asteriscos pelas suas informações):
	`RABBITMQ_HOST: "**********.mq.us-east-2.amazonaws.com"`
	`RABBITMQ_VHOST: "/"`
	`RABBITMQ_USERNAME: "admin"`
	`RABBITMQ_PASSWORD: "*******"`
		Ansible

Tarefa	Descrição	Habilidades necessárias
Crie um manual do Ansible.	Para obter um exemplo de manual, consulte `ansible-rabbit-config.yaml` no anexo. Faça o download e salve esse arquivo. O manual do Ansible importa e gerencia todas as configurações do RabbitMQ, como filas, trocas e vinculações, que os aplicativos exigem. Siga as práticas recomendadas dos manuais do Ansible, como proteger senhas. Use o Ansible Vault para criptografia de senha e recupere a senha do RabbitMQ do arquivo criptografado.	Ansible

Implantar a configuração

Tarefa	Descrição	Habilidades necessárias
Execute o manual.	Execute o manual do Ansible que você criou no épico anterior. `ansible-playbook ansible-rabbit-config.yaml` Você pode verificar as novas configurações no console do RabbitMQ.	RabbitMQ, Amazon MQ, Ansible

Recursos relacionados

- Migração do RabbitMQ para o Amazon MQ (publicação no blog da AWS)
- Ferramenta de linha de comando de gerenciamento (documentação do RabbitMQ)
- Crie ou exclua uma CloudFormation pilha da AWS (documentação do Ansible)
- Migração de aplicativos orientados por mensagens para o Amazon MQ para RabbitMQ (publicação no blog da AWS)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Melhore a qualidade das chamadas nas estações de trabalho dos atendentes nas centrais de atendimento do Amazon Connect

Criado por Ernest Ozdoba (AWS)

Resumo

Os problemas de qualidade das chamadas são alguns dos problemas mais difíceis de solucionar nas centrais de atendimento. Para evitar problemas de qualidade de voz e procedimentos complexos de solução de problemas, você deve otimizar o ambiente de trabalho e as configurações da estação de trabalho de seus atendentes. Esse padrão descreve técnicas de otimização da qualidade de voz para estações de trabalho de atendentes nas centrais de atendimento do Amazon Connect. Ele fornece recomendações nas seguintes áreas:

- Ajustes no ambiente de trabalho. O ambiente dos atendentes não afeta a forma como a voz é transmitida pela rede, mas afeta a qualidade da chamada.
- Configurações da estação de trabalho do atendente. As configurações de hardware e rede para estações de trabalho de central de atendimento têm efeitos significativos na qualidade das chamadas.
- Configurações do navegador. Os atendentes usam um navegador da web para acessar o site do Amazon Connect Contact Control Panel (CCP) e se comunicar com os clientes, portanto, as configurações do navegador podem afetar a qualidade da chamada.

Os componentes a seguir também podem afetar a qualidade da chamada, mas estão fora do escopo da estação de trabalho e não são abordados nesse padrão:

- O tráfego flui para a nuvem da Amazon Web Services (AWS) por meio do AWS Direct Connect, uma VPN de túnel completo ou uma VPN de túnel dividido
- Condições de rede ao trabalhar dentro ou fora do escritório corporativo
- Conectividade de rede telefônica pública comutada (PSTN)
- O dispositivo e a operadora de telefonia do cliente
- Configuração da infraestrutura de área de trabalho virtual (VDI)

Para obter mais informações relacionadas a essas áreas, consulte Problemas comuns do Painel de Controle de Contato (CCP) e Use o Endpoint Test Utility na documentação do Amazon Connect.

Pré-requisitos e limitações

Pré-requisitos

- Os fones de ouvido e as estações de trabalho devem estar em conformidade com os requisitos especificados no Guia do administrador do Amazon Connect.

Limitações

- As técnicas de otimização desse padrão se aplicam à qualidade de voz do telefone virtual. Elas não se aplicam quando você configura o Amazon Connect CCP no modo de telefone fixo. No entanto, você pode usar o modo telefone de mesa se a configuração do seu softphone não fornecer uma qualidade de voz aceitável para a chamada.

Versões do produto

- Para ver os navegadores e versões compatíveis, consulte o Guia do administrador do Amazon Connect.

Arquitetura

Esse padrão é independente da arquitetura porque tem como alvo as configurações da estação de trabalho do atendente. Como mostra o diagrama a seguir, o caminho de voz do atendente para o cliente é afetado pelo fone de ouvido, navegador, sistema operacional, hardware da estação de trabalho e rede do atendente.

Nas centrais de contato do Amazon Connect, a conectividade de áudio do usuário é estabelecida com o WebRTC. A voz é codificada com o codec de áudio interativo Opus e criptografada com o Protocolo de Transporte Seguro em Tempo Real (SRTP) em trânsito. Outras arquiteturas de rede são possíveis, incluindo redes VPN, WAN/LAN privadas e ISP.

Ferramentas

- Amazon Connect Endpoint Test Utility: esse utilitário verifica a conectividade de rede e as configurações do navegador.
- Editores de configuração do navegador para configurações do WebRTC:
  - Para Firefox: about:config

  - Para Chrome: chrome://flags
- CCP Log Parser : essa ferramenta ajuda você a analisar os registros do CCP para fins de solução de problemas.

Épicos

Ajuste o ambiente de trabalho

Tarefa	Descrição	Habilidades necessárias
Reduza o ruído de fundo.	Evite ambientes ruidosos. Se isso não for possível, otimize o ambiente com estas dicas de isolamento acústico: • Absorva o ruído usando superfícies de dissipação de som, como cortinas, tapetes e móveis macios. • Bloqueie o ruído colocando barreiras entre as mesas. • Considere uma solução de cancelamento de ruído ativo (ANC), como um gerador de ruído branco, para ajudar na concentração e garantir a privacidade, ou use fones de ouvido com cancelamento de ruído. • Evite o eco em suas chamadas. Espaços grandes e vazios podem criar efeitos de eco ou amplificar ruídos. Cobrir superfícies que podem	Atendente e gerente

Tarefa	Descrição	Habilidades necessárias
	emitir sons ajudará a reduzir os ecos.	

Otimize as configurações da estação de trabalho do atendente

Tarefa	Descrição	Habilidades necessárias
Escolha o fone de ouvido certo.	• Se o ambiente estiver barulhento, escolha um fone de ouvido estéreo. Direcionar o som para os dois ouvidos ajuda os atendentes a se concentrarem e ouvirem melhor o cliente, além de reduzir o ruído geral, diminuindo a probabilidade de os atendentes aumentarem a voz. • Evite usar alto-falantes ou áudio embutido no computador. Para obter a melhor qualidade, use um fone de ouvido com fio dedicado ao uso na central de atendimento. Os fones de ouvido sem fio são convenientes, mas podem ser uma fonte de atraso adicional de áudio e redução da qualidade do áudio devido à interferência de rádio e à transcodificação.	Atendente e gerente

Tarefa	Descrição	Habilidades necessárias
Use o fone de ouvido conforme pretendido.	• Ative os recursos ativos de cancelamento de ruído e aprimoramento de fala do fone de ouvido, se estiverem disponíveis. Procure configurações como ANC ou ANR. Para obter instruções sobre como ativar essas configurações, consulte o manual do usuário do fone de ouvido. • Ajuste seu microfone para que você possa falar diretamente nele. A melhor posição para o microfone é logo abaixo do queixo. O posicionamento correto pode fazer uma diferença de 10 decibéis (dB) no nível do som. A maioria dos fones de ouvido permite que você gire ou dobre o braço do microfone (boom), por isso é importante mantê-lo no lugar certo quando estiver falando. • Alguns fones de ouvido são equipados com vários microfones e recursos avançados, como formação de feixe de voz, que ajuda a capturar a fala sem o boom. Para ter certeza de que você está usando	Agente

Tarefa	Descrição	Habilidades necessárias
	o microfone principal conforme pretendido pelo fabricante, consulte o manual do usuário do seu dispositivo.	
Verifique os recursos da estação de trabalho.	Certifique-se de que os computadores de seus atendentes tenham bom desempenho. Se eles usarem aplicativos de terceiros que consomem recursos, seus computadores podem não atender aos requisitos mínimos de hardware para executar o CCP. Se os atendentes tiverem problemas de qualidade de chamada, verifique se eles têm capacidade de processamento (CPU), espaço em disco, largura de banda da rede e memória suficientes disponíveis para o CCP. Os atendentes devem fechar todos os aplicativos e guias desnecessários para melhorar o desempenho do CCP e a qualidade das chamadas.	Administrador

Tarefa	Descrição	Habilidades necessárias
Defina as configurações de som do sistema operacional.	As configurações padrão para nível e aumento do microfone geralmente funcionam bem. Se você achar que a voz de saída está baixa ou o microfone está captando demais, talvez seja útil ajustar essas configurações. As configurações do microfone podem ser encontradas na configuração de som do sistema do seu computador (Som, Entrada no macOS, Propriedades do microfone no Windows). Você pode acessar configurações avançadas que podem afetar a qualidade da voz por meio de ferramentas do sistema ou aplicativos de terceiros. Aqui estão algumas das configurações que você pode verificar: • Taxa de amostragem: esse valor determina quantas vezes o som é sondado por segundo. A configuração padrão geralmente é de 44 ou 48 quilohertz (kHz). O valor ideal para o Amazon Connect é 48 kHz. Você pode usar as configurações do seu navegador para substituir o valor padrão. Para obter mais informaçõ	Atendente e administrador

Tarefa	Descrição	Habilidades necessárias
	es, consulte a seção de solução de problemas do Guia do administrador do Amazon Connect. • Ganho: esse valor determina o quanto o microfone amplifica o som. Se você aumentar o ganho, seu microfone poderá captar mais ruído de fundo. • Profundidade de bits: esse valor de resolução digital descreve quantos níveis de amplitude do som estão sendo reconhecidos. Quanto maior a profundidade de bits, mais suave será o som da voz. No entanto, muitas redes de telefonia tradicionais usam o padrão de modulação por código de pulso (PCM), que suporta apenas resolução de 8 bits. • Limite aberto: essa é a amplitude mínima do som que um microfone capta. Se você estiver enfrentando problemas de qualidade de voz, tente restaurar esses valores às configurações padrão antes de investigar mais a fundo.	

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações sobre essas e outras configurações ajustáveis, consulte o manual do seu dispositivo.	

Tarefa	Descrição	Habilidades necessárias
Use uma rede com fio.	Normalmente, a Ethernet com fio tem menor latência, por isso é mais fácil fornecer a qualidade de transmissão consistente necessária para a transmissão de dados de voz. Recomendamos, no mínimo, 100 KB de largura de banda por chamada. • Se os atendentes estiverem trabalhando em casa, recomendamos conexões com fio via wireless. Não deve levar mais de 150 milissegundos para ouvir o cliente. Você pode acessar o teste de latência do Amazon Connect a partir do Amazon Connect Endpoint Test Utility. No entanto, esse utilitário mede o atraso do navegador para as regiões do Amazon Connect, não para os clientes. A recomenda ção de atraso unidireci onal de 150 milissegundos impede que o atendente e o cliente conversem um com o outro. O valor é medido de ponta a ponta, e cada elemento adiciona um atraso, incluindo a parte da chamada entre a região	Administradores de rede, atendente

Tarefa	Descrição	Habilidades necessárias
	do Amazon Connect e o cliente. • Se os atendentes estiverem trabalhando no escritório, o Wi-Fi corporativo é aceitável, desde que os parâmetros estejam na faixa recomendada e o tráfego do Protocolo de Transporte em Tempo Real (RTP) seja priorizado.	
Atualize os drivers de hardware.	Ao usar um USB ou outro tipo de fone de ouvido que tenha seu próprio firmware, recomendamos que você o mantenha atualizado com a versão mais recente. Fones de ouvido simples que usam uma porta auxiliar usam o dispositivo de áudio integrado do computador, portanto, verifique se o driver de hardware do sistema operacional está atualizado. Em casos raros, uma atualização do driver de áudio pode causar problemas de áudio e talvez seja necessário revertê-la. Para obter mais informações sobre como alterar as versões do firmware e do driver, consulte o manual do dispositivo.	Administrador

Tarefa	Descrição	Habilidades necessárias
Evite hubs e dongles USB.	Ao conectar o fone de ouvido, evite dispositivos adicionais, como dongles, conversores de tipo de porta, hubs e cabos de extensão. Esses dispositivos podem afetar a qualidade da chamada. Em vez disso, conecte seu dispositivo diretamente à porta do seu computador.	Agente

Tarefa	Descrição	Habilidades necessárias
Verifique os logs do CCP.	O CCP Log Parser fornece uma maneira fácil de verificar os logs do aplicativo. 1. Baixe os logs do CCP após uma chamada. 2. Abra o CCP Log Parser. 3. Arraste e solte o arquivo de log para fazer o upload do log para análise. 4. Quando o log for analisado , a guia Snapshots & Logs será selecionada por padrão. Escolha a guia Métricas ao lado dela para verificar os insights. 5. Na seção Métricas da WebRTC - entrada de áudio, verifique o seguinte: • O gráfico do Nível de áudio, para ver se o nível de áudio recebido está acima de 0. Isso indica que o áudio foi recebido do seu chamador. • O gráfico de Pacotes para qualquer pacote perdido. Se esse gráfico mostrar aumentos significativos, entre em contato com sua equipe de suporte de TI.	Atendente (habilidades avançadas)

Tarefa	Descrição	Habilidades necessárias
	6. Na seção Métricas da WebRTC - saída de áudio, verifique o seguinte: • O gráfico do Nível de áudio, para confirmar que o áudio foi enviado do seu dispositivo. • O gráfico de Pacotes. Se você observar um pico de perda de pacotes, comunique-o à sua equipe de suporte de TI. • O gráfico de Buffer de instabilidade e RTT. Valores de tempo de ida e volta (RTT) acima de 300 afetarão a experiênc ia da chamada. Relate essas informações à sua equipe de suporte de TI.	

Para otimizar as configurações do navegador

Tarefa	Descrição	Habilidades necessárias
Restaurar configurações padrão do WebRTC.	O WebRTC deve estar habilitado para fazer chamadas telefônicas flexíveis com o CCP. Recomenda mos que você mantenha as configurações padrão dos recursos relacionados ao WebRTC.	Administrador

Tarefa	Descrição	Habilidades necessárias
	• No Chrome, você pode definir sinalizadores navegando até o URL chrome://flags. Digite WebRTC na caixa de pesquisa para encontrar configurações que possam interferir com o CCP e defina-as como Padrão. • No Firefox, digite about:config na barra de endereço e, em seguida, digite WebRTC na caixa de pesquisa da página de configuração. As configurações não padrão aparecem em negrito e podem ser alteradas para Padrão.	
Desative as extensões do navegador ao solucionar problemas.	Algumas extensões do navegador podem afetar a qualidade das chamadas ou até mesmo impedir que as chamadas se conectem corretamente. Use a janela anônima ou o modo privado em seu navegador e desative todas as extensões. Se isso resolver o problema, revise as extensões do seu navegador e procure complementos suspeitos ou desative-os individualmente.	Atendente e administrador

Tarefa	Descrição	Habilidades necessárias
Verifique a taxa de amostragem do navegador.	Confirme se a entrada do microfone está configurada para a taxa de amostragem ideal de 48 kHz. Para obter instruções, consulte o Guia do administrador do Amazon Connect.	Atendente e administrador

Recursos relacionados

Se você seguiu as etapas desse padrão, mas ainda está enfrentando problemas com a qualidade da chamada, consulte os recursos a seguir para obter dicas de solução de problemas.

- Analise os problemas comuns do Painel de Controle de Contato (CCP).
- Verifique a conexão com o Endpoint Test Utility.
- Siga o guia de solução de problemas para outros problemas.

Se a solução de problemas e os ajustes não resolverem o problema de qualidade da chamada, a causa raiz pode ser externa à sua estação de trabalho. Para solucionar problemas adicionais, entre em contato com sua equipe de suporte de TI.

Mais padrões

- Decomponha monólitos em microsserviços usando o CQRS e o fornecimento de eventos
- Implemente uma ChatOps solução para gerenciar os resultados do escaneamento SAST usando o Amazon Q Developer em aplicativos de bate-papo, ações personalizadas e AWS CloudFormation
- Integre o Amazon API Gateway com o Amazon SQS para lidar com REST assíncrono APIs
- Registrar várias contas da AWS com um único endereço de e-mail usando o Amazon SES
- Executar workloads orientadas por mensagens em grande escala usando o AWS Fargate
- Simplifique o desenvolvimento e a implantação de bots do Amazon Lex usando um fluxo de trabalho automatizado

Segurança, identidade e conformidade

Tópicos

- Acesso Serviços da AWS a partir de um aplicativo ASP.NET Core usando grupos de identidade do Amazon Cognito
- Autentique o Microsoft SQL Server na Amazon EC2 usando o AWS Directory Service
- Automatize a resposta a incidentes e forense
- Automatize a remediação para descobertas padrão AWS Security Hub
- Automatize as verificações de segurança para cargas de trabalho entre contas usando o Amazon Inspector e AWS Security Hub
- Audite automaticamente grupos AWS de segurança que permitem acesso a partir de endereços IP públicos
- Reative automaticamente a AWS CloudTrail usando uma regra de remediação personalizada no AWS Config
- Corrija automaticamente instâncias e clusters de banco de dados Amazon RDS não criptografados
- Alterne automaticamente as chaves de acesso do usuário do IAM em grande escala com o AWS Organizations e o AWS Secrets Manager
- Valide e implante automaticamente políticas e funções do IAM em uma conta da AWS usando o CodePipeline IAM Access Analyzer e macros da AWS CloudFormation
- Integre bidirecionalmente AWS Security Hub com o software Jira
- Crie um pipeline para imagens de contêiner reforçadas usando o EC2 Image Builder e o Terraform
- Centralize o gerenciamento de chaves de acesso do IAM no AWS Organizations usando o Terraform
- Verifique a versão de registro de acesso, HTTPS e TLS em uma CloudFront distribuição da Amazon
- Verifique as entradas de rede de host único nas regras de entrada do grupo de segurança para e IPv4 IPv6
- Escolha um fluxo de autenticação do Amazon Cognito para aplicativos corporativos
- Crie regras AWS Config personalizadas usando AWS CloudFormation Guard políticas
- Crie um relatório consolidado das descobertas de segurança da Prowler a partir de vários Contas da AWS
- Exclua volumes não utilizados do Amazon EBS usando e AWS ConfigAWS Systems Manager

- Implemente e gerencie AWS Control Tower controles usando AWS CDK e CloudFormation
- Implemente e gerencie AWS Control Tower controles usando o Terraform
- Implemente um pipeline que detecte simultaneamente problemas de segurança em vários produtos de código
- Implemente controles de acesso baseados em atributos de detetive para sub-redes públicas usando AWS Config
- Implemente controles de acesso preventivos baseados em atributos para sub-redes públicas
- Implemente as automações de segurança para a AWS WAF solução usando o Terraform
- Detecte instâncias de banco de dados Amazon RDS e Aurora que têm certificados CA expirados
- Gere dinamicamente uma política do IAM com o IAM Access Analyzer usando Step Functions
- Habilite a Amazon GuardDuty condicionalmente usando modelos AWS CloudFormation
- Suporte para criptografia de dados transparente no Amazon RDS para SQL Server
- Garanta que os balanceadores de carga da AWS usem protocolos receptores seguros (HTTPS, SSL/TLS)
- Garanta que a criptografia para dados em repouso do Amazon EMR esteja habilitada no lançamento
- Certifique-se de que um perfil do IAM esteja associado a uma EC2 instância
- Garanta que um cluster do Amazon Redshift seja criptografado na criação
- Exporte um relatório das identidades do AWS IAM Identity Center e suas atribuições usando PowerShell
- Monitorar e corrigir a exclusão programada das chaves do AWS KMS
- Identifique buckets públicos do Amazon S3 usando o Security AWS Organizations Hub
- Ingira e analise os registros de segurança da AWS no Microsoft Sentinel
- Gerencie AWS Organizations políticas como código usando o AWS CodePipeline Amazon Bedrock
- Gerencie conjuntos de AWS IAM Identity Center permissões como código usando AWS CodePipeline
- Gerenciar credenciais usando o AWS Secrets Manager
- Monitore ElastiCache clusters para grupos de segurança
- Monitorar clusters do Amazon EMR para criptografia em trânsito na execução
- Monitore ElastiCache clusters da Amazon para criptografia em repouso
- Monitore pares de chaves de EC2 instância usando o AWS Config

- Monitorar a atividade do usuário raiz do IAM
- Enviar uma notificação quando um usuário do IAM for criado
- Impeça o acesso à Internet no nível da conta usando uma política de controle de serviços
- Restrinja o acesso com base no endereço IP ou geolocalização usando AWS WAF
- Examine os repositórios Git em busca de informações confidenciais e problemas de segurança usando git-secrets
- Envie alertas do AWS Network Firewall para um canal do Slack
- Simplificar o gerenciamento de certificados privados usando a CA privada da AWS e o AWS RAM
- Desative os controles padrão de segurança em todas as contas de membros do Security Hub em um ambiente com várias contas
- Atualize as credenciais da AWS CLI do AWS IAM Identity Center usando PowerShell
- Use o AWS Config para monitorar as configurações de segurança do Amazon Redshift
- Use o Network Firewall para capturar os nomes de domínio DNS da Indicação de Nome do Servidor para tráfego de saída
- Use o Terraform para habilitar automaticamente a Amazon GuardDuty para uma organização
- Verifique as melhores práticas operacionais para o PCI DSS 4.0 usando AWS Config
- Verificar se os novos clusters do Amazon Redshift têm os endpoints SSL necessários
- Verificar se os novos clusters do Amazon Redshift são executados em uma VPC
- Mais padrões

Acesso Serviços da AWS a partir de um aplicativo ASP.NET Core usando grupos de identidade do Amazon Cognito

Criado por Bibhuti Sahu (AWS) e Marcelo Barbosa (AWS)

Resumo

Esse padrão discute como você pode configurar grupos de usuários e grupos de identidades do Amazon Cognito e, em seguida, habilitar um aplicativo ASP.NET Core para AWS acessar recursos após a autenticação bem-sucedida.

O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para aplicativos web e móveis. Os dois principais componentes do Amazon Cognito são grupos de usuários e bancos de identidades.

Grupo de usuários é um diretório de usuários no Amazon Cognito. Com um grupo de usuários, seus usuários podem fazer login em aplicações Web ou móveis por meio do Amazon Cognito. Os usuários também podem fazer login por meio de provedores de identidade social, como o Google, o Facebook, a Amazon ou a Apple, e por meio de provedores de identidade SAML.

Os grupos de identidades do Amazon Cognito (identidades federadas) permitem a criação de identidades exclusivas para os usuários e federá-las com provedores de identidade. Com um pool de identidades, você pode obter AWS credenciais temporárias com privilégios limitados para acessar outras. Serviços da AWS Antes de começar a usar seu novo pool de identidade do Amazon Cognito, você deve atribuir uma ou mais funções AWS Identity and Access Management (IAM) para determinar o nível de acesso que você deseja que os usuários do aplicativo tenham aos seus AWS recursos. Os grupos de identidades definem dois tipos de identidades: autenticadas e não autenticadas. Cada tipo de identidade pode ter sua própria função no IAM. As identidades autenticadas pertencem aos usuários que serão autenticados por um provedor de login público (grupos de usuários do Amazon Cognito, Facebook, Google, SAML ou qualquer provedor do OpenID Connect) ou um provedor de desenvolvedor (seu próprio processo de autenticação de backend), enquanto identidades não autenticadas geralmente pertencem a usuários convidados. Quando o Amazon Cognito recebe uma solicitação do usuário, o serviço determina se a solicitação é autenticada ou não, determina qual perfil está associado com esse tipo de autenticação e, então, usa a política anexada a essa função para responder à solicitação.

Pré-requisitos e limitações

Pré-requisitos

- E Conta da AWS com permissões Amazon Cognito e IAM
- Acesso aos AWS recursos que você deseja usar
- ASP.NET Core 2.0.0 ou superior

Arquitetura

Pilha de tecnologia

- Amazon Cognito
- ASP.NET Core

Arquitetura de destino

Ferramentas

Ferramentas SDKs, e Serviços da AWS

- Visual Studio ou Visual Studio Code
- Amazon. AspNetCore.Identity.Cognito (1.0.4) — pacote NuGet
- AWSSDK.S3 (3.3.110.32) — pacote NuGet
- Amazon Cognito

Código

O arquivo .zip anexado inclui arquivos de amostra que ilustram:

- Como recuperar um token de acesso para o usuário conectado
- Como trocar um token de acesso por AWS credenciais
- Como acessar o serviço Amazon Simple Storage Service (Amazon S3) com credenciais AWS

Função do IAM para identidades autenticadas

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

```
    {
      "Effect": "Allow",
      "Action": [
        "mobileanalytics:PutEvents",
        "cognito-sync:*",
        "cognito-identity:*",
        "s3:ListAllMyBuckets*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Épicos

Criar um grupo de usuários do Amazon Cognito

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de usuários.	1. Faça login no AWS Management Console e abra o console do Amazon Cognito. 2. Selecione Manage User Pools. 3. No canto superior direito da página, selecione Criar um grupo de usuários. 4. Forneça um nome para seu grupo de usuários, escolha Revisar padrões e, em seguida, escolha Criar grupo. 5. Observe o ID do grupo.	Desenvolvedor
Adicione um cliente de aplicativo.	Você pode criar um aplicativo para usar as páginas da Web	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	integradas a fim de fazer login e cadastro de seus usuários. 1. Na barra de navegação no lado esquerdo da página de grupo de usuários, escolha Clientes do aplicativo em Configurações gerais, depois escolha Adicionar um cliente do aplicativo. 2. Dê um nome para o aplicativo e escolha Criar cliente do aplicativo. 3. Anote a ID do cliente do aplicativo e o segredo do cliente (escolha Mostrar detalhes para ver o segredo do cliente).	

Como criar um grupo de identidades do Amazon Cognito

Tarefa	Descrição	Habilidades necessárias
Crie um banco de identidades do.	1. No console do Amazon Cognito, escolha Gerenciar bancos de identidades e, em seguida, escolha Criar novo banco de identidades. 2. Digite um nome para o banco de identidades. 3. Se você quiser ativar identidades não autentica das, selecione essa opção	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	na seção Identidades não autenticadas. 4. Na seção Provedores de autenticação, configure o pool de identidade do Amazon Cognito definindo o ID do grupo de usuários e o ID do cliente do aplicativo e, em seguida, escolha Create Pool.	
Atribua perfis do IAM para o banco de identidades.	Você pode editar os perfis do IAM para usuários autenticados e não autenticados ou manter os padrões e escolher Permitir. Para esse padrão, editaremos o perfil do IAM autenticado e forneceremos acesso para `s3:ListAllMyBuckets`. Para ver um exemplo de código, consulte o perfil do IAM fornecida anteriormente na seção Ferramentas.	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
Copie o ID do banco de identidades.	Quando você escolhe Permitir na etapa anterior, a página Conceitos básicos do Amazon Cognito é exibida. Nessa página, você pode copiar o ID do banco de identidades da seção Obter credenciais da AWS ou escolher Editar banco de identidades no canto superior direito e copiar a ID do grupo de identidades da tela exibida.	Desenvolvedor

Configure seu aplicativo de amostra

Tarefa	Descrição	Habilidades necessárias
Clone o aplicativo web ASP.NET de amostra.	1. Clone a amostra do aplicativo web.NET core em https://github.com/aws/aws-aspnet-cognito-identity-provider.git. 2. Navegue até a pasta `samples` e abra a solução. Neste projeto, você configurará o arquivo `appsettings.json` e adicionará uma nova página que renderizará todos os buckets do S3 após o login bem-sucedido.	Desenvolvedor
Adicione dependências.	Adicione uma NuGet dependência `Amazon.As`	Desenvolvedor

Tarefa	Descrição	Habilidades necessárias
	pNetCore.Identity.Cognito para seu aplicativo ASP.NET Core.	
Adicione as chaves e os valores de configuração appsettings.json a.	Inclua o código do arquivo appsettings.json anexado em seu arquivo appsettings.json e, em seguida, substitua os espaços reservados pelos valores das etapas anteriores.	Desenvolvedor
Crie um novo usuário e faça login.	Crie um novo usuário no grupo de usuários do Amazon Cognito e verifique se o usuário existe em Usuários e grupos no grupo de usuários.	Desenvolvedor
Crie uma nova página do Razor chamadaMyS3Buckets .	Adicione uma nova página Razor Page ASP.NET Core ao seu aplicativo de amostra e substitua o conteúdo por MyS3Bucket.cshtml e MyS3Bucket.cshtml.cs da amostra anexada. Adicione a nova página MyS3Bucket em navegação, na página_Layout.cshtml .	Desenvolvedor

Solução de problemas

Problema	Solução
Depois de abrir o aplicativo de amostra no GitHub repositório, você recebe um erro ao	Na pasta src, certifique-se de remover a referência ao projeto Amazon.AspNetCore.

Problema	Solução
tentar adicionar o NuGet pacote ao projeto Samples.	`Identity.Cognito` do arquivo`Samples.sln` . Em seguida, você pode adicionar o NuGet pacote ao projeto Samples sem problemas.

Recursos relacionados

- Amazon Cognito
- Grupos de usuários do Amazon Cognito
- Bancos de identidades do Amazon Cognito
- Exemplos de políticas de acesso
- GitHub - Provedor de Identidade Cognito AWS ASP.NET

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Autentique o Microsoft SQL Server na Amazon EC2 usando o AWS Directory Service

Criado por Jagadish Kantubugata (AWS) e Oludahun Bade Ajidahun (AWS)

Resumo

Esse padrão descreve como criar um diretório do AWS Directory Service e usá-lo para autenticar o Microsoft SQL Server em uma instância do Amazon Elastic Compute Cloud EC2 (Amazon).

O AWS Directory Service oferece várias formas de usar o Amazon Cloud Directory e o Microsoft Active Directory (AD) com outros serviços da AWS. Os diretórios armazenam informações sobre usuários, grupos e dispositivos, e os administradores os utilizam para gerenciar o acesso a informações e recursos. O AWS Directory Service fornece várias opções de diretórios para quem quiser usar seus aplicativos existentes habilitados para Microsoft AD ou Lightweight Directory Access Protocol (LDAP) na nuvem. Ele também oferece essas mesmas opções para os desenvolvedores que precisam de um diretório para gerenciar usuários, grupos, dispositivos e acesso.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) com no mínimo duas sub-redes privadas e duas sub-redes públicas
- Um perfil do AWS Identity and Access Management (IAM) para unir o servidor ao domínio

Arquitetura

Pilha de tecnologia de origem

- A origem pode ser um Active Directory on-premises

Pilha de tecnologias de destino

- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)

Arquitetura de destino

Ferramentas

- O Microsoft SQL Server Management Studio (SSMS) é uma ferramenta para gerenciar o SQL Server, incluindo acesso, configuração e administração de componentes do SQL Server.

Épicos

Configurar um diretório

Tarefa	Descrição	Habilidades necessárias
Escolha o ID do diretório do Microsoft Managed AD.	No console do AWS Directory Service, escolha Diretórios, Configurar diretório, AWS Managed Microsoft AD e Avançar.	DevOps
Selecione a edição.	Nas edições disponíveis para o AWS Managed Microsoft AD, escolha Standard Edition.	DevOps
Especifique o nome DNS do diretório.	Nome para usar para nomes de domínio totalmente qualificados. Esse nome será resolvido apenas dentro de sua VPC. Ele não precisa ser resolvido publicamente.	DevOps
Defina a senha de administrador.	Defina a senha do usuário administrativo padrão denominado Admin.	DevOps
Escolha a VPC e as sub-redes.	Escolha a VPC que conterá seu diretório e as sub-redes dos controladores de domínio.	DevOps

Tarefa	Descrição	Habilidades necessárias
	Se você não tiver uma VPC com ao menos duas sub-redes, será preciso criar uma.	
Revise e crie o diretório.	Revise as informações de edição e preço do diretório e escolha Criar diretório.	DevOps

Execute uma EC2 instância para o SQL Server no domínio

Tarefa	Descrição	Habilidades necessárias
Selecione uma AMI para o SQL Server.	As etapas desse épico unem perfeitamente uma EC2 instância do Windows ao seu diretório AWS Managed Microsoft AD. No EC2 console da Amazon, escolha Launch instance e, em seguida, selecione a Amazon Machine Image (AMI) apropriada para o SQL Server.	DevOps, DBA
Configure os detalhes da instância.	Configure a instância do Windows para atender aos seus requisitos do SQL Server.	DevOps, DBA
Selecione o nome do par de chaves.	Selecione um par de chaves e, em seguida, execute a instância.	DevOps, DBA

Tarefa	Descrição	Habilidades necessárias
Adicione uma rede.	Você pode selecionar a VPC em que seu diretório foi criado.	DevOps, DBA
Selecione um perfil do IAM.	Em Configurações avançadas, selecione um perfil do IAM que tenha as políticas gerenciadas pela AWS `AmazonSSMManagedInstanceCore` e `AmazonSSMDirectoryServiceAccess`, anexadas a ele.	DevOps, DBA
Adicionar uma sub-rede.	Selecione uma das sub-redes públicas na sua VPC. Todo o tráfego externo da sub-rede selecionada deve ser roteado para um gateway da Internet. Caso contrário, não será possível conectar-se à instância de maneira remota.	DevOps, DBA
Escolha o seu domínio.	Escolha o domínio que você criou da lista do diretório Associar ao domínio.	DevOps, DBA
Iniciar a instância.	Escolha Iniciar instância.	DBA

Autenticar o SQL Server usando o Directory Service

Tarefa	Descrição	Habilidades necessárias
Faça login como administrador do Windows.	Faça login na EC2 instância do Windows usando as	DBA

Tarefa	Descrição	Habilidades necessárias
	credenciais de administrador do Windows.	
Faça login no SQL Server.	Inicie o SQL Server Management Studio (SSMS) e faça login no SQL Server usando o método de autentica ção do Windows.	DBA
Crie um login para o usuário do diretório.	No SSMS, escolha Segurança e, em seguida, Novo login.	DBA
Pesquise um nome de login.	Escolha o botão de pesquisa ao lado da caixa de texto de login.	DBA
Selecione um local.	Na caixa de diálogo Seleciona r usuário ou grupo, escolha Locais.	DBA
Insira credenciais de rede.	Insira as credenciais de rede totalmente qualificadas que você usou ao criar o serviço de diretório; por exemplo: `test.com\admin` .	DBA
Selecione o diretório.	Escolha o nome do diretório AWS e escolha OK.	DBA
Selecione um nome de objeto.	Selecione o usuário para o qual você deseja criar o login. Selecione o local, escolha o diretório inteiro, pesquise o usuário e adicione o login.	DBA

Tarefa	Descrição	Habilidades necessárias
Faça login na instância do SQL Server.	Faça login na EC2 instância do Windows para SQL Server usando suas credenciais de domínio.	DBA
Faça login no SQL Server como usuário do domínio.	Inicie o SSMS e conecte-se ao mecanismo de banco de dados usando o método de autenticação do Windows.	DBA

Recursos relacionados

- Documentação do AWS Directory Service (site da AWS)
- Crie seu diretório do AWS Managed Microsoft AD (documentação do AWS Directory Service)
- Participe facilmente de uma EC2 instância do Windows (documentação do AWS Directory Service)
- Microsoft SQL Server na AWS (site do AWS)
- Documentação do SSMS (site da Microsoft)
- Crie um login no SQL Server (documentação do SQL Server)

Automatize a resposta a incidentes e forense

Criado por Lucas Kauffman (AWS) e Tomek Jakubowski (AWS)

Resumo

Esse padrão implanta um conjunto de processos que usam AWS Lambda funções para fornecer o seguinte:

- Uma forma de iniciar o processo de resposta a incidentes com o mínimo de conhecimento
- Processos automatizados e repetíveis que estão alinhados com o Guia de Resposta a Incidentes AWS de Segurança
- Separação de contas para operar as etapas de automação, armazenar artefatos e criar ambientes forenses

A estrutura de resposta automatizada a incidentes e forense segue um processo forense digital padrão que consiste nas seguintes fases:

1. Contenção
2. Aquisição
3. Examinação
4. Análise

Você pode realizar investigações em dados estáticos (por exemplo, memória adquirida ou imagens de disco) e em dados dinâmicos ativos, mas em sistemas separados.

Para obter detalhes, consulte a seção Informações adicionais.

Pré-requisitos e limitações

Pré-requisitos

- Dois Contas da AWS:
  - Conta de segurança, que pode ser uma conta existente, mas é de preferência nova
  - Conta forense, de preferência nova
- AWS Organizations configurar
- Nas contas dos membros da Organizações:

  - A função Amazon Elastic Compute Cloud (Amazon EC2) deve ter acesso Get and List ao Amazon Simple Storage Service (Amazon S3) e estar acessível por. AWS Systems Manager Recomendamos usar a função `AmazonSSMManagedInstanceCore` AWS gerenciada. Observe que essa função será automaticamente anexada à EC2 instância da Amazon quando a resposta ao incidente for iniciada. Depois que a resposta for concluída, o AWS Identity and Access Management (IAM) removerá todos os direitos da instância.
  - Endpoints de nuvem privada virtual (VPC) na conta do AWS membro e na resposta e análise de incidentes. VPCs Esses endpoints são: S3 Gateway, EC2 Mensagens, SSM e Mensagens SSM.
- AWS Command Line Interface (AWS CLI) instalado nas EC2 instâncias da Amazon. Se as EC2 instâncias da Amazon não estiverem AWS CLI instaladas, será necessário acesso à Internet para que o instantâneo do disco e a aquisição de memória funcionem. Nesse caso, os scripts entrarão em contato com a Internet para baixar os arquivos de AWS CLI instalação e os instalarão nas instâncias.

Limitações

- Essa estrutura não pretende gerar artefatos que possam ser considerados evidências eletrônicas, submissíveis em juízo.
- Atualmente, esse padrão é compatível somente a instâncias baseadas em Linux executadas na arquitetura x86.

Arquitetura

Arquitetura de destino

Além da conta do membro, o ambiente de destino consiste em duas contas principais: uma conta de segurança e uma conta forense. Duas contas são usadas pelos seguintes motivos:

- Para separá-las de quaisquer outras contas de clientes para reduzir o raio de explosão em caso de falha na análise forense
- Para ajudar a garantir o isolamento e a proteção da integridade dos artefatos que estão sendo analisados
- Para manter a investigação confidencial
- Para evitar situações em que os agentes da ameaça possam ter usado todos os recursos imediatamente disponíveis para você, Conta da AWS atingindo as cotas de serviço e impedindo que você instancie uma instância da EC2 Amazon para realizar investigações.

Além disso, ter contas de segurança e forense separadas permite a criação de perfis separados: uma Respondente para adquirir evidências e um Investigador para analisá-las. Cada perfil teria acesso a própria conta separada.

O diagrama a seguir mostra somente a interação entre as contas. Os detalhes de cada conta são mostrados nos diagramas subsequentes e um diagrama completo é anexado.

O diagrama a seguir mostra a conta do membro.

1. Um evento é enviado para o tópico Amazon Simple Notification Service (Amazon SNS) do Slack.

O diagrama a seguir mostra a conta de segurança.

2. O tópico do Amazon SNS na conta de segurança inicia eventos forenses.

O diagrama a seguir mostra a conta Forensics.

A conta de segurança é onde os dois AWS Step Functions fluxos de trabalho principais são criados para aquisição de memória e imagem de disco. Depois que os fluxos de trabalho são executados, eles acessam a conta membro que tem as EC2 instâncias da Amazon envolvidas em um incidente e iniciam um conjunto de funções do Lambda que reunirão um despejo de memória ou um despejo de disco. Esses artefatos são então armazenados na conta forense.

A conta Forensics armazenará os artefatos coletados pelo fluxo de trabalho Step Functions no bucket Amazon S3 de artefatos de análise. A conta Forensics também terá um pipeline do Amazon EC2 Image Builder que cria uma Amazon Machine Image (AMI) de uma instância forense. Atualmente, a imagem é baseada na estação de trabalho SANS SIFT.

O processo de compilação usa a VPC de manutenção, que tem conectividade com a Internet. Posteriormente, a imagem pode ser usada para ativar a EC2 instância da Amazon para análise dos artefatos coletados na VPC de Análise.

A Analysis VPC não tem conectividade à internet. Por padrão, o padrão cria três sub-redes de análise privadas. Você pode criar até 200 sub-redes, que é a cota para o número de sub-redes em uma VPC, mas os VPC endpoints precisam ter essas sub-redes adicionadas para automatizar a execução de comandos nelas. AWS Systems Manager Session Manager

Do ponto de vista das melhores práticas, recomendamos usar AWS CloudTrail e AWS Config fazer o seguinte:

- Rastrear as alterações feitas em sua conta forense
- Monitorar o acesso e a integridade dos artefatos que são armazenados e analisados

Fluxo de trabalho

O diagrama a seguir mostra as principais etapas de um fluxo de trabalho que inclui o processo e a árvore de decisão desde o momento em que uma instância é comprometida até ser analisada e contida.

1. A tag `SecurityIncidentStatus` foi definida com o valor Analyze? Em caso positivo, faça o seguinte:
   a. Anexe os perfis IAM corretos para AWS Systems Manager o Amazon S3.
   b. Envie uma mensagem do Amazon SNS para a fila do Amazon SNS no Slack.
   c. Envie uma mensagem do Amazon SNS para a fila `SecurityIncident`.
   d. Invoque a máquina de estado de aquisição de memória e disco.
2. A memória e o disco foram adquiridos? Se não foram, há um erro.
3. Marque a EC2 instância da Amazon com a `Contain` tag.
4. Anexe o perfil do IAM e o grupo de segurança para isolar totalmente a instância.

Automação e escala

A intenção desse padrão é fornecer uma solução escalável para realizar a resposta a incidentes e a análise forense em várias contas em uma única organização. AWS Organizations

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto para interagir por Serviços da AWS meio de comandos em seu shell de linha de comando.

- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS. Também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala.

Código

Para obter o código e as diretrizes específicas de implementação e uso, consulte o repositório do GitHub Automated Incident Response and Forensics Framework.

Épicos

Implante os CloudFormation modelos

Tarefa	Descrição	Habilidades necessárias
Implante CloudFormation modelos.	Os CloudFormation modelos são marcados de 1 a 7 com	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	a primeira palavra do nome do script indicando em qual conta o modelo precisa ser implantado. Observe que a ordem de lançamento dos CloudFormation modelos é importante. • `1-forensic-AnalysisVPCnS3Buckets.yaml` : implantado na conta forense. Ele cria os buckets do Amazon S3 e a VPC de análise e é ativado. CloudTrail • `2-forensic-MaintenanceVPCnEC2ImageBuilderPipeline.yaml` : implanta o pipeline de manutenção da VPC e do construtor de imagens com base no SANS SIFT. • `3-security_IR-Disk_Mem_automation.yaml` : implanta as funções na conta de segurança que permitem a aquisição de disco e memória. • `4-security_LiME_Volatility_Factory.yaml` : inicia uma função de construção para começar a criar os módulos de memória com base na AMI	

Tarefa	Descrição	Habilidades necessárias
	IDs fornecida. Observe que IDs as AMI são diferentes Regiões da AWS. Sempre que precisar de novos módulos de memória, você pode executar novamente esse script com a nova AMI. IDs Considere integrá-lo aos seus pipelines dourados do AMI Builder (se usado em seu ambiente). • `5-member-IR-automation.yaml` : cria a função de automação de resposta a incidentes do membro, que inicia o processo de resposta a incidentes. Ele permite compartilhar volumes do Amazon Elastic Block Store (Amazon EBS) entre contas, publicar automaticamente nos canais do Slack durante o processo de resposta a incidentes, iniciar o processo forense e isolar as instâncias após a conclusão do processo. • `6-forensic-artifact-s3-policies.yaml` : após a implantação de todos os scripts, esse script corrige as permissões	

Tarefa	Descrição	Habilidades necessárias
	s necessárias para todas as interações entre contas. • `7-security-IR-vpc.yaml` : configura uma VPC usada para processamento do volume de resposta a incidentes. Para iniciar a estrutura de resposta a incidentes para uma EC2 instância específica da Amazon, crie uma tag com a chave `SecurityIncidentStatus` e o valor`Analyze`. Isso inicializará a função do Lambda do membro, que iniciará automaticamente o isolamento e a memória, bem como a aquisição de disco.	
Opere a estrutura.	A função do Lambda também remarcará o ativo no final (ou em caso de falha) com `Contain`. Isso inicia a contenção, que isola totalmente a instância com um grupo de segurança sem ENTRADA/SAÍDA e com um perfil do IAM que proíbe todo o acesso. Siga as etapas no GitHub repositório.	Administrador da AWS

Implemente ações personalizadas do Security Hub

Tarefa	Descrição	Habilidades necessárias
Implante as ações personalizadas do Security Hub usando um CloudFormation modelo.	Para criar uma ação personalizada para que você possa usar a lista suspensa do Security Hub, implante o `Modules/SecurityHub Custom Actions/SecurityHubCustomActions.yaml` CloudFormation modelo. Em seguida, modifique o perfil `IRAutomation` em cada uma das contas dos membros para permitir que a função do Lambda que executa a ação assuma o perfil `IRAutomation`. Para obter mais informações, consulte o GitHub repositório.	Administrador da AWS

Recursos relacionados

- AWS Guia de resposta a incidentes de segurança

Mais informações

Ao usar esse ambiente, uma equipe do Centro de operações de segurança (Security Operations Center, SOC) pode melhorar o processo de resposta a incidentes de segurança ao:

- Ter a capacidade de realizar forenses em um ambiente segregado para evitar o comprometimento acidental dos recursos de produção
- Ter um processo padronizado, repetível e automatizado para fazer contenção e análise.

- Dar a qualquer proprietário ou administrador da conta a capacidade de iniciar o processo de resposta a incidentes com o mínimo de conhecimento de como usar tags
- Ter um ambiente padronizado e limpo para realizar análises de incidentes e forenses sem o ruído de um ambiente maior
- Ter a capacidade de criar vários ambientes de análise em paralelo
- Foco nos recursos do SOC na resposta a incidentes em vez de na manutenção e documentação de um ambiente forense em nuvem
- Substituição de um processo manual para um automatizado para obter escalabilidade
- Usando CloudFormation modelos para obter consistência e evitar tarefas repetíveis

Além disso, você evita usar uma infraestrutura persistente e paga pelos recursos quando precisa deles.

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Automatize a remediação para descobertas padrão AWS Security Hub

Criado por Chandini Penmetsa (AWS) e Aromal Raj Jayarajan (AWS)

Resumo

Com AWS Security Hub, você pode habilitar verificações de melhores práticas padrão, como as seguintes:

- AWS Melhores práticas básicas de segurança
- Referência do CIS AWS Foundations
- Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)

Cada um desses padrões tem controles predefinidos. O Security Hub verifica o controle em um dado Conta da AWS e relata as descobertas.

AWS Security Hub envia todas as descobertas para a Amazon EventBridge por padrão. Esse padrão fornece um controle de segurança que implanta uma EventBridge regra para identificar as descobertas padrão das Melhores AWS Práticas de Segurança Fundamental. A regra identifica as seguintes descobertas para escalabilidade automática, nuvens privadas virtuais (VPCs), Amazon Elastic Block Store (Amazon EBS) e Amazon Relational Database Service (Amazon RDS) do padrão Foundational Security Best Practices: AWS

- [AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do balanceador de carga
- [EC2.2] O grupo de segurança padrão da VPC não deve permitir tráfego de entrada e saída
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todos VPCs
- [EC2.7] A criptografia padrão do EBS deve estar ativada
- [RDS.1] Os snapshots do RDS devem ser privados
- [RDS.6] O monitoramento aprimorado deve ser configurado para instâncias e clusters de banco de dados do RDS
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada

A EventBridge regra encaminha essas descobertas para uma AWS Lambda função, que corrige a descoberta. A função do Lambda então envia uma notificação com informações de remediação para um tópico do Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um endereço de e-mail no qual você deseja receber a notificação de remediação
- Security Hub e AWS Config habilitado no Região da AWS local em que você pretende implantar o controle
- Um bucket do Amazon Simple Storage Service (Amazon S3) na mesma região do controle para carregar o código AWS Lambda

Limitações

- Esse controle de segurança corrige automaticamente as novas descobertas relatadas após a implantação do controle de segurança. Para corrigir as descobertas existentes, selecione as descobertas manualmente no console do Security Hub. Em seguida, em Ações, selecione a ação AFSBPRemedypersonalizada que foi criada como parte da implantação por AWS CloudFormation.
- Esse controle de segurança é regional e deve ser implantado no local Regiões da AWS que você pretende monitorar.
- Para a solução EC2 6.6, para habilitar os VPC Flow Logs, um grupo de logs do CloudWatch Amazon Logs será criado `/VpcFlowLogs/vpc_id` com o formato. Se existir um grupo de logs com o mesmo nome, o grupo de logs existente será usado.
- Para a solução EC2 7.7, para habilitar a criptografia padrão do Amazon EBS, a chave default AWS Key Management Service (AWS KMS) é usada. Essa alteração impede o uso de determinadas instâncias que não são compatíveis com a criptografia.

Arquitetura

Pilha de tecnologias de destino

- Função do Lambda
- Tópico do Amazon SNS

- EventBridge regra
- AWS Identity and Access Management Funções (IAM) para a função Lambda, VPC Flow Logs e Amazon RDS Enhanced Monitoring

Arquitetura de destino

Automação e escala

Se você estiver usando AWS Organizations, você pode usar AWS CloudFormation StackSetspara implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

- AWS CloudFormationé um serviço que ajuda você a modelar e configurar AWS recursos usando a infraestrutura como código.
- EventBridgeA Amazon fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos de software como serviço (SaaS) e Serviços da AWS roteia esses dados para destinos como funções Lambda.
- AWS Lambdasuporta a execução de código sem provisionar ou gerenciar servidores.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que você pode usar para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- O Amazon Simple Notification Service (Amazon SNS) coordena e gerencia a entrega ou o envio de mensagens entre editores e clientes, incluindo servidores web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Práticas recomendadas

- Nove AWS Security Hub melhores práticas
- AWS Padrão básico de melhores práticas de segurança

Épicos

Implemente o controle de segurança

Tarefa	Descrição	Habilidades necessárias
Defina o bucket do Amazon S3.	No console do Amazon S3, escolha ou crie um bucket do Amazon S3 com um nome exclusivo que não contenha barras iniciais. O nome de um bucket do Amazon S3 é globalmente exclusivo e o namespace é compartil hado por todos. Contas da AWS Seu bucket do Amazon S3 deve estar na mesma região das descobertas do Security Hub que estão sendo avaliadas.	Arquiteto de nuvem
Faça o upload do código Lambda para o bucket do Amazon S3.	Faça o upload do arquivo.zip do código Lambda fornecido na seção “Anexos” para o bucket definido do Amazon S3.	Arquiteto de nuvem
Implante o AWS CloudForm ation modelo.	Implante o AWS CloudForm ation modelo fornecido como anexo a esse padrão. No próximo épico, forneça os valores para os parâmetros.	Arquiteto de nuvem

Preencha os parâmetros no AWS CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Forneça o nome do bucket do Amazon S3.	Insira o nome do bucket do Amazon S3 que você criou no primeiro épico.	Arquiteto de nuvem
Forneça o prefixo do Amazon S3.	Forneça a localização do arquivo.zip do código Lambda em seu bucket do Amazon S3, sem barras iniciais (por exemplo,). `<directory>/<file-name>.zip`	Arquiteto de nuvem
Forneça o ARN do tópico do Amazon SNS.	Se você quiser usar um tópico existente do Amazon SNS para notificações de remediação, forneça o Amazon Resource Name (ARN) do tópico do Amazon SNS. Se você quiser usar um novo tópico do Amazon SNS, mantenha o valor como `None` (o valor padrão).	Arquiteto de nuvem
Forneça um endereço de e-mail.	Forneça um endereço de e-mail no qual você deseja receber as notificações de remediação (necessárias somente quando você AWS CloudFormation deseja criar o tópico do Amazon SNS).	Arquiteto de nuvem
Defina o nível de registro em log.	Defina o nível de registro em log e a frequência da sua função do Lambda. `Info` designa mensagens	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	informativas detalhadas sobre o progresso do aplicativo. `Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	
Forneça o ARN da função do IAM para os registros de fluxo da VPC.	Forneça o ARN da função do IAM a ser usada nos registros de fluxo da VPC. Se você entrar`None`, AWS CloudFormation cria uma função do IAM e a usa.	Arquiteto de nuvem
Forneça o ARN da função do IAM para o monitoramento aprimorado do Amazon RDS.	Forneça o ARN da função do IAM a ser usada para o monitoramento aprimorado do Amazon RDS. Se você entrar`None`, AWS CloudFormation cria uma função do IAM e a usa.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura do Amazon SNS.	Quando o modelo é implantado com sucesso, se um novo tópico do Amazon SNS foi criado, uma mensagem de assinatura é enviada para o endereço de e-mail que você forneceu. Para receber	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	notificações de remediaçã o, você deve confirmar essa mensagem de assinatura de e-mail.	

Recursos relacionados

- Criando uma pilha no console AWS CloudFormation
- AWS Lambda site
- AWS Security Hub documentação

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Automatize as verificações de segurança para cargas de trabalho entre contas usando o Amazon Inspector e AWS Security Hub

Criado por Ramya Pulipaka (AWS) e Mikesh Khanal (AWS)

Resumo

Esse padrão descreve como verificar automaticamente vulnerabilidades em cargas de trabalho entre contas na nuvem da Amazon Web Services ()AWS.

O padrão ajuda a criar um cronograma para escaneamentos baseados em host de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que são agrupadas por tags ou para escaneamentos do Amazon Inspector baseados em rede. Uma AWS CloudFormation pilha implanta todos os AWS recursos e serviços necessários em seu. Contas da AWS

As descobertas do Amazon Inspector são exportadas AWS Security Hub e fornecem informações sobre vulnerabilidades em suas contas Regiões da AWS, nuvens privadas virtuais () VPCs e instâncias da Amazon. EC2 Você pode receber essas descobertas por e-mail ou criar um tópico do Amazon Simple Notification Service (Amazon SNS) que usa um endpoint HTTP para enviar as descobertas para ferramentas de emissão de bilhetes, software de gerenciamento de eventos e informações de segurança (SIEM) ou outras soluções de segurança de terceiros.

Pré-requisitos e limitações

Pré-requisitos

- Ativo Contas da AWS que hospeda cargas de trabalho entre contas, incluindo uma conta de auditoria central.
- Um endereço de e-mail existente para receber notificações do Amazon SNS por e-mail.
- Um endpoint HTTP existente usado por ferramentas de emissão de tíquetes, software SIEM ou outras soluções de segurança de terceiros.
- Security Hub habilitado e configurado. Você pode usar esse padrão sem o Security Hub, mas recomendamos usar o Security Hub por causa dos insights que ele gera. Para obter mais informações, consulte Configurando o Security Hub na documentação do Security Hub.
- Um agente do Amazon Inspector deve ser instalado em cada EC2 instância que você deseja escanear. Você pode instalar o agente do Amazon Inspector em várias EC2 instâncias usando o AWS Systems Manager Run Command.

Habilidades

- Experiência de uso `self-managed` e `service-managed` permissões para conjuntos de pilhas em CloudFormation. Se você quiser usar `self-managed` permissões para implantar instâncias de pilha em contas específicas em regiões específicas, crie as funções necessárias AWS Identity and Access Management (IAM). Se você quiser usar `service-managed` permissões para implantar instâncias de pilha AWS Organizations em contas gerenciadas por regiões específicas, não precisa criar as funções necessárias do IAM. Para obter mais informações, consulte Criar um conjunto de pilhas na CloudFormation documentação.

Limitações

- Se nenhuma etiqueta for aplicada às EC2 instâncias da Amazon em uma conta, o Amazon Inspector escaneia todas as instâncias dessa conta.
- Os conjuntos de CloudFormation pilhas e o `onboard-audit-account.yaml` arquivo (anexado) devem ser implantados na mesma região.
- A abordagem desse padrão pode ser escalada abaixo da cota de publicação de 30.000 transações por segundo (TPS) para um tópico do Amazon SNS na região Leste dos EUA (Norte da Virgínia) (`us-east-1`), embora os limites variem de acordo com a região. Para escalar com mais eficiência e evitar perda de dados, recomendamos usar o Amazon Simple Queue Service (Amazon SQS) antes do tópico Amazon SNS.

Arquitetura

O diagrama a seguir ilustra o fluxo de trabalho para escanear automaticamente as EC2 instâncias da Amazon.

O fluxo de trabalho consiste nas seguintes etapas:

1. Uma EventBridge regra da Amazon usa uma expressão cron para se iniciar automaticamente em uma programação específica e inicia o Amazon Inspector.
2. O Amazon Inspector verifica as EC2 instâncias marcadas da Amazon na conta.
3. O Amazon Inspector envia as descobertas para o Security Hub, que gera insights para fluxo de trabalho, priorização e remediação.

4. O Amazon Inspector também envia o status da avaliação para um tópico do Amazon SNS na conta de auditoria. Uma AWS Lambda função é invocada se um `findings reported` evento for publicado no tópico do Amazon SNS.
5. A função Lambda busca, formata e envia as descobertas para outro tópico do Amazon SNS na conta de auditoria.
6. As descobertas são enviadas para os endereços de e-mail inscritos no tópico do Amazon SNS. Os detalhes e recomendações completos são enviados no formato JSON para o endpoint HTTP inscrito.

Ferramentas

- AWS CloudFormationajuda você a modelar e configurar seus AWS recursos para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos.
- AWS CloudFormation StackSetsamplia a funcionalidade das pilhas, permitindo que você crie, atualize ou exclua pilhas em várias contas e regiões com uma única operação.
- AWS Control Towercria uma camada de abstração ou orquestração que combina e integra os recursos de várias outras, inclusive. Serviços da AWS AWS Organizations
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que facilita a conexão de seus aplicativos com dados de várias fontes.
- AWS Lambdaé um serviço de computação que ajuda você a executar código sem provisionar ou gerenciar servidores.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança na AWS e ajuda você a verificar seu ambiente em relação aos padrões e melhores práticas do setor de segurança.
- O Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens de publicadores para assinantes.

Épicos

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo na conta de auditoria.	Baixe e salve o arquivo `onboard-audit-account.yaml` (anexado) em um caminho local no seu computador. Faça login no AWS Management Console para sua conta de auditoria, abra o CloudFormation console e escolha Criar pilha. Escolha Preparar modelo na seção Pré-requisitos e escolha O modelo está pronto. Escolha Origem do modelo e, na seção Especificar modelo, selecione O modelo está pronto. Faça o upload do arquivo `onboard-audit-account.yaml` e configure as opções restantes de acordo com seus requisitos. Certifique-se de configurar os seguintes parâmetros de entrada: • `DestinationEmailAddress` : insira um endereço de e-mail para receber as descobertas.	Desenvolvedor, engenheiro de segurança

Tarefa	Descrição	Habilidades necessárias
	• `HTTPEndpoint` : forneça um endpoint HTTP para suas ferramentas de emissão de bilhetes ou SIEM. **Note** Você também pode implantar o CloudFormation modelo usando AWS Command Line Interface (AWS CLI). Para obter mais informações sobre isso, consulte Criação de uma pilha na CloudFormation documentação.	
Confirmar a assinatura do Amazon SNS.	Abra sua caixa de entrada de e-mail e escolha Confirmar a assinatura no e-mail que você receber do Amazon SNS. Isso abre uma janela do navegador da web e exibe a confirmação da assinatura.	Desenvolvedor, engenheiro de segurança

Crie conjuntos de CloudFormation pilhas para automatizar o cronograma de escaneamento do Amazon Inspector

Tarefa	Descrição	Habilidades necessárias
Crie conjuntos de pilhas na conta de auditoria.	Faça o download do arquivo `vulnerability-management-program.yaml` (anexado) para um caminho local no seu computador. No CloudFormation console, escolha Exibir conjuntos de pilhas e, em seguida, escolha Criar. StackSet Escolha O modelo está pronto, escolha Fazer o upload de um arquivo de modelo e, em seguida, carregue o arquivo `vulnerability-management-program.yaml` . Se você quiser usar `self-managed` permissões, siga as instruções em Criar um conjunto de pilhas com permissões autogerenciadas na CloudFormation documentação. Isso cria conjuntos de pilhas em contas individuais. Se você quiser usar `service-managed` permissões, siga as instruções em Criar um conjunto de pilhas com permissões	Desenvolvedor, engenheiro de segurança

Tarefa	Descrição	Habilidades necessárias
	gerenciadas por serviços na documentação. CloudFormation Isso cria conjuntos de pilhas em toda a organização ou em unidades organizacionais especificadas (OUs). Certifique-se de que os seguintes parâmetros de entrada estejam configurados para seus conjuntos de pilhas: • `AssessmentSchedule` — O cronograma para EventBridge usar expressões cron. • `Duration`: a duração da execução de avaliação do Amazon Inspector, em segundos. • `CentralSNSTopicArn` — O nome de recurso da Amazon (ARN) para o tópico central do Amazon SNS. • `Tagkey`: a chave de tag que está associada ao grupo de recursos. • `Tagvalue`: o valor da tag que está associado ao grupo de recursos. Se você quiser escanear EC2 instâncias da Amazon	

Tarefa	Descrição	Habilidades necessárias
	na conta de auditoria, você deve executar o `vulnerability-management-program.yaml` arquivo como uma CloudFormation pilha na conta de auditoria.	
Valide a solução.	Verifique se você recebe as descobertas por e-mail ou endpoint HTTP na programação que você especificou para o Amazon Inspector.	Desenvolvedor, engenheiro de segurança

Recursos relacionados

- Dimensione seus testes de vulnerabilidade de segurança com o Amazon Inspector (AWS postagem no blog)
- Corrija automaticamente as descobertas de segurança do Amazon InspectorAWS (postagem no blog)
- Como simplificar a configuração da avaliação de segurança usando a Amazon EC2 e AWS Systems Manager o Amazon Inspector (AWS postagem no blog)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Audite automaticamente grupos AWS de segurança que permitem acesso a partir de endereços IP públicos

Criado por Eugene Shifer (AWS) e Stephen (DiCato AWS)

Resumo

Como prática recomendada de segurança, é crucial minimizar a exposição dos AWS recursos somente ao absolutamente necessário. Por exemplo, servidores web que atendem ao público em geral precisam permitir o acesso de entrada pela Internet, mas o acesso a outras cargas de trabalho deve ser restrito a redes específicas para reduzir a exposição desnecessária. Os grupos de segurança na Amazon Virtual Private Cloud (Amazon VPC) são um controle eficaz para ajudar você a limitar o acesso aos recursos. No entanto, avaliar grupos de segurança pode ser uma tarefa complicada, especialmente em arquiteturas com várias contas. AWS Config regras e AWS Security Hub controles podem ajudá-lo a identificar grupos de segurança que permitem o acesso da Internet pública (0.0.0.0/0) a protocolos de comunicação de rede específicos, como Secure Shell (SSH), HTTP, HTTPS e protocolo de desktop remoto (RDP) do Windows. No entanto, essas regras e controles não são aplicáveis se os serviços forem executados em portas não padrão ou se o acesso for restrito a determinados endereços IP públicos. Por exemplo, isso pode ocorrer quando um serviço Web está associado à porta TCP 8443 em vez da porta TCP padrão 443. Isso também pode ocorrer quando os desenvolvedores têm acesso ao servidor a partir de suas redes domésticas, como para fins de teste.

Para resolver isso, você pode usar a solução de infraestrutura como código (IaC) fornecida nesse padrão para identificar grupos de segurança que permitem o acesso de qualquer endereço IP não privado (não compatível com a RFC 1918) a qualquer carga de trabalho em sua organização. Conta da AWS AWS O AWS CloudFormationmodelo fornece uma AWS Config regra personalizada, uma AWS Lambdafunção e as permissões necessárias. Você pode implantá-lo como uma pilha em uma única conta ou como um conjunto de pilhas em toda a organização, gerenciado por meio de. AWS Organizations

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Experiência usando GitHub
- Se você estiver implantando em um único Conta da AWS:

  - Permissões para criar CloudFormation pilhas
  - AWS Config configurado na conta de destino
  - (Opcional) Security Hub configurado na conta de destino
- Se você estiver implantando em uma AWS organização:
  - Permissões para criar conjuntos CloudFormation de pilhas
  - Security Hub configurado com AWS Organizations integração
  - AWS Config configurado nas contas em que você está implantando essa solução
  - Designe um Conta da AWS para ser o administrador delegado do Security Hub AWS Config e do Security Hub

Limitações

- Se você estiver implantando em uma conta individual que não tem o Security Hub ativado, você pode usar AWS Config para avaliar as descobertas.
- Se você estiver implantando em uma organização que não tem um administrador delegado para AWS Config o Security Hub, você deve fazer login nas contas individuais dos membros para ver as descobertas.
- Se você usa AWS Control Tower para gerenciar e governar as contas em sua organização, implante o IaC nesse padrão usando Personalizações para AWS Control Tower (cFct). O uso do CloudFormation console criaria um desvio de configuração a partir das AWS Control Tower grades de proteção e exigiria que você reinscrevesse as unidades organizacionais () OUs ou as contas gerenciadas.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte Serviços da AWS por região. Para endpoints específicos, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Implantação em um indivíduo Conta da AWS

O diagrama de arquitetura a seguir mostra a implantação dos AWS recursos em um único Conta da AWS. Você provisiona os recursos usando um CloudFormation modelo diretamente pelo CloudFormation console. Se o Security Hub estiver ativado, você poderá visualizar os resultados em um AWS Config ou no Security Hub. Se o Security Hub não estiver ativado, você poderá visualizar os resultados somente em AWS Config.

O diagrama mostra o seguinte fluxo de trabalho:

1. Você cria uma CloudFormation pilha. Isso implanta uma função Lambda e AWS Config uma regra. Tanto a regra quanto a função são configuradas com as permissões AWS Identity and Access Management (IAM) necessárias para publicar avaliações de recursos AWS Config e registros.
2. A AWS Config regra opera no modo de avaliação de detetive e invoca a função Lambda a cada 24 horas.
3. A função Lambda avalia os grupos de segurança e envia atualizações para o. AWS Config
4. O Security Hub recebe todas as AWS Config descobertas.
5. Você pode ver as descobertas no Security Hub ou no AWS Config, dependendo dos serviços que você configurou na conta.

Implantação em uma organização AWS

O diagrama a seguir mostra a implantação do padrão em várias contas gerenciadas por meio de AWS Organizations AWS Control Tower e. Você implanta o CloudFormation modelo por meio do cFct. Os resultados da avaliação são centralizados no Security Hub na conta do administrador delegado. A seção AWS CodePipeline de fluxo de trabalho do diagrama mostra as etapas em segundo plano que ocorrem durante a implantação do cFCT.

O diagrama mostra o seguinte fluxo de trabalho:

1. Na conta de gerenciamento, você carrega um arquivo compactado (ZIP) do modelo IaC em um bucket do Amazon Simple Storage Service (Amazon S3) que é implantado pelo cFCT.
2. O pipeline cFct descompacta o arquivo, executa as verificações cfn-nag (GitHub) e implanta o modelo como um conjunto de pilhas. CloudFormation
3. Dependendo da configuração especificada no arquivo de manifesto cFct, CloudFormation StackSets implanta pilhas em contas individuais ou especificadas. OUs Isso implanta uma função Lambda e AWS Config uma regra nas contas de destino. Tanto a regra quanto a função são configuradas com as permissões do IAM necessárias para publicar avaliações de recursos AWS Config e registros.
4. A AWS Config regra opera no modo de avaliação de detetive e invoca a função Lambda a cada 24 horas.
5. A função Lambda avalia os grupos de segurança e envia atualizações para o. AWS Config

6. AWS Config encaminha todas as descobertas para o Security Hub.
7. As descobertas do Security Hub são agregadas na conta do administrador delegado.
8. Você pode ver as descobertas agregadas no Security Hub na conta de administrador delegado.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo. Uma AWS Config regra define suas configurações ideais para um recurso e AWS Config pode avaliar se seus AWS recursos estão em conformidade com as condições da regra.
- AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas. O Customizations for AWS Control Tower (cFct) ajuda você a personalizar sua AWS Control Tower landing zone e a se manter alinhado com as melhores práticas. AWS As personalizações dessa solução são implementadas por meio de CloudFormation modelos e políticas de controle AWS Organizations de serviços () SCPs.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS. Também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança.

Outras ferramentas

- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub Detectar grupos de segurança vulneráveis.

Práticas recomendadas

Recomendamos que você siga as melhores práticas dos seguintes recursos:

- Melhores práticas para unidades organizacionais com AWS Organizations (blog de operações e migrações AWS na nuvem)
- Orientação para estabelecer uma base inicial usando AWS Control Tower on AWS (Biblioteca de AWS soluções)
- Orientação para criar e modificar AWS Control Tower recursos (AWS Control Tower documentação)
- Considerações sobre a implantação do cFCT (documentação)AWS Control Tower
- Aplique permissões com privilégios mínimos (documentação do IAM)

Épicos

Revise o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Determine sua estratégia de implantação.	Analise a solução e o código para determinar a estratégia de implantação para seu AWS ambiente. Determine se você está implantando em uma única conta ou em uma AWS organização.	Proprietário do aplicativo, General AWS
Clonar o repositório.	Digite o comando a seguir para clonar o repositório Detectar grupos de segurança vulneráveis: `git clone https://github.com/aws-samp`	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
	`les/detect-public-security-groups.git`	
Valide a versão do Python.	1. Navegue até o diretório de nível superior no repositório clonado: `cd detect-public-security-groups` 2. Abra Security-Group-Public-Assessment.yaml. 3. No `SgPublicAccessCheckLambdaFunction` recurso, confirme se a versão do Python é compatível com seu destino. Regiões da AWS Por padrão, essa função usa o Python 3.12. Para obter mais informações, consulte AWS Lambda adiciona suporte ao Python 3.12. Se necessário, atualize a versão do Python. 4. Salve e feche o Security-Group-Public-Assessment.yaml.	Administrador da AWS, desenvolvedor de aplicativos

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	Implante o CloudFormation modelo em seu AWS ambiente. Execute um destes procedimentos: • Se você estiver implantando em uma única Conta da AWS, siga as instruções em Criação de uma pilha. • Se você estiver implantando em uma organização que não é gerenciada por AWS Control Tower, siga as instruções em Criar um conjunto de pilhas. • Se você estiver implantando em uma organização gerenciada por AWS Control Tower, consulte as instruções em Crie suas próprias personalizações.	Desenvolvedor de aplicativos, administrador da AWS, AWS geral
Verificar a implantação.	No CloudFormation console, verifique se a pilha ou o conjunto de pilhas foi implantado com êxito.	Administrador da AWS, proprietário do aplicativo

Analise as descobertas

Tarefa	Descrição	Habilidades necessárias
Veja as conclusões da AWS Config regra.	No Security Hub, faça o seguinte para ver uma lista de descobertas individuais: 1. Abra o console do Security Hub. 2. No painel de navegação, selecione Descobertas. 3. Na caixa Adicionar filtros, adicione os seguintes filtros: • O status de conformidade é `FAILED` • O título é `SgPublicAccessCheck` 4. Escolha Aplicar. No Security Hub, faça o seguinte para ver uma lista do total de descobertas agrupadas por Conta da AWS: 1. Abra o console do Security Hub. 2. No painel de navegação, escolha Insights. 3. Escolha Criar insight. 4. Para selecionar o atributo de agrupamento do insight:	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
	a. Escolha a caixa de pesquisa para exibir as opções de filtro. b. Escolha Agrupar por. c. Selecione AwsAccountId. d. Escolha Aplicar. 5. Na caixa Adicionar filtros, adicione os seguintes filtros: • O título é `SgPublicAccessCheck` • O status de conformidade é `FAILED` 6. Escolha Criar insight. 7. Insira um Nome do insight e escolha Criar insight. Em AWS Config, para ver uma lista de descobertas, siga as instruções em Exibindo informações de conformidade e resultados da avaliação na AWS Config documentação.	

Solução de problemas

Problema	Solução
A criação ou exclusão do conjunto de CloudFormation pilhas falha.	Quando AWS Control Tower implantado, ele impõe as proteções necessárias e assume o controle sobre agregadores e regras. AWS Config Isso inclui evitar quaisquer alteraçõe

Problema	Solução
	s diretas. CloudFormation Para implantar ou remover adequadamente esse CloudFormation modelo, incluindo todos os recursos associado s, você deve usar o cFct.
O cFct não consegue excluir o CloudFormation modelo.	Se o CloudFormation modelo persistir mesmo depois de fazer as alterações necessárias no arquivo de manifesto e remover os arquivos de modelo, confirme se o arquivo de manifesto contém o `enable_stack_set_deletion` parâmetro e se o valor está definido como. `false` Para obter mais informações, consulte Excluir um conjunto de pilhas na documenta ção do cFct.

Recursos relacionados

- AWS Config Regras personalizadas (AWS Config documentação)

Reative automaticamente a AWS CloudTrail usando uma regra de remediação personalizada no AWS Config

Criado por Manigandan Shri (AWS)

Resumo

A visibilidade da atividade em sua conta da Amazon Web Services (AWS) é uma importante prática recomendada operacional e de segurança. CloudTrail A AWS ajuda você com a governança, a conformidade e a auditoria operacional e de risco da sua conta.

Para garantir que CloudTrail permaneça habilitado em sua conta, o AWS Config fornece a regra *`cloudtrail-enabled`* gerenciada. Se CloudTrail estiver desativada, a `cloudtrail-enabled` regra a reativa automaticamente usando a correção automática.

No entanto, você deve se certificar de seguir as melhores práticas de segurança para CloudTrail usar a remediação automática. Essas melhores práticas incluem habilitar CloudTrail em todas as regiões da AWS, registrar cargas de trabalho de leitura e gravação, habilitar insights e criptografar arquivos de log com criptografia do lado do servidor usando chaves gerenciadas (SSE-KMS) do AWS Key Management Service (AWS KMS).

Esse padrão ajuda você a seguir essas melhores práticas de segurança, fornecendo uma ação de remediação personalizada para ser reativada automaticamente CloudTrail em sua conta.

> **Important**
>
> Recomendamos o uso de políticas de controle de serviço (SCPs) para evitar qualquer adulteração. CloudTrail Para obter mais informações sobre isso, consulte a CloudTrail seção Prevenir adulteração na AWS sobre Como usar o AWS Organizations para simplificar a segurança em grande escala no blog de segurança da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Permissões para criar um runbook do AWS Systems Manager Automation

- Uma trilha existente para sua conta

Limitações

Esse padrão não é compatível com as seguintes ações:

- Configurar uma chave de prefixo do Amazon Simple Storage Service (Amazon S3) para o local de armazenamento da chave de prefixo
- Publicar para um tópico do Amazon Simple Notification Service (Amazon SNS)
- Configurando o Amazon CloudWatch Logs para monitorar seus CloudTrail registros

Arquitetura

Pilha de tecnologia

- AWS Config
- CloudTrail
- Systems Manager
- Automação do Systems Manager

Ferramentas

- O AWS Config oferece uma exibição detalhada da configuração dos recursos da AWS em sua conta.
- CloudTrailA AWS ajuda você a viabilizar a governança, a conformidade e a auditoria operacional e de risco da sua conta.
- O AWS Key Management Service (AWS KMS) é um serviço de criptografia e gerenciamento de chave com escalabilidade para a nuvem.
- O AWS Systems Manager ajuda a visualizar e controlar a infraestrutura na AWS.
- O AWS Systems Manager Automation simplifica tarefas comuns de manutenção e implantação de instâncias do Amazon Elastic Compute Cloud EC2 (Amazon) e outros recursos da AWS.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Código

O cloudtrail-remediation-actionarquivo.yml (anexado) ajuda você a criar um runbook do Systems Manager Automation para configurar e reativar CloudTrail usando as melhores práticas de segurança.

Épicos

Configure CloudTrail

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	Faça login no AWS Management Console, abra o console Amazon S3 e crie um bucket S3 para armazenar os registros. CloudTrail Para obter mais informações, consulte Criar um bucket S3 na documentação do Amazon S3.	Administrador de sistemas
Adicione uma política de bucket para permitir CloudTrail a entrega de arquivos de log para o bucket do S3.	CloudTrail deve ter as permissões necessárias para entregar arquivos de log ao seu bucket do S3. No console do Amazon S3, escolha o bucket do S3 criado anteriormente e escolha Permissões. Crie uma política de bucket do S3 usando a política de bucket do Amazon S3 da CloudTrail CloudTrail documentação. Para visualizar as etapas de como adicionar uma política a um bucket do S3, consulte Adicionar uma política de	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	bucket usando o console do Amazon S3 na documentação do Amazon S3. **Important** Se você especificou um prefixo ao criar sua trilha CloudTrail, certifique-se de incluí-lo na política de bucket do S3. O prefixo é uma opção adicional para a chave do objeto do S3 que cria uma organização em formato de pasta no seu bucket do S3. Para obter mais informações sobre isso, consulte Criação de uma trilha na CloudTrail documentação.	

Tarefa	Descrição	Habilidades necessárias
Crie uma chave do KMS.	Crie uma chave do AWS KMS para CloudTrail criptografar objetos antes de adicioná-los ao bucket do S3. Para obter ajuda com essa história, consulte Criptografar arquivos de CloudTrail log com chaves gerenciadas do AWS KMS (SSE-KMS) na documentação. CloudTrail	Administrador de sistemas
Adicione uma política de chaves à chave do KMS.	Anexe uma política de chave KMS para CloudTrail permitir o uso da chave KMS. Para obter ajuda com essa história, consulte Criptografar arquivos de CloudTrail log com chaves gerenciadas pelo AWS KMS (SSE-KMS) na documentação. CloudTrail **Important** CloudTrail não exige `Decrypt` permissões.	Administrador de sistemas
Crie AssumeRole o runbook do Systems Manager	Crie um `AssumeRole` para que o Systems Manager Automation execute o runbook. Para obter instruções e mais informações, consulte Configurando a automação na documentação do Systems Manager.	Administrador de sistemas

Crie e teste o runbook do Systems Manager Automation

Tarefa	Descrição	Habilidades necessárias
Crie um runbook do Systems Manager Automation.	Use o arquivo `cloudtrail-remediation-action.yml` (anexado) para criar o runbook do Systems Manager Automation. Para obter mais informações, consulte Criação de documentos do Systems Manager na documentação do Systems Manager.	Administrador de sistemas
Teste o runbook.	No console do Systems Manager, teste o runbook do Systems Manager Automation que você criou anteriormente. Para obter mais informações, consulte Executar uma automação simples na documentação do Systems Manager.	Administrador de sistemas

Configure a regra de remediação automática no AWS Config

Tarefa	Descrição	Habilidades necessárias
Adicione a regra CloudTrail - enabled.	No console do AWS Config, escolha Regras e, em seguida, escolha Adicionar regra. Na página Add rule (Adicionar regra), selecione Add custom rule (Adicionar regra personalizada). Na	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	página Configurar regra, digite um nome e uma descrição para a regra `cloudtrail-enabled`. Para obter mais informações, consulte Gerenciar suas regras do AWS Config na documentação do AWS Config.	

Tarefa	Descrição	Habilidades necessárias
Adicione a ação de correção automática.	Na lista suspensa Ações, escolha Gerenciar remediação. Escolha Remediação automática e, em seguida, escolha o runbook do Systems Manager que você criou anteriormente. A seguir estão os parâmetros de entrada necessários para CloudTrail: • `CloudTrailName` • `CloudTrailS3BucketName` • `CloudTrailKmsKeyId` • `AssumeRole` (opcional) Os seguintes parâmetros de entrada são definidos como verdadeiros por padrão: • `IsMultiRegionTrail` • `IsOrganizationTrail` • `IncludeGlobalServiceEvents` • `EnableLogFileValidation` Mantenha os valores padrão para o parâmetro Parâmetros de limite de taxa e parâmetro	Administrador de sistemas

Tarefa	Descrição	Habilidades necessárias
	de ID de recurso. Escolha Salvar. Para obter mais informações, consulte Remediar recursos da AWS não compatíveis com as regras do AWS Config na documentação do AWS Config.	
Teste a regra de remediação automática.	Para testar a regra de remediação automática, abra o CloudTrail console, escolha Trilhas e, em seguida, escolha a trilha. Escolha Parar registro em log para desativar o registro na trilha. Quando você for solicitado a confirmar , escolha Parar de registrar . CloudTrail interrompe a atividade de registro dessa trilha. Siga as instruções de Avaliação de seus recursos na documentação do AWS Config para garantir CloudTrail que ela seja reativada automatic amente.	Administrador de sistemas

Recursos relacionados

Configurar CloudTrail

- Criar um bucket do S3

- Política de bucket do Amazon S3 para CloudTrail
- Adicionar uma política de bucket usando o console do Amazon S3
- Criar uma trilha
- Configurar a automação
- Criptografando arquivos de CloudTrail log com chaves gerenciadas do AWS KMS (SSE-KMS)

Crie e teste o runbook do Systems Manager Automation

- Criar documentos do Systems Manager
- Executar uma automação simples

Configure a regra de remediação automática no AWS Config

- Gerenciando suas regras do AWS Config
- Corrigir recursos da AWS não compatíveis de acordo com as regras do AWS Config

Recursos adicionais

- AWS CloudTrail — Melhores práticas de segurança
- Conceitos básicos do AWS Systems Manager
- Conceitos básicos do AWS Config
- Comece a usar a AWS CloudTrail

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Corrija automaticamente instâncias e clusters de banco de dados Amazon RDS não criptografados

Criado por Ajay Rawat (AWS) e Josh Joy (AWS)

Resumo

Esse padrão descreve como corrigir automaticamente instâncias de banco de dados e clusters não criptografados do Amazon Relational Database Service (Amazon RDS) no Amazon Web Services (AWS) usando AWS Config, AWS Systems Manager runbooks e chaves (). AWS Key Management Service AWS KMS

As instâncias criptografadas do RDS DB fornecem uma camada adicional de proteção de dados, protegendo seus dados contra o acesso não autorizado ao armazenamento subjacente. Você pode usar a criptografia do Amazon RDS para aumentar a proteção dos dados de seus aplicativos implantados no e cumprir os Nuvem AWS requisitos de conformidade para criptografia em repouso. Você só pode habilitar a criptografia para uma instância do banco de dados do RDS ao criá-la, não depois de ela ter sido criada. No entanto, você pode adicionar criptografia a uma instância do banco de dados do RDS não criptografada criando um snapshot da sua instância de banco de dados e depois criando uma cópia criptografada desse snapshot. Em seguida, você pode restaurar uma instância de banco de dados a partir do snapshot criptografado, você terá uma cópia criptografada da sua instância de banco de dados original.

Esse padrão é usado Regras do AWS Config para avaliar instâncias e clusters de banco de dados do RDS. Ele aplica a remediação usando AWS Systems Manager runbooks, que definem as ações a serem executadas em recursos incompatíveis do Amazon RDS, AWS KMS e chaves para criptografar os DB snapshots. Em seguida, ele aplica políticas de controle de serviço (SCPs) para impedir a criação de novas instâncias de banco de dados e clusters sem criptografia.

O código desse padrão é fornecido em GitHub.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Arquivos do repositório de GitHub código-fonte desse padrão baixados para o seu computador

- Uma instância de banco de dados do RDS ou outro cluster
- Uma AWS KMS chave existente para criptografar instâncias e clusters de banco de dados do RDS
- Acesso para atualizar a política de recursos principais do KMS
- AWS Config habilitado em seu Conta da AWS (consulte Introdução AWS Config na AWS documentação)

Limitações

- Você só pode habilitar a criptografia para uma instância de banco de dados do RDS ao criá-la, não depois de ela ter sido criada.
- Não é possível ter uma réplica de leitura criptografada de uma instância de banco de dados não criptografada nem uma réplica de leitura não criptografada de uma instância de banco de dados criptografada.
- Não é possível restaurar um backup ou um snapshot não criptografado em uma instância de banco de dados criptografada.
- A criptografia do Amazon RDS está disponível para a maioria das classes de instância de banco de dados. Para obter uma lista de exceções, consulte Criptografar recursos do Amazon RDS na documentação do Amazon RDS.
- Para copiar um instantâneo criptografado de um Região da AWS para outro, você deve especificar a chave KMS no destino. Região da AWS Isso ocorre porque as chaves KMS são específicas do local em Região da AWS que foram criadas.
- O snapshot de origem permanece criptografado ao longo do processo de cópia. O Amazon RDS usa criptografia envelopada para proteger os dados durante o processo de cópia. Para obter mais informações, consulte Criptografia de envelope na AWS KMS documentação.
- Não é possível descriptografar uma instância de banco de dados criptografada. No entanto, é possível exportar dados de uma instância de banco de dados criptografada e importar os dados para uma instância de banco de dados não criptografado.
- Só exclua uma chave do KMS quando você tiver certeza de que não vai mais precisar dela. Caso não tenha certeza, desabilite a chave do KMS em vez de excluí-la. Você poderá reabilitar a chave do KMS desabilitada se precisar usá-la mais tarde, mas não poderá recuperar aquela que foi excluída.
- Se você optar por não reter backups automatizados, seus backups automatizados que estão na Região da AWS mesma instância de banco de dados serão excluídos. Eles não podem ser recuperados depois de excluir a instância de banco de dados.

- Os backups automatizados são retidos pelo período de retenção definido na instância de banco de dados no momento em que você a exclui. Esse período de retenção definido ocorre independentemente de você optar ou não por criar um snapshot de banco de dados final.
- Se a correção automática estiver ativada, essa solução criptografará todos os bancos de dados que tenham a mesma chave KMS.

Arquitetura

O diagrama a seguir ilustra a arquitetura da AWS CloudFormation implementação. Observe que você também pode implementar esse padrão usando AWS Cloud Development Kit (AWS CDK) o.

Ferramentas

Ferramentas

- AWS CloudFormationajuda você a configurar automaticamente seus AWS recursos. Ele permite que você use um arquivo de modelo para criar e configurar um conjunto de recursos da como uma unidade única (uma pilha).
- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software para definir sua infraestrutura de nuvem em código e provisioná-la usando linguagens de programação conhecidas.

Serviços e atributos da AWS

- AWS Configacompanha a configuração de seus AWS recursos e suas relações com seus outros recursos. Ele também pode avaliar esses AWS recursos para fins de conformidade. Esse serviço usa regras que podem ser configuradas para avaliar AWS os recursos em relação às configurações desejadas. Você pode usar um conjunto de regras AWS Config gerenciadas para cenários comuns de conformidade ou criar suas próprias regras para cenários personalizados. Quando um AWS recurso não está em conformidade, você pode especificar uma ação de remediação por meio de um AWS Systems Manager runbook e, opcionalmente, enviar um alerta por meio de um tópico do Amazon Simple Notification Service (Amazon SNS). Em outras palavras, você pode associar ações de remediação Regras do AWS Config e optar por executá-las automaticamente para lidar com recursos não compatíveis sem intervenção manual. Se um recurso ainda não for compatível após a correção automática de não conformidade, você poderá definir a regra para tentar fazer a correção automática novamente.

- Com o Amazon Relational Database Service (Amazon RDS), é mais fácil configurar, operar e escalar um banco de dados relacional na nuvem. O componente básico do Amazon RDS é a instância de banco de dados, que é um ambiente de banco de dados isolado no Nuvem AWS. O Amazon RDS fornece uma seleção de tipos de instância otimizadas para se adequarem a diferentes casos de uso de banco de dados relacional. Os tipos de instância incluem várias combinações de capacidade de CPU, memória, armazenamento e redes e oferecem a flexibilidade de escolher a combinação de recursos adequada para seu banco de dados. Cada tipo de instância inclui vários tamanhos de instância, permitindo que você escale seus bancos de dado de acordo com os requisitos de sua workload de destino.
- AWS Key Management Service (AWS KMS) é um serviço gerenciado que facilita a criação e o controle AWS KMS keys, que criptografa seus dados. Uma chave do KMS é uma representação lógica de uma chave raiz. A chave do KMS inclui metadados, como o ID da chave, a data de criação, a descrição e o estado da chave.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- As políticas de controle de serviço (SCPs) oferecem controle central sobre o máximo de permissões disponíveis para todas as contas em sua organização. SCPs ajudam você a garantir que suas contas permaneçam dentro das diretrizes de controle de acesso da sua organização. SCPs não afetam usuários ou funções na conta de gerenciamento. Elas afetam apenas as contas-membro de sua organização. É altamente recomendável que você não se vincule SCPs à raiz da sua organização sem testar minuciosamente o impacto que a política tem nas contas. Em vez disso, crie uma unidade organizacional (UO) para a qual você possa mover suas contas, uma por vez, ou pelo menos em pequenas quantidades, para garantir que não seja possível bloquear acidentalmente usuários nos serviços principais.

Código

O código-fonte e os modelos desse padrão estão disponíveis em um GitHub repositório. O padrão fornece duas opções de implementação: você pode implantar um AWS CloudFormation modelo para criar a função de remediação que criptografa instâncias e clusters de banco de dados do RDS ou usar o. AWS CDK O repositório tem pastas separadas para essas duas opções.

A seção Epics fornece step-by-step instruções para implantar o CloudFormation modelo. Se você quiser usar o AWS CDK, siga as instruções no `README.md` arquivo no GitHub repositório.

Práticas recomendadas

- Ative a criptografia de dados em repouso e em trânsito.
- Ativar AWS Config em todas as contas Regiões da AWS e.
- Registre as alterações de configuração em todos os tipos de recursos.
- Mude suas credenciais do IAM regularmente.
- Aproveite a marcação para AWS Config, que facilita o gerenciamento, a pesquisa e a filtragem de recursos.

Épicos

Crie a função de remediação do IAM e o runbook do Systems Manager

Tarefa	Descrição	Habilidades necessárias
Faça o download do CloudFormation modelo.	Baixe o `unencrypted-to-encrypted-rds.template.json` arquivo do GitHub repositório.	DevOps engenheiro
Crie a CloudFormation pilha.	1. Faça login no AWS Management Console e abra o CloudFormation console. 2. Inicie o modelo `unencrypted-to-encrypted-rds.template.json` para criar uma nova pilha. Para obter mais informações sobre a implantação de modelos, consulte a AWS CloudFormation documentação.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Revise CloudFormation os parâmetros e valores.	1. Revise os detalhes da pilha e atualize os valores com base nos requisitos do seu ambiente. 2. Selecione Criar pilha para implantar o modelo.	DevOps engenheiro
Analise os recursos.	O status mudará para CREATE_COMPLETE depois que a pilha tiver sido criada. Analise os recursos criados (função do IAM, runbook do Systems Manager) no CloudFormation console.	DevOps engenheiro

Atualize a política de AWS KMS chaves

Tarefa	Descrição	Habilidades necessárias
Atualize sua política de chaves do KMS.	1. Verifique se o alias da chave `alias/RDS EncryptionAtRestKMSAlias` existe. 2. A declaração de política de chave deve incluir a função de correção do IAM. (Confira os recursos criados pelo CloudForm ation modelo que você implantou no épico anterior.) 3. Na política de chaves a seguir, atualize as partes que estão em negrito para	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	corresponder à sua conta e ao perfil do IAM que foi criado. `{ "Sid": "Allow access through RDS for all principals in the account that are authorized to use RDS", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam:: <your-AWS-account-ID>”:role/<your-IAM-remediation-role>" }, "Action": ["kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*", "kms:GenerateDataKey*", "kms:CreateGrant", "kms:ListGrants", "kms:DescribeKey"], "Resource": "*", "Condition": { "StringEquals": { "kms:ViaService": "rds.us-east-1.amazonaws.com",`	

Tarefa	Descrição	Habilidades necessárias

	<pre>"kms:Call
	erAccount": "<your-AW
	S-account-ID>"
	}
	}
	}</pre>	

Encontre e corrija recursos que não estejam em conformidade

Tarefa	Descrição	Habilidades necessárias
Visualize recursos não compatíveis.	1. Para ver uma lista de recursos não compatíveis, abra o AWS Config console. 2. No painel de navegação, escolha Regras e, em seguida escolha a regra `rds-storage-encrypted` . Os recursos não compatíveis listados no AWS Config console serão instâncias, não clusters. A automação de correção criptografa instâncias e clusters e cria uma instância recém-criptografada ou um cluster recém-criado. No entanto, certifique-se de não corrigir simultaneamente várias instâncias que pertencem ao mesmo cluster.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Antes de corrigir quaisquer instâncias ou volumes de banco de dados do RDS, certifique-se de que a instância de banco de dados do RDS não esteja em uso. Confirme se não há operações de gravação ocorrendo enquanto o snapshot está sendo criado, para garantir que o snapshot contenha os dados originais. Considere aplicar uma janela de manutenção durante a qual a correção será executada.	

Tarefa	Descrição	Habilidades necessárias
Corrija recursos que não estejam em conformidade.	1. Quando você estiver pronto e a janela de manutenção estiver em vigor, escolha o recurso a ser corrigido e, em seguida, escolha Corrigir. A coluna Status da ação agora deve exibir a Execução da ação na fila. 2. Visualize o progresso e o status da correção no Systems Manager. Abra o console do Systems Manager. No painel de navegação, escolha Automação e, em seguida, selecione o ID de execução da automação correspon dente para ver mais detalhes.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Verifique se a instância de banco de dados do RDS está disponível.	Depois que a automação for concluída, a instância de banco de dados do RDS recém-criptografada ficará disponível. A instância de banco de dados do RDS criptografada terá o prefixo `encrypted` seguido pelo nome original. Por exemplo, se o nome da instância de banco de dados do RDS não criptografada fosse `database-1` , a instância de banco de dados do RDS recém-criptografada seria `encrypted-database-1` .	DevOps engenheiro
Encerre a instância não criptografada.	Depois que a correção for concluída e o recurso recém-criptografado tiver sido validado, você poderá encerrar a instância não criptografada. Certifique-se de confirmar se o recurso recém-criptografado corresponde ao recurso não criptografado antes de encerrar qualquer recurso.	DevOps engenheiro

Aplicar SCPs

Tarefa	Descrição	Habilidades necessárias
Aplicar SCPs.	Aplique SCPs para evitar que instâncias e clusters de banco de dados sejam criados sem criptografia no futuro. Use o `rds_encrypted.json` arquivo fornecido no GitHub repositório para essa finalidad e e siga as instruções na AWS documentação.	Engenheiro de segurança

Recursos relacionados

Referências

- Configuração AWS Config
- AWS Config regras personalizadas
- AWS KMS conceitos
- AWS Systems Manager documentos
- Políticas de controle de serviço

Ferramentas

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK)

Guias e padrões

- Reative automaticamente AWS CloudTrail usando uma regra de remediação personalizada no AWS Config

Mais informações

Como AWS Config funciona?

Quando você usa AWS Config, ele primeiro descobre os AWS recursos compatíveis que existem na sua conta e gera um item de configuração para cada recurso. AWS Config também gera itens de configuração quando a configuração de um recurso é alterada e mantém registros históricos dos itens de configuração de seus recursos a partir do momento em que você inicia o gravador de configuração. Por padrão, AWS Config cria itens de configuração para cada recurso suportado no Região da AWS. Se você não quiser AWS Config criar itens de configuração para todos os recursos compatíveis, você pode especificar os tipos de recursos que você deseja monitorar.

Como estão AWS Config e Regras do AWS Config com os quais se relacionam AWS Security Hub?

AWS Security Hub é um serviço de segurança e conformidade que fornece gerenciamento da postura de segurança e conformidade como um serviço. Ele usa AWS Config e Regras do AWS Config como mecanismo primário para avaliar a configuração dos AWS recursos. Regras do AWS Config também pode ser usado para avaliar diretamente a configuração do recurso. Outros Serviços da AWS, tais AWS Control Tower e AWS Firewall Manager, também usam Regras do AWS Config.

Alterne automaticamente as chaves de acesso do usuário do IAM em grande escala com o AWS Organizations e o AWS Secrets Manager

Criado por Tracy Hickey (AWS), Gaurav Verma (AWS), Laura Seletos (AWS), Michael Davie (AWS) e Arvind Patel (AWS)

Resumo

> **Important**
>
> Como melhor prática, a AWS recomenda que você use funções do AWS Identity and Access Management (IAM) em vez de usuários do IAM com credenciais de longo prazo, como chaves de acesso. A abordagem documentada nesse padrão se destina somente a implementações antigas que exigem credenciais de API da AWS de longa duração. Para essas implementações, ainda recomendamos que você considere opções para usar credenciais de curto prazo, como usar perfis de instância do Amazon Elastic Compute Cloud (Amazon EC2) ou IAM Roles Anywhere. A abordagem neste artigo é somente para casos em que você não consegue passar a usar credenciais de curto prazo imediatam ente e exige que as credenciais de longo prazo sejam alternadas de acordo com um cronograma. Com essa abordagem, você é responsável por atualizar periodicamente o código ou a configuração do aplicativo antigo para usar as credenciais alternadas da API.

As chaves de acesso são credenciais de longo prazo para um usuário do IAM. A rotação regular de suas credenciais do IAM ajuda a evitar que um conjunto comprometido de chaves de acesso do IAM acesse componentes em sua conta da AWS. A rotação das credenciais do IAM também é uma parte importante das melhores práticas de segurança no IAM.

Esse padrão ajuda você a alternar automaticamente as chaves de acesso do IAM usando CloudFormation modelos da AWS, que são fornecidos no repositório de rotação de chaves do GitHub IAM.

O padrão oferece suporte à implantação em uma única conta ou em várias contas. Se você estiver usando o AWS Organizations, essa solução identifica todas as contas da AWS IDs em sua organização e escala dinamicamente à medida que as contas são removidas ou novas contas

são criadas. A função centralizada do AWS Lambda usa um perfil assumido do IAM para executar localmente as funções de rotação em várias contas selecionadas por você.

- Novas chaves de acesso do IAM são geradas quando as chaves de acesso existentes têm 90 dias.
- As novas chaves de acesso são armazenadas como um segredo no AWS Secrets Manager. Uma política baseada em recursos permite que somente a entidade principal do IAM acesse e recupere o segredo. Se você optar por armazenar as chaves na conta de gerenciamento, as chaves de todas as contas serão armazenadas na conta de gerenciamento.
- O endereço de e-mail atribuído ao proprietário da conta da AWS em que as novas chaves de acesso foram criadas recebe uma notificação.
- As chaves de acesso anteriores são desativadas aos 100 dias e depois excluídas aos 110 dias.
- Uma notificação centralizada por e-mail é enviada ao proprietário da conta da AWS.

As funções Lambda e a Amazon executam essas ações CloudWatch automaticamente. Em seguida, você pode recuperar o novo par de chaves de acesso e substitui-lo em seu código ou aplicativos. Os períodos de rotação, exclusão e desativação podem ser personalizados.

Pré-requisitos e limitações

- Pelo menos uma conta ativa da AWS.
- AWS Organizations, configurado e definido (veja o tutorial).
- Permissões para consultar o AWS Organizations em sua conta de gerenciamento. Para obter mais informações, consulte AWS Organizations e funções vinculadas ao serviço na documentação do AWS Organizations.
- Um diretor do IAM que tem permissões para lançar o CloudFormation modelo da AWS e os recursos associados. Para obter mais informações, consulte Conceder permissões autogerenciadas na CloudFormation documentação da AWS.
- Um bucket do Amazon Simple Storage Service (Amazon S3) existente para implantar os recursos.
- O Amazon Simple Email Service (Amazon SES) saiu do sandbox. Para obter mais informações, consulte Saída da sandbox do Amazon SES na documentação do Amazon SES.
- Se você optar por executar o Lambda em uma nuvem privada virtual (VPC), os seguintes recursos, que devem ser criados antes de você executar o modelo principal: CloudFormation
  - Uma VPC.

  - Uma sub-rede.
  - Endpoints para Amazon SES, AWS Systems Manager, AWS Security Token Service (AWS STS), Amazon S3 e AWS Secrets Manager. (Você pode executar o modelo de endpoint fornecido no repositório de rotação de chaves do GitHub IAM para criar esses endpoints.)
- O usuário e a senha do Simple Mail Transfer Protocol (SMTP) armazenados nos parâmetros do AWS Systems Manager (parâmetros SSM). Os parâmetros devem corresponder aos parâmetros principais CloudFormation do modelo.

Arquitetura

Pilha de tecnologia

- Amazon CloudWatch
- Amazon EventBridge
- IAM
- AWS Lambda
- AWS Organizations
- Amazon S3

Arquitetura

Os diagramas a seguir mostram os componentes e os fluxos de trabalho desse padrão. A solução oferece suporte a dois cenários para armazenar as credenciais: em uma conta de membro e na conta de gerenciamento.

Opção 1: armazenar as credenciais em uma conta de membro

Opção 2: armazenar as credenciais em uma conta de gerenciamento

O diagrama mostra o seguinte fluxo de trabalho:

1. Um EventBridge evento inicia uma função `account_inventory` Lambda a cada 24 horas.
2. Essa função do Lambda consulta o AWS Organizations para obter uma lista de todas as contas IDs, nomes de contas e e-mails de contas da AWS.

3. A função do Lambda `account_inventory` inicia uma função do Lambda `access_key_auto_rotation` para cada ID de conta da AWS e passa os metadados para processamento adicional.
4. A função do Lambda `access_key_auto_rotation` usa um perfil do IAM assumido para acessar a ID da conta da AWS. O script do Lambda executa uma auditoria em todos os usuários e suas chaves de acesso do IAM na conta.
5. Se a idade da chave de acesso do IAM não exceder o limite de melhores práticas, a função do Lambda não tomará nenhuma ação adicional.
6. Se a idade da chave de acesso do IAM tiver excedido o limite de melhores práticas, a função do Lambda `access_key_auto_rotation` determinará qual ação de rotação deve ser executada.
7. Quando uma ação é necessária, a função do Lambda `access_key_auto_rotation` cria e atualiza um segredo no AWS Secrets Manager se uma nova chave for gerada. Também é criada uma política baseada em recursos que permite que somente a entidade principal especificada do IAM acesse e recupere o segredo. No caso da opção 1, as credenciais são armazenadas no Secrets Manager na respectiva conta. No caso da opção 2 (se o sinalizador `StoreSecretsInCentralAccount` estiver definido como Verdadeiro), as credenciais são armazenadas no Secrets Manager na conta de gerenciamento.
8. Uma função do Lambda `notifier` é iniciada para notificar o proprietário da conta sobre a atividade de rotação. Essa função recebe a ID da conta da AWS, o nome da conta, o e-mail da conta e as ações de rotação que foram executadas.
9. A função do Lambda `notifier` consulta o bucket S3 de implantação em busca de um modelo de e-mail e o atualiza dinamicamente com os metadados de atividade relevantes. O e-mail é então enviado para o endereço de e-mail do proprietário da conta.

Observações:

- Essa solução oferece suporte à resiliência em várias zonas de disponibilidade. No entanto, ela não oferece suporte à resiliência em várias regiões da AWS. Para obter suporte em várias regiões, você pode implantar a solução na segunda região e manter a EventBridge regra de rotação de chaves desativada. Em seguida, você pode ativar a regra quando quiser executar a solução na segunda região.
- Você pode executar essa solução no modo de auditoria. No modo de auditoria, as chaves de acesso do IAM não são modificadas, mas um e-mail é enviado para notificar os usuários. Para executar a solução no modo de auditoria, defina o sinalizador `DryRunFlag` como Verdadeiro

ao executar o modelo de rotação de chaves ou na variável de ambiente da função do Lambda `access_key_auto_rotation`.

Automação e escala

Os CloudFormation modelos que automatizam essa solução são fornecidos no repositório de rotação de chaves GitHub do IAM e listados na seção Código. No AWS Organizations, você pode usar CloudFormation StackSetspara implantar o `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` CloudFormation modelo em várias contas em vez de implantar a solução individualmente em cada conta membro.

Ferramentas

Serviços da AWS

- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus recursos da AWS e dos aplicativos que você executa na AWS em tempo real.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Organizations é um serviço de gerenciamento de contas que ajuda a consolidar várias contas da AWS em uma organização que você cria e gerencia de maneira centralizada.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O Amazon Simple Email Service (Amazon SES) ajuda você a enviar e receber e-mails usando seus próprios endereços de e-mail e domínios.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.

- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.
- Os endpoints do Amazon VPC fornecem uma interface para conexão com serviços desenvolvidos pela AWS PrivateLink, incluindo muitos serviços da AWS. Para cada sub-rede que você especifica em sua VPC é criada uma interface de rede de endpoint na sub-rede e atribuído a ela um endereço IP privado do intervalo de endereços da sub-rede.

Código

Os CloudFormation modelos da AWS, os scripts Python e a documentação do runbook necessários estão disponíveis no repositório de rotação de chaves do GitHub IAM. Os modelos são implantados da seguinte forma.

Modelo	Implantar no	Observações
`ASA-iam-key-auto-rotation-and-notifier-solution.yaml`	Conta de implantação	Esse é o modelo principal da solução.
`ASA-iam-key-auto-rotation-iam-assumed-roles.yaml`	Contas de um ou vários membros nas quais você deseja alternar as credenciais	Você pode usar conjuntos de CloudFormation pilhas para implantar esse modelo em várias contas.
`ASA-iam-key-auto-rotation-list-accounts-role.yaml`	Conta da central/do gerenciamento	Use esse modelo para manter um inventário das contas no AWS Organizations.
`ASA-iam-key-auto-rotation-vpc-endpoints.yaml`	Conta de implantação	Use esse modelo para automatizar a criação de endpoints somente se quiser executar as funções do Lambda em uma VPC (defina o parâmetro `RunLambdaInVPC` como Verdadeiro no modelo principal).

Épicos

Configure a solução

Tarefa	Descrição	Habilidades necessárias
Escolha o bucket do S3 de implantação.	Faça login no Console de Gerenciamento da AWS da sua conta, abra o console do Amazon S3 e escolha o bucket S3 para sua implantação. Se quiser implementar a solução para várias contas no AWS Organizations, faça login na conta de gerenciamento da sua organização.	Arquiteto de nuvem
Clonar o repositório.	Clone o repositório de rotação de chaves GitHub do IAM em seu desktop local.	Arquiteto de nuvem
Faça upload dos arquivos no bucket do S3.	Faça upload dos arquivos clonados no bucket do S3. Use a seguinte estrutura de pastas padrão para copiar e colar todos os arquivos e diretórios clonados: `asa/asa-iam-rotation` **Note** Você pode personalizar essa estrutura de pastas nos CloudFormation modelos.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Modifique o modelo de e-mail.	Modifique o modelo de e-mail `iam-auto-key-rotation-enforcement.html` (localizado na pasta `template`) de acordo com seus requisitos. Substitua `[Department Name Here]` no final do modelo pelo nome do seu departamento.	Arquiteto de nuvem

Implante a solução

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo para rotação de chaves.	1. Inicie o modelo `ASA-iam-key-auto-rotation-and-notifier-solution.yaml` na conta de implantação. Para obter mais informações, consulte Seleção de um modelo de pilha na CloudFormation documentação. 2. Especifique valores para parâmetros, incluindo: • CloudFormation Nome do bucket do S3 (`S3BucketName`) — O nome do bucket do S3 de implantação que contém seu código Lambda. • CloudFormation Prefixo do bucket do S3	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	(**`S3BucketPrefix`**) — O prefixo do bucket do S3. • Nome do perfil do IAM assumido (`IAMRoleName`): o nome da função que a função do Lambda `key-rotation` assumirá para girar as chaves. • Nome da função de execução do IAM (`ExecutionRoleName`): o nome da função de execução do IAM usada pela função do Lambda `key-rotation`. • Nome da função de execução do inventário (`InventoryExecutionRoleName`): o nome da função de execução do IAM usada pela função do Lambda `account_inventory`. • Sinalizador de execução a seco (modo de auditoria) (`DryRunFlag`): defina como Verdadeiro para ativar o modo de auditoria (padrão). Defina como	

Tarefa	Descrição	Habilidades necessárias
	Falso para ativar o modo de aplicação. • Conta para listar contas da organizaç ão(`OrgListAccount`): a ID da conta central/ de gerenciamento que será usado para listar as contas na organização. • Nome da função da lista de contas (`OrgListRo le`): o nome da função que será usado para listar as contas na organização. • Sinalizador Secrets Store para conta central (`StoreSecr etsInCent ralAccount`): defina como Verdadeiro para armazenar segredos na conta central. Defina como Falso para armazenar segredos na respectiva conta. • Regiões para replicar as credenciais (`Credentia lReplicat ionRegions`): as regiões da AWS onde você deseja replicar as credenciais (Secrets Manager), separadas por	

Tarefa	Descrição	Habilidades necessárias
	vírgulas; por exemplo, `us-east-2,us-west-1,us-west-2` . Pule a região em que você está criando a pilha. • Executar Lambda em VPC (`RunLambdaInVpc`): defina como Verdadeiro para executar funções do Lambda em uma VPC especific ada. Você deve ter endpoints da VPC criados e conectar um gateway NAT à sub-rede que contém a função do Lambda. Para obter mais informações, consulte o artigo re:Post sobre essa opção. • ID da VPC para funções do Lambda (`VpcId`), CIDR de VPC para regra de grupo de segurança (`VpcCidr`) e ID de sub-rede para funções do Lambda (`SubnetId`): forneça informações sobre a VPC, CIDR e sub-rede se você definir `RunLambdaInVpc` como Verdadeiro. • Endereço de e-mail do administr	

Tarefa	Descrição	Habilidades necessárias
	ador (`AdminEmailAddress`): um endereço de e-mail válido para enviar notificações. • ID do AWS Organizations (`AWSOrgID`): a ID exclusiva da sua organização. Esse ID começa com `o-` e é seguido por 10 a 32 letras minúsculas ou dígitos. • Nome do arquivo do modelo de e-mail [Modo de auditoria] (`EmailTemplateAudit`) e [Modo de aplicação] (`EmailTemplateEnforce`): o nome do arquivo do modelo HTML de e-mail a ser enviado pelo módulo `notifier` para o modo de auditoria e o modo de aplicação. • Nome do parâmetro SSM do usuário SMTP (`SMTPUserParamName`) e senha SMTP Nome do parâmetro SSM (`SMTPPasswordParamName`): informações de usuário	

Tarefa	Descrição	Habilidades necessárias
	e senha para o Simple Mail Transfer Protocol (SMTP).	

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo para funções assumidas.	1. No CloudFormation console da AWS, execute o `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` modelo para cada conta em que você deseja alternar as chaves. Se você tiver mais de uma conta, poderá implantar o CloudFormation modelo principal em sua conta de gerenciamento como uma pilha e implantar o `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` modelo com conjuntos de CloudFormation pilhas em todas as contas necessárias. Para obter mais informações, consulte Como trabalhar com a AWS CloudFormation StackSets na CloudFormation documentação. 2. Especifique os seguintes parâmetros e valores: • Nome do perfil do IAM assumido (`IAMRoleName`): nome do perfil do IAM que será assumido pela função do Lambda `access_key_auto_ro`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`tation` . Você pode manter o valor padrão. • Nome da função de execução do IAM (`Execution RoleName`): o perfil do IAM que assumirá a função de subconta para executar a função do Lambda. • ID da conta primária da AWS (`PrimaryAc countID`): a ID da conta da AWS em que o modelo principal será implantado. • Grupo de isenção do IAM (`IAMExempt ionGroup`): a nome do grupo do IAM que está sendo usado para facilitar as contas do IAM que você deseja excluir da rotação automática de chaves.	

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo para o inventário da conta.	1. Inicie o modelo `ASA-iam-key-auto-rotation-list-accounts-role.yaml` na conta de gerenciamento/central 2. Especifique os seguintes parâmetros e valores: • Nome do perfil do IAM assumido (`IAMRoleName`): nome do perfil do IAM que a função do Lambda `access_key_auto_rotation` assumirá. • Nome da função de execução do IAM para a conta Lambda (`AccountExecutionRoleName`): o nome do perfil do IAM que a função do Lambda `notifier` assumirá. • Nome da função de execução do IAM para rotação Lambda (`RotationExecutionRoleName`): o nome do perfil do IAM que a função do Lambda `access_key_auto_rotation` assumirá. • ID da conta primária da AWS (`PrimaryAc`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`countID`): a ID da conta da AWS em que o modelo principal será implantado.	
Inicie o CloudFormation modelo para VPC endpoints.	Esta tarefa é opcional. 1. Inicie o modelo `ASA-iam-key-auto-rotation-vpc-endpoints.yaml` na conta de implantação. 2. Especifique os seguintes parâmetros e valores: • VPC ID (`pVpcId`), ID de sub-rede (`pSubnetId`) e intervalo CIDR para VPC (**`pVPCCidr`**): forneça informações sobre VPC, CIDR e sub-rede. • Defina o parâmetro para cada endpoint da VPC como Verdadeiro. Se você já tem endpoints, pode escolher Falso.	Arquiteto de nuvem

Recursos relacionados

- Práticas recomendadas de segurança no IAM (documentação do IAM)
- AWS Organizations e funções vinculadas ao serviço (documentação do AWS Organizations)
- Seleção de um modelo de pilha (CloudFormation documentação)
- Trabalhando com a AWS CloudFormation StackSets (CloudFormation documentação)

Valide e implante automaticamente políticas e funções do IAM em uma conta da AWS usando o CodePipeline IAM Access Analyzer e macros da AWS CloudFormation

Criado por Helton Ribeiro (AWS) e Guilherme Simoes (AWS)

Resumo

Aviso: CodeCommit A AWS não está mais disponível para novos clientes. Os clientes atuais da AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais.

Esse padrão descreve as etapas e fornece código para criar um pipeline de implantação que permite que suas equipes de desenvolvimento criem políticas e perfis do AWS Identity and Access Management (IAM) em suas contas da Amazon Web Services (AWS). Essa abordagem ajuda sua organização a reduzir a sobrecarga de suas equipes operacionais e acelerar o processo de implantação. Também ajuda seus desenvolvedores a criar funções e políticas do IAM que sejam compatíveis com seus controles de governança e segurança existentes.

A abordagem desse padrão usa o AWS Identity and Access Management Access Analyzer para validar as políticas do IAM que você deseja anexar às funções do IAM e usa a AWS CloudFormation para implantar as funções do IAM. No entanto, em vez de editar diretamente o arquivo de CloudFormation modelo da AWS, sua equipe de desenvolvimento cria políticas e funções do IAM formatadas em JSON. Uma CloudFormation macro da AWS transforma esses arquivos de política formatados em JSON em tipos de recursos CloudFormation do AWS IAM antes de iniciar a implantação.

O pipeline de implantação (`RolesPipeline`) tem estágios de origem, validação e implantação. Durante o estágio de origem, sua equipe de desenvolvimento envia os arquivos JSON que contêm a definição das funções e políticas do IAM para um repositório da AWS CodeCommit . CodeBuild Em seguida, a AWS executa um script para validar esses arquivos e os copia em um bucket do Amazon Simple Storage Service (Amazon S3). Como suas equipes de desenvolvimento não têm acesso direto ao arquivo de CloudFormation modelo da AWS armazenado em um bucket S3 separado, elas devem seguir o processo de criação e validação do arquivo JSON.

Finalmente, durante a fase de implantação, a AWS CodeDeploy usa uma CloudFormation pilha da AWS para atualizar ou excluir as políticas e funções do IAM em uma conta.

> **Important**
>
> O fluxo de trabalho desse padrão é uma prova de conceito (POC) e recomendamos que você o use somente em um ambiente de teste. Se você quiser usar a abordagem desse padrão em um ambiente de produção, consulte Práticas recomendadas de segurança em IAM na documentação do IAM e faça as alterações necessárias nos seus perfis do IAM e nos serviços da AWS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket S3 novo ou existente para o pipeline `RolesPipeline`. Garanta que as credenciais de acesso que você está usando tenham permissões para carregar objetos nesse bucket.
- AWS Command Line Interface (AWS CLI), instalada e configurada. Para obter mais informações, consulte Instalação, atualização e desinstalação da AWS CLI na documentação da AWS CLI.
- CLI do AWS Serverless Application Model (AWS SAM), instalada e configurada. Para obter mais informações sobre isso, consulte Instalação da CLI do AWS SAM na documentação do AWS SAM.
- Python 3, instalado na sua máquina local. Para obter mais informações, consulte a documentação do Pyton.
- Um cliente Git, instalado e configurado.
- O GitHub `IAM roles pipeline` repositório, clonado em sua máquina local.
- Políticas e perfis do IAM existentes em formato JSON. Para obter mais informações sobre isso, consulte o ReadMearquivo no `IAM roles pipeline` repositório Github.
- Sua equipe de desenvolvedores não deve ter permissões para editar a AWS e CodePipeline CodeBuild os CodeDeploy recursos dessa solução.

Limitações

- O fluxo de trabalho desse padrão é uma prova de conceito (POC) e recomendamos que você o use somente em um ambiente de teste. Se você quiser usar a abordagem desse padrão em um

ambiente de produção, consulte Práticas recomendadas de segurança em IAM na documentação do IAM e faça as alterações necessárias nos seus perfis do IAM e nos serviços da AWS.

Arquitetura

O diagrama a seguir mostra como validar e implantar automaticamente funções e políticas do IAM em uma conta usando o CodePipeline IAM Access Analyzer e macros da AWS CloudFormation .

O diagrama mostra o seguinte fluxo de trabalho:

1. Um desenvolvedor grava arquivos JSON que contêm as definições das políticas e perfis do IAM. O desenvolvedor envia o código para um CodeCommit repositório e, em CodePipeline seguida, inicia o pipeline. `RolesPipeline`
2. CodeBuild valida os arquivos JSON usando o IAM Access Analyzer. Se houver alguma descoberta relacionada a erros ou segurança, o processo de implantação será interrompido.
3. Se não houver descobertas relacionadas a erros ou segurança, os arquivos JSON serão enviados para o bucket do S3 `RolesBucket`.
4. Em seguida, uma CloudFormation macro da AWS implementada como uma função do AWS Lambda lê os arquivos JSON do `RolesBucket` bucket e os transforma em tipos de recursos do AWS CloudFormation IAM.
5. Uma CloudFormation pilha predefinida da AWS instala, atualiza ou exclui as políticas e funções do IAM na conta.

Automação e escala

CloudFormation Os modelos da AWS que implantam automaticamente esse padrão são fornecidos no repositório do pipeline de funções GitHub do IAM.

Ferramentas

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

- O IAM Access Analyzer ajuda você a identificar os recursos em sua organização e suas contas, como buckets do S3 ou funções do IAM, que são compartilhados com uma entidade externa. Isso ajuda a identificar o acesso não intencional aos seus recursos e dados.
- O AWS Serverless Application Model (AWS SAM) é uma estrutura de código aberto que ajuda na criação de aplicativos sem servidor na Nuvem AWS.

Código

O código-fonte e os modelos desse padrão estão disponíveis no repositório do pipeline de funções GitHub do IAM.

Épicos

Clone o repositório

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de amostras.	Clone o repositório do pipeline de funções GitHub do IAM em sua máquina local.	Desenvolvedor de aplicativos, AWS geral

Implante o RolesPipeline pipeline

Tarefa	Descrição	Habilidades necessárias
Implante o pipeline.	1. Navegue até o diretório que contém o repositório clonado. 2. **Important** Execute o `make deploy bucket=<bucket_name>` comando.: você deve <bucket_n	Desenvolvedor de aplicativos, AWS geral

Tarefa	Descrição	Habilidades necessárias
	ame> substitui r pelo nome do bucket do S3 existente. 3. Execute o comando `aws codepipeline get-pipeline –name RolesPipeline` para verificar se sua implantação foi bem-sucedida.	
Clone o repositório do pipeline.	1. A CloudFormation pilha `RolesPipeline` da AWS cria o `roles-pipeline-repo` CodeCommit repositório. 2. Faça login no Console de Gerenciamento da AWS, abra o CodeCommit console da AWS e copie a URL do CodeCommit repositório para cloná-la em sua máquina local. Para obter mais informações sobre isso, consulte Conecte-se a um CodeCommit repositório da AWS na CodeCommit documentação da AWS.	Desenvolvedor de aplicativos, AWS geral

Teste o RolesPipeline pipeline

Tarefa	Descrição	Habilidades necessárias
Teste o RolesPipeline pipeline com políticas e funções válidas do IAM.	1. Crie arquivos JSON para suas políticas e perfis do IAM. Você pode usar as amostras no `role-example` diretório do GitHub `IAM roles pipeline` repositório. 2. **Important** Defina suas políticas e perfis do IAM com as configurações necessárias. : certifique-se de seguir o formato descrito no `ReadMe` arquivo do GitHub `IAM roles pipeline` repositório. 3. Envie as modificações para o `roles-pipeline-repo` CodeCommit repositório. 4. Verifique a implementação do pipeline `RolesPipeline` . 5. Certifique-se de que as políticas e perfis do IAM	Desenvolvedor de aplicativos, AWS geral

Tarefa	Descrição	Habilidades necessárias
	estejam implantadas corretamente na conta. 6. Valide se há um limite de permissões associado às políticas ou funções do IAM. Para obter mais informações sobre isso, consulte Limites de permissões para identidades do IAM na documentação do IAM.	
Teste o RolesPipeline pipeline com políticas e funções inválidas do IAM.	1. Modifique o `roles-pipeline-repo` CodeCommit repositório e inclua funções ou políticas inválidas do IAM. Por exemplo, você pode usar uma ação que não existe ou uma versão inválida da política do IAM. 2. Verifique a implementação do pipeline. O IAM Access Analyzer interrompe o pipeline durante o estágio de validação se detectar políticas ou perfis inválidos do IAM.	Desenvolvedor de aplicativos, AWS geral

Limpe os seus recursos

Tarefa	Descrição	Habilidades necessárias
Preparar para a limpeza.	Esvazie os buckets do S3 e execute o comando `destroy`.	Desenvolvedor de aplicativos, AWS geral
Exclua a RolesStack pilha.	1. O `RolesPipeline` pipeline cria uma CloudFormation pilha `RolesStack` da AWS que implanta as políticas e funções do IAM. Você deve excluir essa pilha antes de excluir o pipeline `RolesPipeline` . 2. Faça login no Console de Gerenciamento da AWS, abra o CloudFormation console da AWS, escolha a `RolesStack` pilha e escolha Excluir.	Desenvolvedor de aplicativos, AWS geral
Exclua a RolesPipeline pilha.	Para excluir a CloudFormation pilha `RolesPipeline` da AWS, siga as instruções do ReadMearquivo no repositór io do Github. `IAM roles pipeline`	Desenvolvedor de aplicativos, AWS geral

Recursos relacionados

- Validação de política do IAM Access Analyzer (Blog da notícias da AWS)
- Usando CloudFormation macros da AWS para realizar processamento personalizado em modelos (CloudFormation documentação da AWS)
- Criar funções do Lambda com Python (documentação do AWS Lambda)

Integre bidirecionalmente AWS Security Hub com o software Jira

Criado por Joaquin Rinaudo (AWS)

Resumo

Essa solução oferece suporte a uma integração bidirecional entre AWS Security Hub e o Jira. Usando essa solução, você pode criar e atualizar tíquetes do Jira de forma automática e manual a partir das descobertas do Security Hub. As equipes de segurança podem usar essa integração para notificar as equipes de desenvolvedores sobre descobertas graves de segurança que exigem ação.

A solução permite que você:

- Selecione quais controles do Security Hub criam ou atualizam automaticamente os tíquetes no Jira.
- No console do Security Hub, use as ações personalizadas do Security Hub para escalar manualmente os tíquetes no Jira.
- Atribua tickets automaticamente no Jira com base nas Conta da AWS tags definidas em AWS Organizations. Se essa tag não for definida, um destinatário padrão será usado.
- Suprima automaticamente as descobertas do Security Hub marcadas como falso positivo ou risco aceito no Jira.
- Feche automaticamente um tíquete do Jira quando sua descoberta relacionada for arquivada no Security Hub.
- Reabra os tíquetes do Jira quando as descobertas do Security Hub ocorrerem novamente.

Fluxo de trabalho do Jira

A solução usa um fluxo de trabalho personalizado do Jira que permite aos desenvolvedores gerenciar e documentar riscos. À medida que o problema avança no fluxo de trabalho, a integração bidirecional garante que o status do tíquete do Jira e a descoberta do Security Hub sejam sincronizados entre os fluxos de trabalho em ambos os serviços. Este fluxo de trabalho é um derivado do SecDevOps Risk Workflow de Dinis Cruz, licenciado sob a versão 2.0 da Licença Apache. Recomendamos adicionar uma condição de fluxo de trabalho do Jira para que somente membros da sua equipe de segurança possam alterar o status do tíquete.

Para ver um exemplo de um tíquete do Jira gerado automaticamente por essa solução, consulte a seção Informações adicionais desse padrão.

Pré-requisitos e limitações

Pré-requisitos

- Se você quiser implantar essa solução em um AWS ambiente com várias contas:
  - Seu ambiente de várias contas está ativo e é gerenciado por AWS Organizations.
  - O Security Hub está habilitado em seu Contas da AWS.
  - Em AWS Organizations, você designou uma conta de administrador do Security Hub.
  - Você tem uma função entre contas AWS Identity and Access Management (IAM) que tem `AWSOrganizationsReadOnlyAccess` permissões para a conta AWS Organizations de gerenciamento.
  - (Opcional) Você marcou seu Contas da AWS com`SecurityContactID`. Essa tag é usada para atribuir tíquetes do Jira aos contatos de segurança definidos.
- Se você quiser implantar essa solução em uma única solução Conta da AWS:
  - Você tem uma Conta da AWS ativa.
  - O Security Hub está habilitado em seu Conta da AWS.
- Uma instância do Jira Data Center

> **Important**
>
> Essa solução oferece suporte ao uso do Jira Cloud. No entanto, o Jira Cloud não suporta a importação de fluxos de trabalho XML, então você precisa recriar manualmente o fluxo de trabalho no Jira. Você pode encontrar as transições e o status no GitHub repositório.

- Permissões de administrador no Jira
- Use um dos seguintes tokens do Jira:
  - Para o Jira Enterprise, um token de acesso pessoal (PAT). Para obter mais informações, consulte Uso de tokens de acesso pessoal (suporte da Atlassian).
  - Para o Jira Cloud, um token da API do Jira. Para obter mais informações, consulte Gerenciamento de tokens de API (suporte da Atlassian).

Arquitetura

Esta seção ilustra a arquitetura da solução em vários cenários, como quando o desenvolvedor e o engenheiro de segurança decidem aceitar o risco ou resolver o problema.

Cenário 1: o desenvolvedor resolve o problema

1. O Security Hub gera uma descoberta em relação a um controle de segurança específico, como os do padrão AWS Foundational Security Best Practices.
2. Um CloudWatch evento da Amazon associado à descoberta e à `CreateJIRA` ação inicia uma AWS Lambda função.
3. A função do Lambda usa seu arquivo de configuração e o campo `GeneratorId` da descoberta para avaliar se ela deve escalar a descoberta.
4. A função Lambda determina que a descoberta deve ser escalada e obtém a etiqueta da conta AWS Organizations na `SecurityContactID` conta de gerenciamento. AWS Esse ID está associado ao desenvolvedor e é usado como ID do destinatário do tíquete do Jira.
5. A função Lambda usa as credenciais armazenadas AWS Secrets Manager para criar um ticket no Jira. O Jira notifica o desenvolvedor.
6. O desenvolvedor aborda a descoberta de segurança subjacente e, no Jira, altera o status do tíquete para `TEST FIX`.
7. O Security Hub atualiza a descoberta como `ARCHIVED`, à medida que um novo evento é gerado. Esse evento faz com que a função do Lambda encerre o tíquete do Jira automaticamente.

Cenário 2: o desenvolvedor decide aceitar o risco

1. O Security Hub gera uma descoberta em relação a um controle de segurança específico, como os do padrão AWS Foundational Security Best Practices.
2. Um CloudWatch evento associado à descoberta e à `CreateJIRA` ação inicia uma função Lambda.
3. A função do Lambda usa seu arquivo de configuração e o campo `GeneratorId` da descoberta para avaliar se ela deve escalar a descoberta.
4. A função Lambda determina que a descoberta deve ser escalada e obtém a etiqueta da conta AWS Organizations na `SecurityContactID` conta de gerenciamento. AWS Esse ID está associado ao desenvolvedor e é usado como ID do destinatário do tíquete do Jira.

5. A função do Lambda usa as credenciais armazenadas no Secrets Manager para criar um tíquete no Jira. O Jira notifica o desenvolvedor.
6. O desenvolvedor decide aceitar o risco e, no Jira, altera o status do tíquete para `AWAITING RISK ACCEPTANCE`.
7. O engenheiro de segurança analisa a solicitação e considera a justificativa comercial apropriada. O engenheiro de segurança altera o status do tíquete do Jira para `ACCEPTED RISK`. Isso fecha o tíquete do Jira.
8. Um evento CloudWatch diário inicia a função de atualização do Lambda, que identifica tickets fechados do Jira e atualiza suas descobertas relacionadas ao Security Hub como. `SUPPRESSED`

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- O Amazon CloudWatch Events ajuda você a monitorar eventos do sistema para seus AWS recursos usando regras para combinar eventos e encaminhá-los para funções ou fluxos.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS. Também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança.

Repositório de código

O código desse padrão está disponível em GitHub, no repositório aws-securityhub-jira-software-integration. Ele inclui o código de amostra e o fluxo de trabalho do Jira para essa solução.

Épicos

Configurar o Jira

Tarefa	Descrição	Habilidades necessárias
Implantar o fluxo de trabalho.	Como administrador no Jira, importe o `issue-workflow.xml` arquivo para sua instância do Jira Data Center. Se você usa o Jira Cloud, precisa criar o fluxo de trabalho de acordo com os `assets/jira-cloud-status.png` arquivos `assets/jira-cloud-transitions.png` e. Os arquivos podem ser encontrados no repositório aws-securityhub-jira-software-integration em. GitHub Para obter instruções, consulte Uso do XML para criar um fluxo de trabalho (documentação do Jira).	Administrador do Jira
Ative e atribua o fluxo de trabalho.	Os fluxos de trabalho ficam inativos até que você os atribua a um esquema de fluxo de trabalho. Em seguida, você atribui o esquema do fluxo de trabalho a um projeto. 1. Para seu projeto, certifique-se de ter identificado um esquema de tipo de problema para o projeto.	Administrador do Jira

Tarefa	Descrição	Habilidades necessárias
	Você pode criar um novo tipo de problema ou selecionar um existente, como Bug. 2. Atribua o fluxo de trabalho importado a um esquema de fluxo de trabalho de acordo com as instruções em Ativar um fluxo de trabalho (documentação do Jira). 3. Atribua o esquema de fluxo de trabalho a um projeto de acordo com as instruções em Associar um esquema de fluxo de trabalho a um projeto (documentação do Jira).	

Estabeleça os parâmetros da solução

Tarefa	Descrição	Habilidades necessárias
Configure os parâmetros da solução.	1. Na pasta conf, abra `params_prod.shfile` . 2. Forneça valores para os parâmetros a seguir: • `ORG_ACCOUNT_ID` — O ID da conta da sua conta AWS Organizations de gerenciamento. A solução lê as tags da conta e atribui tickets aos	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	contatos de segurança específicos definidos nessas Conta da AWS tags. • `ORG_ROLE`— O nome da função do IAM usada para acessar a conta AWS Organizations de gerenciamento. Esse perfil deve ter `OrganizationsReadOnlyAccess` permissões. • `EXTERNAL_ID` : um parâmetro opcional se você estiver usando um ID externo para assumir o perfil do IAM definido em `ORG_ROLE`. Para obter mais informações, consulte Como usar uma ID externa (document ação do IAM). • `JIRA_DEFAULT_ASSIGNEE` — Esse é o responsável padrão do Jira para todos os problemas de segurança. Esse destinatário padrão é usado caso a conta não esteja marcada corretamente ou a função não possa ser assumida.	

Tarefa	Descrição	Habilidades necessárias
	• `JIRA_INSTANCE` — O endereço HTTPS do seu endpoint Jira no seguinte formato: `team-<team-id>.atlassian.net/` • `JIRA_PROJECT_KEY` : o nome da chave do projeto Jira usada para criar tíquetes, como `SEC` ou `TEST`. Esse projeto já deve existir no Jira. • `ISSUE_TYPE` : o nome do esquema de tipo de problema atribuído ao projeto no Jira, como `Bug` ou `Security Issue`. • `REGIONS`— Lista de Região da AWS códigos nos quais você deseja implantar essa solução, como`eu-west-1` . 3. Salve e feche o arquivo de parâmetros da solução.	

Tarefa	Descrição	Habilidades necessárias
Identifique as descobertas que você deseja automatizar.	1. Abra o console do Security Hub. 2. No painel de navegação do Security Hub, selecione Descobertas. 3. Selecione o título da descoberta. 4. Selecione o ID da descoberta. Isso exibe o JSON completo da descoberta. 5. No JSON, copie a string no campo `GeneratorId` . Esse valor está em AWS Security Finding Format (ASFF). Por exemplo, `aws-foundational-security-best-practices/v/1.0.0/S3.1` corresponde às descobertas do controle de segurança S3.1. A configuração S3 Block Public Access deve estar ativada. 6. Repita essas etapas até copiar todos os valores de `GeneratorID` das descobertas que você deseja automatizar.	

Tarefa	Descrição	Habilidades necessárias
Adicione as descobertas ao arquivo de configuração.	1. Em src/code, abra o arquivo `config.jsonconfig` . 2. Cole os valores `GeneratorID` recuperados na história anterior no parâmetro `default` e use vírgulas para separar cada ID. 3. Salve e feche o arquivo de configuração. O exemplo de código a seguir mostra como automatizar as descobertas `aws-foundational-security-best-practices/v/1.0.0/SNS.1` e `aws-foundational-security-best-practices/v/1.0.0/S3.1` . `{ "Controls" : { "eu-west-1": [ "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22" ], "default": [ aws-foundational-security-best-practices/v/1.0.0/SNS.1,`	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>aws-foundational-
	security-best-p
	ractices/v/1.0.0/S3.1
	]
	}
	}</pre>
	Note
	Você pode optar por automatizar descobert as diferentes para cada uma Região da AWS. Uma boa prática para ajudar a evitar descobertas duplicada s é selecionar uma única região para automatizar a criação de controles relaciona dos ao IAM.	

Implantar a integração

Tarefa	Descrição	Habilidades necessárias
Implantar a integração.	Em um terminal de linha de comando, digite o seguinte comando: <pre>./deploy.sh prod</pre>	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
Faça o upload das credencia is do Jira para o Secrets Manager.	1. Abra o console do Secrets Manager. 2. Em Secrets (Segredos), escolha Store a new secret (Armazenar um novo segredo). 3. Em Tipo de segredo, escolha Outro tipo de segredo. 4. Se você estiver usando o Jira Enterprise, faça o seguinte para pares de chave/valor: • Na primeira linha, insira `auth` na caixa chave e, em seguida, insira `token_auth` na caixa de valor. • Adicione uma segunda linha, insira `token` na caixa da chave e, em seguida, insira seu token de acesso pessoal na caixa de valor. Se você estiver usando o Jira Cloud, faça o seguinte para pares de chave/valor: • Na primeira linha, insira `auth` na caixa chave e, em seguida, insira `basic_auth` na caixa de valor.	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	• Adicione uma segunda linha, insira `token` na caixa de chave e, em seguida, insira seu token de API na caixa de valor. • Adicione uma terceira linha, insira `email` na caixa chave e, em seguida, insira seu endereço de e-mail na caixa de valor. 5. Escolha Próximo. 6. Para o Nome do segredo, insira `Jira-Token` e, na parte inferior da página, escolha Próximo. 7. Na página Secret rotation (Alternância do segredo), mantenha Disable automatic rotation (Desabilitar alternância automática) e, em seguida, na parte inferior da página, escolha Next (Próximo). 8. Na página Review (Revisar), revise os detalhes do segredo e escolha Store (Armazenar).	

Tarefa	Descrição	Habilidades necessárias
Crie a ação personalizada do Security Hub.	1. Para cada um Região da AWS, no AWS Command Line Interface (AWS CLI), use o create-action-targetcomando para criar uma ação personalizada do Security Hub chamada`CreateJiraIssue` . `aws securityhub create-action-target --name "CreateJiraIssue" --description "Create ticket in JIRA" --id "CreateJiraIssue" --region $<aws-region>` 2. Abra o console do Security Hub. 3. No painel de navegação do Security Hub, selecione Descobertas. 4. Na lista de descobertas, selecione as que você deseja escalar. 5. No menu Ações, selecione `CreateJiraIssue` .	Administrador de sistemas AWS

Recursos relacionados

- AWS Conector de gerenciamento de serviços para o Jira Service Management
- AWS Padrão básico de melhores práticas de segurança

Mais informações

Exemplo de um tíquete do Jira

Quando ocorre uma descoberta específica do Security Hub, essa solução cria automaticamente um tíquete do Jira. O tíquete inclui as seguintes informações:

- Título: o título identifica o problema de segurança no seguinte formato:

```
AWS Security Issue :: <AWS account ID> :: <Security Hub finding title>
```

- Descrição: a seção de descrição do tíquete descreve o controle de segurança associado à descoberta, inclui um link para a descoberta no console do Security Hub e fornece uma breve descrição de como lidar com o problema de segurança no fluxo de trabalho do Jira.

Veja a seguir um exemplo de um tíquete do Jira gerado automaticamente.

Título	AWS Problema de segurança:: 012345678 912:: Lambda.1 As políticas da função Lambda devem proibir o acesso público.
Descrição	Qual é o problema? Detectamos uma descoberta de segurança no Conta da AWS 012345678912 pelo qual você é responsável. Esse controle verifica se a política de AWS Lambda função anexada ao recurso Lambda proíbe o acesso público. Se a política da função do Lambda permitir acesso público, o controle falhará. <Link para descoberta do Security Hub>

O que devo fazer com o tíquete?

- Acesse a conta e verifique a configuração. Reconheça o trabalho no tíquete movendo-o para “Alocado para correção”. Depois de corrigido, movido para a correção de teste para que a segurança valide que o problema foi resolvido.
- Se você acha que o risco deve ser aceito, mova-o para “Aguardando aceitação do risco”. Isso exigirá a revisão de um engenheiro de segurança.
- Se você achar que é um falso positivo, faça a transição para “Marcar como falso positivo” . Isso será revisado por um engenheiro de segurança e reabrido/fechado adequadamente.

Crie um pipeline para imagens de contêiner reforçadas usando o EC2 Image Builder e o Terraform

Criado por Mike Saintcross (AWS) e Andrew Ranes (AWS)

Resumo

Esse padrão cria um pipeline do EC2 Image Builder que produz uma imagem reforçada de contêiner base do Amazon Linux 2. O Terraform é usado como uma ferramenta de infraestrutura como código (IaC) para configurar e provisionar a infraestrutura usada para criar imagens de contêiner reforçadas. A fórmula ajuda você a implementar uma imagem de contêiner Amazon Linux 2 baseada em Docker que foi reforçada de acordo com o Red Hat Enterprise Linux (RHEL) 7 STIG Version 3 Release 7 – Medium. (Consulte a STIG-Build-Linux-Medium versão 2022.2.1 na seção de componentes Linux STIG da documentação do EC2 Image Builder.) Isso é chamado de imagem de contêiner dourado.

A compilação inclui duas EventBridge regras da Amazon. Uma regra inicia o pipeline de imagens do contêiner quando a descoberta do Amazon Inspector é Alta ou Crítica para que imagens não seguras sejam substituídas. Esta regra exige que a verificação aprimorada do Amazon Inspector e do Amazon Elastic Container Registry (Amazon ECR) seja ativada. A outra regra envia notificações para uma fila do Amazon Simple Queue Service (Amazon SQS) após um envio bem-sucedido de imagens para o repositório do Amazon ECR, para ajudá-lo a usar as imagens de contêiner mais recentes.

> **Note**
>
> O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da AWS na qual você pode implementar a infraestrutura.
- AWS Command Line Interface (AWS CLI) instalada para definir suas credenciais da AWS para implantação local.
- O Terraform foi baixado e configurado seguindo as instruções na documentação do Terraform.

- Git (se você estiver provisionando a partir de uma máquina local).
- Uma função dentro da conta da AWS que você pode usar para criar recursos da AWS.
- Todas as variáveis definidas no arquivo.tfvars. Ou você pode definir todas as variáveis ao aplicar a configuração do Terraform.

Limitações

- Essa solução cria uma infraestrutura de Amazon Virtual Private Cloud (Amazon VPC) que inclui um gateway NAT e um gateway da internet para conectividade com a internet a partir de sua sub-rede privada. Você não pode usar VPC endpoints, porque o processo de bootstrap do AWS Task Orchestrator and Executor () instala a AWSTOE AWS CLI versão 2 da Internet.

Versões do produto

- Amazon Linux 2
- AWS CLI versão 1.1 ou superior

Arquitetura

Pilha de tecnologias de destino

Esse padrão cria 43 recursos, incluindo:

- Dois buckets do Amazon Simple Storage Service (Amazon S3): um para os arquivos de componentes do pipeline e outro para o acesso ao servidor e registros de fluxo do Amazon VPC
- Um Repositório do Amazon ECR
- Uma nuvem privada virtual (VPC) que contém uma sub-rede pública, uma sub-rede privada, tabelas de rotas, um gateway NAT e um gateway da Internet
- Um pipeline, receita e componentes do EC2 Image Builder
- Uma imagem do contêiner
- Uma chave do AWS Key Management Service (AWS KMS) para criptografia de imagens
- Uma fila do SQS.
- Três funções: uma para executar o pipeline do EC2 Image Builder, um perfil de instância para o EC2 Image Builder e outra para EventBridge regras
- Duas EventBridge regras

Estrutura do módulo Terraform

Para obter o código-fonte, consulte o GitHub repositório Terraform EC2 Image Builder Container Hardening Pipeline.

```
### components.tf
### config.tf
### dist-config.tf
### files
#   ###assumption-policy.json
### hardening-pipeline.tfvars
### image.tf
### infr-config.tf
### infra-network-config.tf
### kms-key.tf
### main.tf
### outputs.tf
### pipeline.tf
### recipes.tf
### roles.tf
### sec-groups.tf
### trigger-build.tf
### variables.tf
```

Detalhes do módulo

- `components.tf`contém um recurso de upload do Amazon S3 para carregar o conteúdo do `/files` diretório. Você também pode adicionar modularmente arquivos YAML de componentes personalizados aqui.
- `/files`contém os `.yml` arquivos que definem os componentes usados em`components.tf`.
- `image.tf`contém as definições do sistema operacional da imagem base. É aqui que você pode modificar as definições de um pipeline de imagem base diferente.
- `infr-config.tf`e `dist-config.tf` contenha os recursos para a infraestrutura mínima da AWS necessária para ativar e distribuir a imagem.
- `infra-network-config.tf`contém a infraestrutura mínima de VPC na qual implementar a imagem do contêiner.
- `hardening-pipeline.tfvars`contém as variáveis do Terraform a serem usadas no momento da aplicação.
- `pipeline.tf`cria e gerencia um pipeline do EC2 Image Builder no Terraform.

- `recipes.tf`é onde você pode especificar diferentes misturas de componentes para criar fórmulas em contêineres.
- `roles.tf`contém as definições de política do AWS Identity and Access Management (IAM) para o perfil da instância do Amazon Elastic Compute Cloud (Amazon EC2) e a função de implantação do pipeline.
- `trigger-build.tf`contém as EventBridge regras e os recursos da fila SQS.

Arquitetura de destino

O diagrama a seguir mostra o fluxo de trabalho:

1. EC2 O Image Builder cria uma imagem de contêiner usando a receita definida, que instala atualizações do sistema operacional e aplica o RHEL Medium STIG à imagem base do Amazon Linux 2.
2. A imagem protegida é publicada em um registro privado do Amazon ECR, e uma EventBridge regra envia uma mensagem para uma fila do SQS quando a imagem é publicada com sucesso.
3. Se o Amazon Inspector estiver configurado para escaneamento aprimorado, ele escaneia o registro do Amazon ECR.
4. Se o Amazon Inspector gerar uma descoberta de severidade crítica ou alta para a imagem, uma EventBridge regra acionará o pipeline do Image Builder para ser executado novamente e publicar uma EC2 imagem recém-reforçada.

Automação e escala

- Esse padrão descreve como provisionar a infraestrutura e criar o pipeline em seu computador. No entanto, ele se destina a ser usado em grande escala. Em vez de implementar os módulos do Terraform localmente, você pode usá-los em um ambiente de várias contas, como um ambiente do AWS Control Tower com Account Factory for Terraform. Nesse caso, você deve usar um bucket S3 de estado de backend para gerenciar arquivos de estado do Terraform em vez de gerenciar o estado de configuração localmente.
- Para uso escalonado, implante a solução em uma conta central, como uma conta de Serviços Comuns ou Serviços Comuns, a partir de um modelo de conta Control Tower ou zona de pouso, e conceda às contas dos consumidores permissão para acessar o repositório do Amazon ECR e a chave do AWS KMS. Para obter mais informações sobre a configuração, consulte o artigo do re:POST Como posso permitir que uma conta secundária envie ou extraia imagens no meu

repositório de imagens do Amazon ECR? Por exemplo, em uma máquina de venda automática de contas ou Account Factory for Terraform, adicionar permissões a cada linha de base da conta ou linha de base de personalização da conta para fornecer acesso ao repositório e à chave de criptografia do Amazon ECR.

- Depois que o pipeline de imagem do contêiner for implantado, você poderá modificá-lo usando os recursos do EC2 Image Builder, como componentes, que ajudam a empacotar mais componentes na compilação do Docker.
- A chave do AWS KMS usada para criptografar a imagem do contêiner deve ser compartilhada entre as contas nas quais a imagem deve ser usada.
- Você pode adicionar suporte para outras imagens duplicando todo o módulo Terraform e modificando os seguintes atributos: `recipes.tf`
  - Modifique `parent_image = "amazonlinux:latest"` para outro tipo de imagem.
  - Modifique `repository_name` para apontar para um repositório Amazon ECR existente. Isso cria outro pipeline que implanta um tipo diferente de imagem principal em seu repositório Amazon ECR existente.

Ferramentas

Ferramentas

- Terraform (provisionamento de IaC)
- Git (se estiver provisionando localmente)
- AWS CLI versão 1 ou versão 2 (se estiver provisionando localmente)

Código

O código desse padrão está no GitHub repositório Terraform EC2 Image Builder Container Hardening Pipeline. Para usar o código de amostra, siga as instruções da próxima seção.

Épicos

Provisionar a infraestrutura

Tarefa	Descrição	Habilidades necessárias

Configure as credenciais locais.	Configure suas credenciais temporárias da AWS.
	1. Veja se a AWS CLI está instalada:
	`$ aws --version aws-cli/1.16.249 Python/3.6.8...`
	• A versão da AWS CLI deve ser 1.1 ou superior.
	• Se o comando não for encontrado, instale a AWS CLI.
	2. Execute `aws configure` e forneça os seguintes valores:
	`$ aws configure AWS Access Key ID [**********xxxx]: <Your AWS access key ID> AWS Secret Access Key [**********xxxx]: <Your AWS secret access key> Default region name: [us-east-1]: <Your desired Region for deployment>`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`Default output format [None]: <Your desired output format>`	

Clonar o repositório.	1. Clone o repositório que é fornecido com esse padrão. Use HTTPS ou Secure Shell (SSH).
	
	HTTPS
	
	`git clone https://github.com/aws-samples/terraform-ec2-image-builder-container-hardening-pipeline`
	
	SSH
	
	`git clone git@github.com:aws-samples/terraform-ec2-image-builder-container-hardening-pipeline.git`
	2. Navegue até o diretório local que contém esta solução:
	
	`cd terraform-ec2-image-builder-container-hardening-pipeline`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

Atualizar variáveis.	Atualizar as variáveis no `hardening-pipeline .tfvars` arquivo para que correspondam ao seu ambiente e à configuração desejada. Você deve fornecer o seu`account_id` . No entanto, você também deve modificar o restante das variáveis para se adequar à implantação desejada. Todas as variáveis são obrigatórias.
	
	`account_id = "<DEPLOYMENT-ACCOUNT-ID>"`
	`aws_region = "us-east-1"`
	`vpc_name = "example-hardening-pipeline-vpc"`
	`kms_key_alias = "image-builder-container-key"`
	`ec2_iam_role_name = "example-hardening-instance-role"`
	`hardening_pipeline_role_name = "example-hardening-pipeline-role"`
	`aws_s3_ami_resources_bucket = "example-hardening-ami-resources-bucket-0123"`
	`image_name = "example-hardening-al2-container-image"`
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias

	`ecr_name = "example-hardening-container-repo"`
	`recipe_version = "1.0.0"`
	`ebs_root_vol_size = 10`
	
	Aqui está uma descrição de cada variável:
	
	• `account_id` – O número da conta da AWS na qual você deseja implementar a solução.
	• `aws_region` – A região da AWS na qual você deseja implementar a solução.
	• `vpc_name`– O nome da sua infraestrutura de VPC.
	• `kms_key_alias` – O nome da chave do AWS KMS a ser usado pela configuração da infraestrutura do EC2 Image Builder.
	• `ec2_iam_role_name` – O nome da função que será usada como perfil da EC2 instância.
	• `hardening_pipeline_role_name` : o nome da função que será usada para implementar o pipeline de fortalecimento.
	• `aws_s3_ami_resources_bucket` – O nome	

Tarefa	Descrição	Habilidades necessárias
	de um bucket do S3 que hospedará todos os arquivos necessários para criar as imagens do pipeline e do contêiner. • `image_name` – O nome da imagem do contêiner. Esse valor deve ter entre 3 e 50 caracteres e conter somente caracteres alfanuméricos e hifens. • `ecr_name`– O nome do registro do Amazon ECR no qual armazenar as imagens do contêiner. • `recipe_version` - A versão semântica da fórmula de imagem. O valor padrão é 1.0.0. • `ebs_root_vol_size` – O tamanho (em gigabytes) do volume raiz do Amazon Elastic Block Store (Amazon EBS). O valor padrão é 10 gigabytes.	

Tarefa	Descrição	Habilidades necessárias
Inicializar o Terraform.	Depois de atualizar os valores das variáveis, você pode inicializar o diretório de configuração do Terraform. A inicialização de um diretório de configuração baixa e instala o provedor da AWS, que é definido na configura ção. `terraform init` Você verá uma mensagem dizendo que o Terraform foi inicializado com sucesso e identifica a versão do provedor que foi instalada.	AWS DevOps
Implementar a infraestr utura e criar uma imagem de contêiner.	Usar o comando a seguir para inicializar, validar e aplicar os módulos do Terraform ao ambiente usando as variáveis definidas em seu arquivo: `.tfvars` `terraform init && terraform validate && terraform apply -var-file *.tfvars -auto-approve`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Personalizar o contêiner.	Você pode criar uma nova versão de uma receita de contêiner depois que o EC2 Image Builder implantar o pipeline e a receita inicial. Você pode adicionar qualquer um dos mais de 31 component es disponíveis no EC2 Image Builder para personalizar a construção do contêiner. Para obter mais informações, consulte a seção Component es de Criar uma nova versão de uma receita de contêiner na documentação do EC2 Image Builder.	Administrador da AWS

Validar recursos

Tarefa	Descrição	Habilidades necessárias
Validar o provisionamento da infraestrutura da AWS.	Depois de concluir com êxito seu primeiro `apply` comando do Terraform, se você estiver provisionando localmente, deverá ver este trecho no terminal da sua máquina local: `Apply complete! Resources: 43 added, 0 changed, 0 destroyed.`	AWS DevOps
Valide recursos individuais de infraestrutura da AWS.	Para validar os recursos individuais que foram	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	implantados, se você estiver provisionando localmente, execute o seguinte comando: `terraform state list` Este comando retorna uma lista de 43 recursos.	

Remover o recurso .

Tarefa	Descrição	Habilidades necessárias
Remover a infraestrutura e a imagem do contêiner.	Ao terminar de trabalhar com sua configuração do Terraform, você pode executar o seguinte comando para remover recursos: `terraform init && terraform validate && terraform destroy -var-file *.tfvars -auto-approve`	AWS DevOps

Solução de problemas

Problema	Solução
Erro ao validar as credenciais do provedor	Ao executar o Terraform `apply` ou o `destroy` comando em sua máquina local, você poderá encontrar um erro semelhante ao seguinte:

Problema	Solução
	`Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Esse erro é causado pela expiração do token de segurança das credenciais usadas na configuração da sua máquina local. Para resolver o erro, consulte Definir e visualizar as configurações na documentação da AWS CLI.

Recursos relacionados

- Pipeline de endurecimento de contêineres do Terraform EC2 Image Builder (repositório) GitHub
- EC2 Documentação do Image Builder
- AWS Control Tower Account Factory for Terraform (publicação no blog da AWS)
- Bucket S3 de estado de backend (documentação do Terraform)
- Instalar ou atualizar a versão mais recente da AWS CLI (documentação da AWS CLI)
- Baixar o Terraform

Centralize o gerenciamento de chaves de acesso do IAM no AWS Organizations usando o Terraform

Criado por Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Pradip kumar Pandey (AWS), Mayuri Shinde (AWS) e Pratap Kumar Nanda (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais

Aplicar regras de segurança para chaves e senhas é uma tarefa essencial para todas as organizações. Uma regra importante é alternar as chaves do AWS Identity and Access Management (IAM) em intervalos regulares para reforçar a segurança. As chaves de acesso da AWS geralmente são criadas e configuradas localmente sempre que as equipes desejam acessar a AWS a partir da AWS Command Line Interface (AWS CLI) ou de aplicativos fora da AWS. Para manter uma segurança forte em toda a organização, as chaves de segurança antigas devem ser alteradas ou excluídas após o cumprimento do requisito ou em intervalos regulares. O processo de gerenciar as rotações de chaves em várias contas em uma organização é demorado e tedioso. Esse padrão ajuda você a automatizar o processo de rotação usando o Account Factory for Terraform (AFT) e os serviços da AWS.

O padrão fornece os seguintes benefícios:

- Gerencia sua chave de acesso IDs e chaves de acesso secretas em todas as contas da sua organização a partir de um local central.
- Rotaciona automaticamente `AWS_ACCESS_KEY_ID` as variáveis de `AWS_SECRET_ACCESS_KEY` ambiente.
- Impõe a renovação se as credenciais do usuário forem comprometidas.

O padrão usa o Terraform para implantar funções do AWS Lambda, regras da EventBridge Amazon e funções do IAM. Uma EventBridge regra é executada em intervalos regulares e chama uma função Lambda que lista todas as chaves de acesso do usuário com base em quando elas foram criadas. Funções adicionais do Lambda criam um novo ID de chave de acesso e uma chave de acesso secreta, se a chave anterior for mais antiga do que o período de rotação definido por você (por exemplo, 45 dias), e notificam um administrador de segurança usando o Amazon Simple Notification Service (Amazon SNS) e o Amazon Simple Email Service (Amazon SES). Os segredos são criados

no AWS Secrets Manager para esse usuário, a chave de acesso secreta antiga é armazenada no Secrets Manager e as permissões para acessar a chave antiga são configuradas. Para garantir que a chave de acesso antiga não seja mais usada, ela é desativada após um período inativo (por exemplo, 60 dias, o que seria 15 dias após a rotação das chaves em nosso exemplo). Após um período de buffer inativo (por exemplo, 90 dias ou 45 dias após a rotação das chaves em nosso exemplo), as chaves de acesso antigas são excluídas do AWS Secrets Manager. Para obter uma arquitetura e um fluxo de trabalho detalhados, consulte a seção Arquitetura.

Pré-requisitos e limitações

- Uma landing zone para sua organização criada usando o AWS Control Tower (versão 3.1 ou posterior)
- Account Factory for Terraform (AFT) configurado com três contas:
  - A conta de gerenciamento da organização gerencia toda a organização a partir de um local central.
  - A conta de gerenciamento do AFT hospeda o pipeline do Terraform e implanta a infraestrutura na conta de implantação.
  - A conta de implantação implanta essa solução completa e gerencia as chaves do IAM a partir de um local central.
- Terraform versão 0.15.0 ou posterior para provisionar a infraestrutura na conta de implantação.
- Um endereço de e-mail configurado no Amazon Simple Email Service (Amazon SES).
- (Recomendado) Para aumentar a segurança, implante essa solução em uma sub-rede privada (conta de implantação) em uma nuvem privada virtual (VPC). Você pode fornecer os detalhes da VPC e da sub-rede ao personalizar as variáveis (consulte Personalizar parâmetros para o pipeline de código na seção Epics).

Arquitetura

Repositórios AFT

Esse padrão usa o Account Factory for Terraform (AFT) para criar todos os recursos necessários da AWS e o pipeline de código para implantar os recursos em uma conta de implantação. O pipeline de código é executado em dois repositórios:

- A personalização global contém o código do Terraform que será executado em todas as contas registradas na AFT.

- As personalizações da conta contêm o código do Terraform que será executado na conta de implantação.

Detalhes do recurso

Os CodePipeline trabalhos da AWS criam os seguintes recursos na conta de implantação:

- EventBridge Regra da AWS e regra configurada
- Função do Lambda em `account-inventory`
- Função do Lambda em `IAM-access-key-rotation`
- Função do Lambda em `Notification`
- Bucket do Amazon Simple Storage Service (Amazon S3) que contém um modelo de e-mail
- Política de IAM necessária

Arquitetura

O diagrama ilustra o seguinte:

1. Uma EventBridge regra chama a função `account-inventory` Lambda a cada 24 horas.
2. A função `account-inventory` Lambda consulta o AWS Organizations para obter uma lista de todas as contas IDs, nomes de contas e e-mails de contas da AWS.
3. A função `account-inventory` Lambda inicia uma função `IAM-access-key-auto-rotation` Lambda para cada conta da AWS e passa os metadados para ela para processamento adicional.
4. A função `IAM-access-key-auto-rotation` Lambda usa uma função presumida do IAM para acessar a conta da AWS. O script do Lambda executa uma auditoria em todos os usuários e suas chaves de acesso do IAM na conta.
5. O limite de rotação da chave do IAM (período de rotação) é configurado como uma variável de ambiente quando a função `IAM-access-key-auto-rotation` Lambda é implantada. Se o período de rotação for modificado, a função `IAM-access-key-auto-rotation` Lambda será reimplantada com uma variável de ambiente atualizada. Você pode configurar parâmetros para definir o período de rotação, o período inativo para chaves antigas e o buffer inativo após o qual as chaves antigas serão excluídas (consulte Personalizar parâmetros para o pipeline de código na seção Epics).

6. A função `IAM-access-key-auto-rotation` Lambda valida a idade da chave de acesso com base em sua configuração. Se a idade da chave de acesso do IAM não exceder o período de rotação que você definiu, a função Lambda não realizará nenhuma ação adicional.
7. Se a idade da chave de acesso do IAM exceder o período de rotação que você definiu, a função `IAM-access-key-auto-rotation` Lambda cria uma nova chave e alterna a chave existente.
8. A função Lambda salva a chave antiga no Secrets Manager e limita as permissões para o usuário cujas chaves de acesso se desviaram dos padrões de segurança. A função Lambda também cria uma política baseada em recursos que permite que somente o principal especificado do IAM acesse e recupere o segredo.
9. A função `IAM-access-key-rotation` Lambda chama a função Lambda`Notification`.
10. A função `Notification` Lambda consulta o bucket do S3 em busca de um modelo de e-mail e gera dinamicamente mensagens de e-mail com os metadados de atividade relevantes.
11. A função `Notification` Lambda chama o Amazon SES para ações futuras.
12. O Amazon SES envia um e-mail para o endereço de e-mail do proprietário da conta com as informações relevantes.

Ferramentas

Serviços da AWS

- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los. Esse padrão exige funções e permissões do IAM.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O AWS Secrets Manager ajuda você a substituir credenciais codificadas em seu código, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo programaticamente.
- Amazon Simple Email Service (Amazon SES): ajuda você a enviar e receber e-mails usando seus próprios endereços de e-mail e domínios.

Outras ferramentas

- O Terraform é uma ferramenta de infraestrutura como código (IaC) HashiCorp que ajuda você a criar e gerenciar recursos na nuvem e no local.

Repositório de código

As instruções e o código desse padrão estão disponíveis no repositório de rotação de chaves de acesso GitHub do IAM. Você pode implantar o código na conta de implantação central do AWS Control Tower para gerenciar a rotação de chaves a partir de um local central.

Práticas recomendadas

- Para o IAM, consulte as melhores práticas de segurança na documentação do IAM.
- Para a rotação de chaves, consulte as diretrizes para atualizar as chaves de acesso na documentação do IAM.

Épicos

Configurar arquivos de origem

Tarefa	Descrição	Habilidades necessárias

Clonar o repositório.	1. Clone o GitHub repositório de rotação da chave de acesso do IAM:
	`$ git clone https://github.com/aws-samples/centralized-iam-key-management-aws-organizations-terraform.git`
	2. Confirme se sua cópia local do repositório contém três pastas:
	`$ cd Iam-Access-keys-Rotation`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

	`$ ls`
	`org-account-cus`
	`tomization`
	`global-account-c`
	`ustomization`
	`account-custom`
	`ization`	

Configurar contas

Tarefa	Descrição	Habilidades necessárias

Configure a conta de bootstrapping.	Como parte do processo de inicialização do AFT, você deve ter uma pasta chamada `aft-bootstrap` na sua máquina local.
	1. Copie todos os arquivos do Terraform manualmente da sua GitHub org-account-customizationpasta local para a sua `aft-bootstrap` pasta.
	2. Execute comandos do Terraform para configurar a função global entre contas na conta de gerenciamento do AWS Control Tower:
	`$ cd aft-bootstrap`
	`$ terraform init`
	`$ terraform apply –`
	`auto-approve`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Configure personalizações globais.	Como parte da configuração da pasta AFT, você deve ter uma pasta chamada `aft-global-customizations` em sua máquina local.
	
	1. Copie manualmente todos os arquivos do Terraform da sua GitHub global-account-customizationpasta local para a sua `aft-global-customizations/terraform` pasta.
	2. Envie o código para a AWS CodeCommit:
	
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias

Configure as personalizações da conta.	Como parte da configuração da pasta AFT, você tem que ser uma pasta chamada `aft-account-customizations` em sua máquina local.
	1. Crie uma pasta com o número da sua conta vendida.
	2. Copie manualmente todos os arquivos do Terraform da pasta local GitHub de personalização da conta para sua pasta. `aft-account-customizations/<vended account>/terraform`
	3. Envie o código para a AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps engenheiro

Personalize os parâmetros para o pipeline de código

Tarefa	Descrição	Habilidades necessárias
Personalize parâmetros de pipeline de código não Terraform para todas as contas.	Crie um arquivo chamado `input.auto.tfvars` na `aft-global-customizations/terraform/`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	pasta e forneça os dados de entrada necessários. Consulte o arquivo no GitHub repositório para ver os valores padrão.	

Tarefa	Descrição	Habilidades necessárias
Personalize os parâmetros do pipeline de código para a conta de implantação.	Crie um arquivo chamado `input.auto.tfvars` na `aft-account-customizations/<AccountName>/terraform/` pasta e envie o código para a AWS CodeCommit. Enviar código para a AWS inicia CodeCommit automaticamente o pipeline de código. Especifique valores para parâmetros com base nos requisitos da sua organização, incluindo o seguinte (consulte o arquivo no repositório do Github para ver os valores padrão): • `s3_bucket_name` — Um nome de bucket exclusivo para o modelo de e-mail. • `s3_bucket_prefix` — Um nome de pasta dentro do bucket do S3. • `admin_email_address` — O endereço de e-mail do administrador que deve receber a notificação. • `org_list_account` — O número da conta de gerenciamento. • `rotation_period` — O número de dias após os	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	quais uma chave deve ser girada de ativa para inativa. • `inactive_period` — O número de dias após os quais as teclas giradas devem ser desativadas. Esse valor deve ser maior que o valor de`rotation_period` . • `inactive_buffer` — O período de carência entre a rotação e a desativação de uma chave. • `recovery_grace_period` — O período de carência entre a desativação e a exclusão de uma chave. • `dry_run_flag` — Defina como verdadeiro se quiser enviar uma notificação ao administrador para fins de teste, sem alternar as chaves. • `store_secrets_in_central_account` — Defina como verdadeiro se você quiser armazenar o segredo na conta de implantação. Se a variável for definida como falsa (padrão), o segredo será armazenado na conta do membro.	

Tarefa	Descrição	Habilidades necessárias
	• `credential_replication_region` — A região da AWS em que você deseja implantar a função Lambda e os buckets S3 para o modelo de e-mail. • `run_lambda_in_vpc` — Defina como true para executar a função Lambda dentro da VPC. • `vpc_id`— O ID da VPC da conta de implantação, se você quiser executar a função Lambda dentro da VPC. • `vpc_cidr`— O intervalo CIDR para a conta de implantação. • `subnet_id` — A sub-rede da conta IDs de implantação. • `create_smtp_endpoint` — Defina como verdadeiro se você quiser ativar o endpoint de e-mail.	

Validar a rotação de chaves

Tarefa	Descrição	Habilidades necessárias
Valide a solução.	1. No AWS Management Console, faça login na conta de implantação. 2. Abra o console do IAM e verifique se as credenciais do usuário (chave de acesso IDs e chaves secretas) estão sendo alternadas conforme especificado. 3. Depois que uma chave do IAM for rotacionada, confirme o seguinte: • O valor antigo é armazenado no AWS Secrets Manager. • O nome secreto está no formato `Account_<account ID>_User_<username>_AccessKey`. • O usuário que você especificou no `admin_email_address` parâmetro recebe uma notificação por e-mail sobre a rotação da chave.	DevOps engenheiro

Estenda a solução

Tarefa	Descrição	Habilidades necessárias
Personalize a data da notificação por e-mail.	Se quiser enviar notificações por e-mail em um dia específico antes de desativar a chave de acesso, você pode atualizar a função `IAM-access-key-auto-rotation` Lambda com essas alterações: 1. Defina uma variável chamada`notify-period` . 2. Adicione uma `if` condição `main.py` antes de desativar a chave: `If (keyage>rotation-period-notify-period){ send_to_notifier(context, aws_account_id, account_name, resource_owner, resource_actions[resource_owner], dryrun, config.emailTemplateAudit) }`	DevOps engenheiro

Solução de problemas

Problema	Solução
O trabalho do `account-inventory` Lambda falha `AccessDenied` ao listar contas.	Se você encontrar esse problema, deverá validar as permissões: 1. Faça login na conta recém-vendida, abra o CloudWatch console da Amazon e, em seguida, visualize o grupo `/aws/lambda/account-inventory-lambda` de CloudWatch registros. 2. Nos CloudWatch registros mais recentes, identifique o número da conta que está causando o problema de acesso negado. 3. Faça login na conta de gerenciamento do AWS Control Tower e confirme se a função `allow-list-account` foi criada. 4. Se a função não existir, execute novamente o código do Terraform usando o comando. `terraform apply` 5. Escolha a guia Conta confiável e confirme se a mesma conta é confiável.

Recursos relacionados

- Práticas recomendadas do Terraform (documentação do Terraform)
- Práticas recomendadas de segurança no IAM (documentação do IAM)
- Melhores práticas para rotação de chaves (documentação do IAM)

Verifique a versão de registro de acesso, HTTPS e TLS em uma CloudFront distribuição da Amazon

Criado por SaiJeevan Devireddy (AWS) e Bijesh Bal (AWS)

Resumo

Esse padrão verifica uma CloudFront distribuição da Amazon para garantir que ela use HTTPS, use o Transport Layer Security (TLS) versão 1.2 ou posterior e tenha o registro de acesso ativado. CloudFront é um serviço fornecido pela Amazon Web Services (AWS) que acelera a distribuição de seu conteúdo web estático e dinâmico, como .html, .css, .js e arquivos de imagem, para seus usuários. CloudFront entrega seu conteúdo por meio de uma rede mundial de data centers chamados de pontos de presença. Quando um usuário solicita o conteúdo com o qual você está servindo CloudFront, a solicitação é encaminhada para o ponto de presença que fornece a menor latência (atraso de tempo), para que o conteúdo seja entregue com o melhor desempenho possível.

Esse padrão fornece uma função do AWS Lambda que é iniciada quando o Amazon CloudWatch Events detecta a chamada de CloudFront API CreateDistribution, CreateDistributionWithTagsou. UpdateDistribution A lógica personalizada na função Lambda avalia todas as CloudFront distribuições que foram criadas ou atualizadas na conta da AWS. Ele envia uma notificação de violação usando o Amazon Simple Notification Service (Amazon SNS) se detectar as seguintes violações:

- Verificações globais:
  - O certificado personalizado não usa TLS versão 1.2
  - O registro em log está desativado para distribuição
- Verificações de origem:
  - A origem não está configurada com TLS versão 1.2
  - A comunicação com a origem é permitida em um protocolo diferente de HTTPS
- Verificações de comportamento:
  - A comunicação de comportamento padrão é permitida em um protocolo diferente de HTTPS
  - A comunicação de comportamento personalizada é permitida em um protocolo diferente de HTTPS

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um endereço de e-mail no qual você deseja receber as notificações de violação

Limitações

- Esse controle de segurança não verifica as distribuições existentes do Cloudfront, a menos que uma atualização tenha sido feita na distribuição.
- CloudFront é considerado um serviço global e não está vinculado a uma região específica da AWS. No entanto, CloudWatch os registros de APIs do Amazon Logs e do AWS Cloudtrail para serviços globais ocorrem na região Leste dos EUA (Norte da Virgínia) (`us-east-1`). Portanto, esse formulário de controle de segurança CloudFront deve ser implantado e mantido em`us-east-1`. Essa implantação única monitora todas as distribuições de CloudFront. Não implante o controle de segurança em nenhuma outra região da AWS. (A implantação em outras regiões resultará em uma falha no início dos CloudWatch Eventos e da função Lambda e na ausência de notificações do SNS.)
- Essa solução passou por testes extensivos com distribuições de conteúdo CloudFront da web. Ela não abrange distribuições de fluxo do protocolo de mensagens em tempo real (RTMP).

Arquitetura

Pilha de tecnologias de destino

- Função do Lambda
- Tópico do SNS
- EventBridge Regra da Amazon

Arquitetura de destino

Automação e escala

- Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar o modelo anexado em várias contas que você deseja monitorar.

Ferramentas

Serviços da AWS

- AWS CloudFormation — CloudFormation é um serviço que ajuda você a modelar e configurar recursos da AWS usando a infraestrutura como código.
- Amazon EventBridge — EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos de software como serviço (SaaS) e serviços da AWS, roteando esses dados para destinos como funções Lambda.
- AWS Lambda: o Lambda é compatível com a execução de código sem provisionar ou gerenciar servidores.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- Amazon SNS: o Amazon SNS coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

O código em anexo inclui:

- Um arquivo .zip que contém o código do Lambda (index.py)
- Um CloudFormation modelo (arquivo.yml) que você executa para implantar o código Lambda

Épicos

Fazer o upload do controle de segurança

Tarefa	Descrição	Habilidades necessárias
Criar o bucket do S3 para o código do Lambda.	No console do Amazon S3, crie um bucket do S3 com um nome exclusivo que não contenha barras iniciais.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Um nome de bucket do S3 é globalmente exclusivo, e o namespace é compartil hado por todas as contas da AWS. Seu bucket do S3 deve estar na região em que você planeja implantar o código do Lambda.	
Carregar o código do Lambda para o bucket do S3.	Faça upload do código do Lambda (arquivo cloudfron t_ssl_log_lambda.zip) fornecido na seção Anexos para o bucket do S3 que você criou na etapa anterior.	Arquiteto de nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	No CloudFormation console da AWS, na mesma região da AWS do bucket do S3, implante o CloudFormation modelo (cloudfront-ssl-lo gging.yml) fornecido na seção Anexos.	Arquiteto de nuvem
Especifique o nome do bucket do S3.	Para o parâmetro do bucket do S3, especifique o nome do bucket do S3 que você criou no primeiro épico.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Especifique o nome da chave do Amazon S3 para o arquivo do Lambda.	Para o parâmetro Chave do S3, especifique a localização do arquivo .zip do código do Lambda no Amazon S3 em seu bucket do S3. Não inclua barras iniciais (por exemplo, você pode inserir lambda.zip ou controls/lambda.zip).	Arquiteto de nuvem
Fornecer um endereço de e-mail de notificação.	Para o parâmetro do e-mail de notificação, forneça um endereço de e-mail no qual você gostaria de receber as notificações de violação.	Arquiteto de nuvem
Definir o nível de registro em log.	Para o parâmetro Nível do registro em log do Lambda, defina o nível de registro em log para sua função do Lambda. Escolha um dos seguintes valores: • INFO para obter mensagens informativas detalhadas sobre o progresso do aplicativo. • ERROR para obter informações sobre eventos de erro que ainda podem permitir que o aplicativo continue em execução. • AVISO para obter informações sobre situações potencialmente prejudiciais.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o CloudFormation modelo é implantado com sucesso, um novo tópico do SNS é criado e uma mensagem de assinatura é enviada para o endereço de e-mail que você forneceu. Você deve confirmar essa assinatura de e-mail para receber notificações de violação.	Arquiteto de nuvem

Recursos relacionados

- CloudFormation Informações da AWS
- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação)
- CloudFront registro (CloudFront documentação)
- Informações sobre o Amazon S3
- Informações sobre o AWS Lambda

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Verifique as entradas de rede de host único nas regras de entrada do grupo de segurança para e IPv4 IPv6

Criado por SaiJeevan Devireddy (AWS), Ganesh Kumar (AWS) e John Reynolds (AWS)

Resumo

Esse padrão fornece um controle de segurança que notifica você quando os recursos da Amazon Web Services (AWS) não atendem às suas especificações. Ele fornece uma função do AWS Lambda que procura entradas de rede de host único nos campos de endereço de origem do Internet Protocol versão 4 (IPv4) e do grupo IPv6 de segurança. A função Lambda é iniciada quando o Amazon CloudWatch Events detecta a chamada de API do Amazon Elastic Compute Cloud (Amazon EC2). AuthorizeSecurityGroupIngress A lógica personalizada na função do Lambda avalia a máscara de sub-rede do bloco CIDR da regra de entrada do grupo de segurança. Se a máscara de sub-rede for determinada como algo diferente de /32 (IPv4) ou /128 (IPv6), a função Lambda enviará uma notificação de violação usando o Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um endereço de e-mail no qual você deseja receber as notificações de violação

Limitações

- Essa solução de monitoramento de segurança é regional e deve ser implantada em cada região da AWS que você deseja monitorar.

Arquitetura

Pilha de tecnologias de destino

- Função do Lambda
- Tópico do SNS
- EventBridge Regra da Amazon

Arquitetura de destino

Automação e escala

- Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

Serviços da AWS

- CloudFormationA AWS é um serviço que ajuda você a modelar e configurar recursos da AWS usando a infraestrutura como código.
- EventBridgeA Amazon fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos de software como serviço (SaaS) e serviços da AWS, e encaminha esses dados para destinos como funções Lambda.
- O AWS Lambda é compatível com a execução de código sem provisionar ou gerenciar servidores.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- O Amazon SNS é um serviço da Web que coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

O código em anexo inclui:

- Um arquivo .zip que contém o código de controle de segurança do Lambda (`index.py`)
- Um CloudFormation modelo (`security-control.yml`arquivo) que você executa para implantar o código Lambda

Épicos

Fazer o upload do controle de segurança

Tarefa	Descrição	Habilidades necessárias
Criar o bucket do S3 para o código do Lambda.	No console do Amazon S3, crie um bucket do S3 com um nome exclusivo que não contenha barras iniciais. Um nome de bucket do S3 é globalmente exclusivo, e o namespace é compartilhado por todas as contas da AWS. Seu bucket do S3 deve estar na região da AWS onde você deseja implantar a verificação de entrada do grupo de segurança.	Arquiteto de nuvem
Carregue o código do Lambda para o bucket do S3.	Faça upload do código do Lambda (arquivo `security-control-lambda.zip`) fornecido na seção Anexos para o bucket do S3 que você criou na etapa anterior.	Arquiteto de nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Altere a versão do Python.	Faça o download do CloudFormation modelo (`security-control.yml`) fornecido na seção Anexos. Abra o arquivo e	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	modifique a versão do Python para refletir a versão mais recente suportada pelo Lambda (atualmente Python 3.9). Por exemplo, você pode pesquisar `python` no código e alterar o valor de `Runtime` de `python3.6` para `python3.9` . Para obter as informações mais recentes sobre o suporte à versão de runtime do Python, consulte a documentação do AWS Lambda.	
Implante o CloudFormation modelo da AWS.	No CloudFormation console da AWS, na mesma região da AWS do bucket S3, implante o CloudFormation modelo (`security-control.yml`).	Arquiteto de nuvem
Especifique o nome do bucket do S3.	Para o parâmetro do bucket do S3, especifique o nome do bucket do S3 que você criou no primeiro épico.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Especifique o nome da chave do Amazon S3 para o arquivo do Lambda.	Para o parâmetro de chave do S3, especifique a localizaç ão do arquivo .zip do código Lambda no Amazon S3 no seu bucket do S3. Não inclua barras iniciais (por exemplo, você pode inserir `lambda.zip` ou `controls/lambda.zip`).	Arquiteto de nuvem
Fornecer um endereço de e-mail de notificação.	Para o parâmetro do e-mail de notificação, forneça um endereço de e-mail no qual você gostaria de receber as notificações de violação.	Arquiteto de nuvem
Definir o nível de registro em log.	Para o parâmetro Nível do registro em log do Lambda, defina o nível de registro em log para sua função do Lambda. Escolha um dos seguintes valores: • INFO para obter mensagens informativas detalhada s sobre o progresso do aplicativo. • ERROR para obter informações sobre eventos de erro que ainda podem permitir que o aplicativo continue em execução. • AVISO para obter informaçõ es sobre situações potencial mente prejudiciais.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o CloudFormation modelo é implantado com sucesso, um novo tópico do SNS é criado e uma mensagem de assinatura é enviada para o endereço de e-mail que você forneceu. Você deve confirmar essa assinatura de e-mail para receber notificações de violação.	Arquiteto de nuvem

Recursos relacionados

- CloudFormation Informações da AWS
- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- Grupos de segurança para sua VPC (documentação da Amazon VPC)
- Informações sobre o Amazon S3
- Informações sobre o AWS Lambda

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Escolha um fluxo de autenticação do Amazon Cognito para aplicativos corporativos

Criado por Michael Daehnert (AWS) e Fabian Jahnke (AWS)

Resumo

O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para aplicativos web e móveis. Ele oferece recursos benéficos para autenticação de identidades federadas. Para colocá-lo em funcionamento, os arquitetos técnicos precisam decidir como querem usar esses recursos.

O Amazon Cognito oferece suporte a vários fluxos para solicitações de autenticação. Esses fluxos definem como seus usuários podem verificar sua identidade. A decisão sobre qual fluxo de autenticação usar depende dos requisitos específicos do seu aplicativo e pode se tornar complexa. Esse padrão ajuda você a decidir qual fluxo de autenticação é o mais adequado para seu aplicativo corporativo. Ele pressupõe que você já tenha um conhecimento básico do Amazon Cognito, do OpenID Connect (OIDC) e da federação, e orienta você nos detalhes sobre os diferentes fluxos de autenticação federada.

Essa solução é destinada a tomadores de decisão técnica. Ele ajuda você a entender os diferentes fluxos de autenticação e mapeá-los de acordo com os requisitos do seu aplicativo. Os líderes técnicos devem reunir os insights necessários para iniciar as integrações do Amazon Cognito. Como as organizações corporativas se concentram principalmente na federação SAML, esse padrão inclui descrições para grupos de usuários do Amazon Cognito com federação SAML.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Funções e permissões do AWS Identity and Access Management (IAM) com acesso total ao Amazon Cognito
- (Opcional) Acesso ao seu provedor de identidade (IdP), como Microsoft Entra ID, Active Directory Federation Service (AD FS) ou Okta
- Um alto nível de especialização para sua aplicação
- Conhecimento básico do Amazon Cognito, do OpenID Connect (OIDC) e da federação

Limitações

- Esse padrão se concentra nos grupos de usuários e provedores de identidade do Amazon Cognito. Para obter informações sobre grupos de identidade do Amazon Cognito, consulte a seção Informações adicionais.

Arquitetura

Use a tabela a seguir para ajudá-lo a escolher um fluxo de autenticação. Mais informações sobre cada fluxo são fornecidas nesta seção.

Você precisa de machine-to-machine autenticação?	Seu aplicativo é baseado na web em que o front-end é renderizado no servidor?	Seu aplicativo é um aplicativo de página única (SPA) ou um aplicativo de front-end baseado em dispositivos móveis?	Seu aplicativo exige tokens de atualização para o recurso “mantenha-me conectado”?	O frontend oferece um mecanismo de redirecionamento baseado em navegador?	Fluxo recomendado do Amazon Cognito
Sim	Não	Não	Não	Não	Fluxo de credenciais do cliente
Não	Sim	Não	Sim	Sim	Fluxo do código de autorização
Não	Não	Sim	Sim	Sim	Fluxo de código de autorização com chave de prova para troca

					de código (PKCE)
Não	Não	Não	Não	Não	Fluxo de senha do proprietário do recurso*

* O fluxo de senha do proprietário do recurso deve ser usado somente se for absolutamente necessário. Para obter mais informações, consulte a seção Fluxo de senha do proprietário do recurso nesse padrão.

Fluxo de credenciais do cliente

O fluxo de credenciais do cliente é o mais curto dos fluxos do Amazon Cognito. Ele deve ser usado se sistemas ou serviços se comunicarem entre si sem qualquer interação do usuário. O sistema solicitante usa o ID do cliente e o segredo do cliente para recuperar um token de acesso. Como os dois sistemas funcionam sem a interação do usuário, nenhuma etapa adicional de consentimento é necessária.

O diagrama ilustra o seguinte:

1. O aplicativo 1 envia uma solicitação de autenticação com o ID do cliente e o segredo do cliente para o endpoint do Amazon Cognito e recupera um token de acesso.
2. O aplicativo 1 usa esse token de acesso para cada chamada subsequente para o aplicativo 2.
3. O aplicativo 2 valida o token de acesso com o Amazon Cognito.

Esse fluxo deve ser usado:

- Para comunicações entre aplicativos sem interação com o usuário

Esse fluxo não deve ser usado:

- Para qualquer comunicação na qual as interações do usuário sejam possíveis

Fluxo do código de autorização

O fluxo do Código de Autorização é para autenticação clássica baseada na web. Nesse fluxo, o back-end lida com toda a troca e armazenamento de tokens. O cliente baseado em navegador não vê os tokens reais. Essa solução é usada para aplicativos escritos em estruturas como o.NET Core, Jakarta Faces ou Jakarta Server Pages (JSP).

O fluxo do Código de Autorização é um fluxo baseado em redirecionamento. O cliente deve ser capaz de interagir com o navegador da Web ou com um cliente similar. O cliente é redirecionado para um servidor de autenticação e se autentica nesse servidor. Se o cliente for autenticado com êxito, ele será redirecionado de volta para o servidor.

O diagrama ilustra o seguinte:

1. O cliente envia uma solicitação para o servidor web.
2. O servidor web redireciona o cliente para o Amazon Cognito usando um código de status HTTP 302. O cliente segue automaticamente esse redirecionamento para o login do IdP configurado.
3. O IdP verifica se há uma sessão de navegador existente no lado do IdP. Se nenhum existir, o usuário receberá uma solicitação para se autenticar fornecendo seu nome de usuário e senha. O IdP responde com um token SAML para o Amazon Cognito.
4. O Amazon Cognito retorna o sucesso com um token web JSON (JWT), especificamente um token de código. O servidor web calls /oauth2/token para trocar o token de código por um token de acesso. O servidor web envia o ID do cliente e o segredo do cliente para o Amazon Cognito para validação.
5. O token de acesso é usado para cada chamada subsequente para outros aplicativos.
6. Outros aplicativos validam o token de acesso com o Amazon Cognito.

Esse fluxo deve ser usado:

- Se o usuário conseguir interagir com o navegador da web ou com o cliente. O código do aplicativo é executado e renderizado no servidor para garantir que nenhum segredo seja exposto ao navegador.

Esse fluxo não deve ser usado:

- Para aplicativos de página única (SPAs) ou aplicativos móveis porque eles são renderizados no cliente e não devem usar segredos do cliente.

Fluxo de código de autorização com PKCE

O fluxo de código de autorização com a chave de prova para troca de código (PKCE) deve ser usado para aplicativos de página única e aplicativos móveis. É o sucessor do fluxo implícito e é mais seguro porque usa PKCE. O PKCE é uma extensão da concessão do código de autorização OAuth 2.0 para clientes públicos. O PKCE oferece proteção contra o resgate de códigos de autorização interceptados.

O diagrama ilustra o seguinte:

1. O aplicativo cria um verificador de código e um desafio de código. Esses são valores exclusivos e bem definidos que são enviados ao Amazon Cognito para futura referência.
2. O aplicativo chama o the /oauth2/authorization endpoint do Amazon Cognito. Ele redireciona automaticamente o usuário para o login do IdP configurado.
3. O IdP verifica se há uma sessão existente. Se nenhum existir, o usuário receberá uma solicitação para se autenticar fornecendo seu nome de usuário e senha. O IdP responde com um token SAML para o Amazon Cognito.
4. Depois que o Amazon Cognito retornar o sucesso com um token de código, o servidor web calls / oauth2/token trocará o token de código por um token de acesso.
5. O token de acesso é usado para cada chamada subsequente para outros aplicativos.
6. Os outros aplicativos validam o token de acesso com o Amazon Cognito.

Esse fluxo deve ser usado:

- Para SPAs nossos aplicativos móveis

Esse fluxo não deve ser usado:

- Se o back-end do aplicativo manipular a autenticação

Fluxo de senha do proprietário do recurso

O fluxo de senha do proprietário do recurso é destinado a aplicativos sem recursos de redirecionamento. Ele é construído criando um formulário de login em seu próprio aplicativo. O login é verificado no Amazon Cognito por meio de uma chamada de CLI ou SDK, em vez de depender

de fluxos de redirecionamento. A federação não é possível nesse fluxo de autenticação porque a federação exige redirecionamentos baseados em navegador.

O diagrama ilustra o seguinte:

1. O usuário insere suas credenciais em um formulário de login fornecido pelo aplicativo.
2. A AWS Command Line Interface (AWS CLI) faz admin-initiated-authuma chamada para o Amazon Cognito.

> **Note**
>
> Como alternativa, você pode usar a AWS SDKs em vez da AWS CLI.

3. O Amazon Cognito retorna um token de acesso.
4. O token de acesso é usado para cada chamada subsequente para outros aplicativos.
5. Os outros aplicativos validam o token de acesso com o Amazon Cognito.

Esse fluxo deve ser usado:

- Ao migrar clientes existentes que usam lógica de autenticação direta (como autenticação de acesso básico ou autenticação de acesso resumido) para a OAuth conversão das credenciais armazenadas em um token de acesso

Esse fluxo não deve ser usado:

- Se você quiser usar identidades federadas
- Se seu aplicativo suportar redirecionamentos

Ferramentas

Serviços da AWS

- O Amazon Cognito fornece autenticação, autorização e gerenciamento de usuários para suas aplicações Web e móveis.

Outras ferramentas

- O depurador JSON web token (JWT) é uma ferramenta de validação JWT baseada na web.

Épicos

Avalie sua inscrição

Tarefa	Descrição	Habilidades necessárias
Defina os requisitos de autenticação.	Avalie seu aplicativo de acordo com seus requisitos específicos de autenticação.	Desenvolvedor de aplicativos, arquiteto de aplicativos
Alinhe os requisitos aos fluxos de autenticação.	Na seção Arquitetura, use a tabela de decisão e as explicações de cada fluxo para escolher seu fluxo de autenticação do Amazon Cognito.	Desenvolvedor de aplicativos, AWS geral, arquiteto de aplicativos

Configurar o grupo de usuários do Amazon Cognito

Tarefa	Descrição	Habilidades necessárias
Criar um grupo de usuários.	1. Faça login no Console de Gerenciamento da AWS e, em seguida, abra o console do Amazon Cognito. 2. Crie um novo grupo de usuários do Cognito. Para obter instruções, consulte Grupos de usuários do Amazon Cognito. 3. Atualize as configurações e os atributos do grupo de usuários conforme necessário. Por exemplo,	AWS geral

Tarefa	Descrição	Habilidades necessárias
	defina uma política de senha para o grupo de usuários. Ainda não crie clientes de aplicativos.	
(Opcional) Configure um provedor de identidade.	1. Crie um provedor de identidade SAML no grupo de usuários do Amazon Cognito. Para obter instruções, consulte Adicionar e gerenciar provedores de identidade SAML em um grupo de usuários. 2. Configure seu provedor de identidade SAML terceirizado para trabalhar com federação para grupos de usuários do Amazon Cognito. Para obter mais informações, consulte Configurando seu provedor de identidade SAML terceirizado. Se você estiver usando o AD FS, consulte Como criar uma federação do AD FS para seu aplicativo web usando grupos de usuários do Amazon Cognito (postagem no blog da AWS).	AWS geral, administrador da federação

Tarefa	Descrição	Habilidades necessárias
Crie um cliente de aplicativo.	1. Crie um cliente de aplicativo para o grupo de usuários. Para obter instruções, consulte Criação de um cliente de aplicativo. Observe o seguinte: • Altere as configurações conforme necessário, como expirações de tokens. • Se o fluxo de autenticação não exigir um segredo do cliente, desmarque a caixa de seleção Gerar segredo do cliente. 2. Escolha as configurações do cliente do aplicativo para alterar sua integração com um login de grupo de usuários (nome de usuário e senha) ou login federado por meio de um IdP baseado em SAML. 3. Ative seu IdP definindo URLs e definindo OAuth fluxos ou escopos conforme necessário.	AWS geral

Integre o aplicativo com o Amazon Cognito

Tarefa	Descrição	Habilidades necessárias
Detalhes da integração com o Amazon Cognito do Exchange.	Dependendo do seu fluxo de autenticação, compartil he informações do Amazon Cognito com o aplicativ o, como o ID do grupo de usuários e o ID do cliente do aplicativo.	Desenvolvedor de aplicativos, AWS geral
Implemente a autenticação do Amazon Cognito.	Isso depende do fluxo de autenticação escolhido, da linguagem de programação e das estruturas que você está usando. Para ver alguns links para começar, consulte a seção Recursos relacionados.	Desenvolvedor de aplicativos

Recursos relacionados

Documentação da AWS

- Fluxo de autenticação do grupo de usuários
- Verificando um token web JSON
- Acesse os serviços da AWS a partir de um aplicativo ASP.NET Core usando grupos de identidade do Amazon Cognito
- Frameworks e SDKs:
  - Autenticação do Amazon Amplify
  - Exemplos do Amazon Cognito Identity Provider (documentação do AWS SDK para Java 2.x)
  - Autenticação de usuários com o Amazon Cognito (documentação do AWS SDK para.NET do AWS SDK for .NET)

Publicações do blog da AWS

- Authorization @Edge usando cookies: proteja seu CloudFront conteúdo da Amazon de ser baixado por usuários não autenticados
- Criando uma federação do AD FS para seu aplicativo Web usando grupos de usuários do Amazon Cognito

Parceiros de implementação

- Parceiros da AWS para soluções de autenticação

Mais informações

PERGUNTAS FREQUENTES

Por que o fluxo implícito foi descontinuado?

Desde o lançamento da estrutura OAuth 2.1, o fluxo implícito é marcado como obsoleto por motivos de segurança. Como alternativa, use o fluxo do Código de Autorização com o PKCE descrito na seção Arquitetura.

E se o Amazon Cognito não oferecer alguma funcionalidade que eu exija?

Os parceiros da AWS oferecem diferentes integrações para soluções de autenticação e autorização. Para obter mais informações, consulte Parceiros da AWS para soluções de autenticação.

E quanto aos fluxos do pool de identidade do Amazon Cognito?

Os grupos de usuários e identidades federadas do Amazon Cognito são para autenticação. Os grupos de identidade do Amazon Cognito são usados para autorizar o acesso aos recursos da AWS solicitando credenciais temporárias da AWS. A troca do token de ID e do token de acesso para grupos de identidades não é discutida nesse padrão. Para obter mais informações, consulte Qual é a diferença entre grupos de usuários e grupos de identidades do Amazon Cognito e cenários comuns do Amazon Cognito.

Próximas etapas

Esse padrão fornece uma visão geral dos fluxos de autenticação do Amazon Cognito. Como próxima etapa, a implementação detalhada da linguagem de programação do aplicativo precisa ser escolhida. Oferta SDKs e estruturas de vários idiomas, que você pode usar com o Amazon Cognito. Para referências úteis, consulte a seção Recursos relacionados.

Crie regras AWS Config personalizadas usando AWS CloudFormation Guard políticas

Criado por Andrew Lok (AWS), Kailash Havildar (AWS), Nicole Brown (AWS) e Tanya Howell (AWS)

Resumo

AWS Configas regras ajudam você a avaliar seus AWS recursos e o estado de configuração de destino. Há dois tipos de AWS Config regras: gerenciadas e personalizadas. Você pode criar regras personalizadas com AWS Lambda funções ou com AWS CloudFormation Guard(GitHub), uma policy-as-code linguagem.

As regras criadas com o Guard fornecem um controle mais granular do que as regras gerenciadas e geralmente são mais fáceis de configurar do que as regras Lambda totalmente personalizadas. Essa abordagem fornece aos engenheiros e arquitetos a capacidade de criar regras sem precisar conhecer Python, NodeJS ou Java, que são necessários para implantar regras personalizadas por meio do Lambda.

Esse padrão fornece modelos viáveis, exemplos de código e abordagens de implantação para ajudá-lo a adotar regras personalizadas com o Guard. Ao usar esse padrão, um administrador pode usar AWS Config para criar regras de conformidade personalizadas que tenham atributos de item de configuração. Por exemplo, os desenvolvedores podem usar as políticas do Guard em relação aos itens de AWS Config configuração para monitorar continuamente o estado dos recursos implantados AWS e dos não AWS recursos, detectar violações de regras e iniciar automaticamente a remediação.

Objetivos

Depois de ler esse padrão, você deve ser capaz de:

- Entenda como o código de política do Guard interage com o AWS Config serviço.
- Implante o Cenário 1, que é uma regra AWS Config personalizada que usa a sintaxe do Guard para validar a conformidade de volumes criptografados. Essa regra verifica se a unidade está em uso e se o tipo de unidade é gp3.
- Implante o Cenário 2, que é uma regra AWS Config personalizada que usa a sintaxe do Guard para validar a conformidade da Amazon GuardDuty . Essa regra verifica se GuardDuty os gravadores têm a Proteção Amazon Simple Storage Service (Amazon S3) e a Proteção Amazon Elastic Kubernetes Service (Amazon EKS) ativadas.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- AWS Config, configurado em seu Conta da AWS

Limitações

- As regras personalizadas do Guard só podem consultar pares de valores-chave em um registro JSON do item de configuração de destino

Arquitetura

Você aplica a sintaxe do Guard a uma AWS Config regra como uma política personalizada. AWS Config captura o JSON hierárquico de cada um dos recursos especificados. O JSON do item de AWS Config configuração contém pares de valores-chave. Esses atributos são usados na sintaxe do Guard como variáveis atribuídas ao valor correspondente.

A seguir está uma explicação da sintaxe do Guard. As variáveis do item de configuração JSON são usadas e prefixadas com um caractere. `%`

```
# declare variable
let <variable name> = <'value'>

# create rule and assign condition and policy
    rule <rule name> when
        <CI json key> == <"CI json value"> {
            <top level CI json key>.<next level CI json key> == %<variable name>
        }
```

Cenário 1: volumes do Amazon EBS

O cenário 1 implanta uma regra AWS Config personalizada que usa a sintaxe do Guard para validar a conformidade de volumes criptografados. Essa regra verifica se a unidade está em uso e se o tipo de unidade é gp3.

Veja a seguir um exemplo de um item de AWS Config configuração para o cenário 1. Há três pares de valores-chave nesse item de configuração que são usados como variáveis na política do Guard:

`volumestatusvolumeencryptionstatus`, e. `volumetype` Além disso, a `resourceType` chave é usada como filtro na política do Guard.


```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-01-15T19:04:45.402Z",
  "configurationItemStatus": "ResourceDiscovered",
  "configurationStateId": "4444444444444",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:ec2:us-west-2:111111111111:volume/vol-222222222222",
  "resourceType": "AWS::EC2::Volume",
  "resourceId": "vol-222222222222",
  "awsRegion": "us-west-2",
  "availabilityZone": "us-west-2b",
  "resourceCreationTime": "2023-01-15T19:03:22.247Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [
    {
      "resourceType": "AWS::EC2::Instance",
      "resourceId": "i-33333333333333333",
      "relationshipName": "Is attached to Instance"
    }
  ],
  "configuration": {
    "attachments": [
      {
        "attachTime": "2023-01-15T19:03:22.000Z",
        "device": "/dev/xvda",
        "instanceId": "i-33333333333333333",
        "state": "attached",
        "volumeId": "vol-222222222222",
        "deleteOnTermination": true,
        "associatedResource": null,
        "instanceOwningService": null
      }
    ],
    "availabilityZone": "us-west-2b",
    "createTime": "2023-01-15T19:03:22.247Z",
    "encrypted": false,
    "kmsKeyId": null,
    "outpostArn": null,
```

```
    "size": 8,
    "snapshotId": "snap-55555555555555555",
    "state": "in-use",
    "volumeId": "vol-222222222222",
    "iops": 100,
    "tags": [],
    "volumeType": "gp2",
    "fastRestored": null,
    "multiAttachEnabled": false,
    "throughput": null,
    "sseType": null
  },
  "supplementaryConfiguration": {}
}
```

Veja a seguir um exemplo do uso da sintaxe do Guard para definir as variáveis e regras no cenário 1. No seguinte exemplo:

- As três primeiras linhas definem as variáveis usando o `let` comando. Eles recebem um nome e um valor derivados dos atributos do item de configuração.
- O bloco de `compliancecheck` regras adiciona uma dependência condicional quando que procura um par de `resourceType` valores-chave que corresponda. `AWS::EC2::Volume` Se uma correspondência for encontrada, a regra prosseguirá com o restante dos atributos JSON e procurará correspondências nas três condições a seguir: `stateencrypted`, e. `volumeType`

```
let volumestatus = 'available'
let volumetype = 'gp3'
let volumeencryptionstatus = true

    rule compliancecheck when
        resourceType == "AWS::EC2::Volume" {
            configuration.state == %volumestatus
            configuration.encrypted == %volumeencryptionstatus
            configuration.volumeType == %volumetype
        }
```

Para ver a política personalizada completa do Guard que implementa essa regra personalizada, consulte awsconfig-guard-cft.yaml ou awsconfig-guard-tf-ec2vol.json no repositório de código. GitHub Para o código do HashiCorp Terraform que implanta essa política personalizada no Guard, consulte awsconfig-guard-tf-example.json no repositório de código.

Cenário 2: GuardDuty conformidade

O cenário 2 implanta uma regra AWS Config personalizada que usa a sintaxe do Guard para validar a conformidade da Amazon GuardDuty . Essa regra verifica se GuardDuty os gravadores têm a Proteção Amazon S3 e a Proteção Amazon EKS ativadas. Também verifica se as GuardDuty descobertas são publicadas a cada 15 minutos. Esse cenário pode ser implantado em toda Contas da AWS e Regiões da AWS em uma organização (em AWS Organizations).

Veja a seguir um exemplo de um item de AWS Config configuração para o cenário 2. Há três pares de valores-chave nesse item de configuração que são usados como variáveis na política do Guard: `FindingPublishingFrequency`S3Logs, e. `Kubernetes` Além disso, a `resourceType` chave é usada como filtro na política.

```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-11-27T13:34:28.888Z",
  "configurationItemStatus": "OK",
  "configurationStateId": "7777777777777",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:guardduty:us-
west-2:111111111111:detector/66666666666666666666666666666666",
  "resourceType": "AWS::GuardDuty::Detector",
  "resourceId": "66666666666666666666666666666666",
  "resourceName": "66666666666666666666666666666666",
  "awsRegion": "us-west-2",
  "availabilityZone": "Regional",
  "resourceCreationTime": "2020-02-17T02:48:04.511Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [],
  "configuration": {
    "Enable": true,
    "FindingPublishingFrequency": "FIFTEEN_MINUTES",
    "DataSources": {
      "S3Logs": {
        "Enable": true
      },
      "Kubernetes": {
        "AuditLogs": {
          "Enable": true
        }
```

```
      }
    },

    "Id": "66666666666666666666666666666666",
    "Tags": []
  },
  "supplementaryConfiguration": {
    "CreatedAt": "2020-02-17T02:48:04.511Z"
  }
}
```

Veja a seguir um exemplo do uso da sintaxe do Guard para definir as variáveis e regras no cenário 2. No seguinte exemplo:

- As três primeiras linhas definem as variáveis usando o `let` comando. Eles recebem um nome e um valor derivados dos atributos do item de configuração.
- O bloco de `compliancecheck` regras adiciona uma dependência condicional quando que procura um par de `resourceType` valores-chave que corresponda. `AWS::GuardDuty::Detector` Se uma correspondência for encontrada, a regra prosseguirá com o restante dos atributos JSON e procurará correspondências nas três condições a seguir: `S3Logs.EnableKubernetes.AuditLogs.Enable`, e. `FindingPublishingFrequency`

```
let s3protection = true
let kubernetesprotection = true
let publishfrequency = 'FIFTEEN_MINUTES'

    rule compliancecheck when
        resourceType == "AWS::GuardDuty::Detector" {
            configuration.DataSources.S3Logs.Enable == %s3protection
            configuration.DataSources.Kubernetes.AuditLogs.Enable ==
 %kubernetesprotection
            configuration.FindingPublishingFrequency == %publishfrequency
        }
```

Para ver a política personalizada completa do Guard que implementa essa regra personalizada, consulte awsconfig-guard-cft-gd.yaml no repositório de código. GitHub Para o código do HashiCorp Terraform que implanta essa política personalizada no Guard, consulte awsconfig-guard-tf-gd.json no repositório de código.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo.

Outras ferramentas

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.

Repositório de código

O código desse padrão está disponível no AWS CloudFormation Guard repositório GitHub AWS Config with. Esse repositório de código contém amostras para os dois cenários descritos nesse padrão.

Épicos

Criação AWS Config de regras personalizadas

Tarefa	Descrição	Habilidades necessárias
(Opcional) Selecione pares de valores-chave para a regra.	Conclua estas etapas se você estiver definindo uma política personalizada do Guard. Se você estiver usando um dos exemplos de políticas para o cenário 1 ou 2, pule essas etapas. 1. Faça login no AWS Management Console	Administrador da AWS, engenheiro de segurança

Tarefa	Descrição	Habilidades necessárias
	e abra o AWS Config console. 2. No painel de navegação à esquerda, escolha Recursos. 3. No inventário de recursos, escolha o tipo de recurso para o qual você deseja criar uma regra AWS Config personalizada. 4. Escolha Exibir detalhes. 5. Escolha Exibir item de configuração (JSON). Esta seção se expande para mostrar o item de configuração no formato JSON. 6. Identifique os pares de valores-chave para os quais você gostaria de criar uma regra AWS Config personalizada.	
Crie a regra personalizada.	Usando os pares de valores-chave que você identificou anteriormente ou usando um dos exemplos de políticas do Guard fornecidos, siga as instruções em Criação de regras de política AWS Config personalizadas para criar uma regra personalizada.	Administrador da AWS, engenheiro de segurança

Tarefa	Descrição	Habilidades necessárias
Valide a regra personalizada.	Siga um destes procedimentos para validar a regra personalizada do Guard: • Digite o seguinte comando no AWS Command Line Interface (AWS CLI). `cfn-guard validate -r guard-s3.guard -d s3bucket-prod-pass.json` • Siga as instruções no modo Detective em Avaliando seus recursos com AWS Config regras para implantar a regra em. AWS Config Confirme se a sintaxe do Guard corresponde corretamente aos recursos correspondentes na conta ou arquivo de destino.	Administrador da AWS, engenheiro de segurança

Solução de problemas

Problema	Solução
Teste a política do Guard fora do AWS Config	O teste unitário pode ser feito em seu dispositivo local ou em um ambiente de desenvolvimento integrado (IDE), como um AWS Cloud9 IDE. Para realizar o teste unitário, faça o seguinte:

Problema	Solução

	1. Instale a AWS CloudFormation Guard CLI e suas dependências.
	2. Salve uma amostra de CI formatada em JSON em sua estação de trabalho como um arquivo.json.
	3. Salve a GuardDuty política em sua estação de trabalho como um arquivo.guard.
	4. Na CLI do Guard, insira o comando a seguir para validar o arquivo JSON de amostra usando a política do Guard.
	
	`cfn-guard validate \`
	`-r guard-s3.guard \`
	`-d s3bucket-prod-pass.json`

Depurar uma regra AWS Config personalizada	Em sua política do Guard, altere o `EnableDebugLogDelivery` valor para `true`. O valor padrão é `false`. As mensagens de log são armazenadas na Amazon CloudWatch.

Recursos relacionados

AWS documentação

- Criação de regras de política AWS Config personalizadas (AWS Config documentação)
- AWS CloudFormation Guard Regras de redação (documentação do Guard)

AWS postagens de blog e workshops

- Apresentando a AWS CloudFormation Guard versão 2.0 (postagem AWS no blog)

Outros recursos

- AWS CloudFormation Guard (GitHub)

- AWS CloudFormation Guard Documentação da CLI () GitHub

Crie um relatório consolidado das descobertas de segurança da Prowler a partir de vários Contas da AWS

Criado por Mike Virgilio (AWS), Andrea Di Fabio (AWS) e Jay Durga (AWS)

Resumo

O Prowler (GitHub) é uma ferramenta de linha de comando de código aberto que pode ajudá-lo a avaliar, auditar e monitorar suas contas da Amazon Web Services (AWS) quanto à adesão às melhores práticas de segurança. Nesse padrão, você implanta o Prowler em um ambiente centralizado Conta da AWS em sua organização, gerenciado por AWS Organizations, e depois usa o Prowler para realizar uma avaliação de segurança de todas as contas na organização.

Embora existam muitos métodos para implantar e utilizar o Prowler para uma avaliação, essa solução foi projetada para implantação rápida, análise completa de todas as contas na organização ou contas de destino definidas e relatórios acessíveis das descobertas de segurança. Nessa solução, quando a Prowler conclui a avaliação de segurança de todas as contas da organização, ela consolida os resultados. Ele também filtra todas as mensagens de erro esperadas, como erros relacionados a restrições que impedem o Prowler de escanear buckets do Amazon Simple Storage Service (Amazon S3) em contas provisionadas por meio do AWS Control Tower. Os resultados filtrados e consolidados são relatados em um modelo do Microsoft Excel incluído nesse padrão. Você pode usar esse relatório para identificar possíveis melhorias nos controles de segurança em sua organização.

Essa solução foi projetada com o seguinte em mente:

- Os AWS CloudFormation modelos reduzem o esforço necessário para implantar os AWS recursos nesse padrão.
- Você pode ajustar os parâmetros nos CloudFormation modelos e no script prowler_scan.sh no momento da implantação para personalizar os modelos para seu ambiente.
- As velocidades de avaliação e emissão de relatórios do Prowler são otimizadas por meio do processamento paralelo de Contas da AWS resultados agregados, relatórios consolidados com correções recomendadas e visualizações geradas automaticamente.
- O usuário não precisa monitorar o progresso da verificação. Quando a avaliação for concluída, o usuário é notificado por meio de um tópico do Amazon Simple Notification Service (Amazon SNS) para que ele possa recuperar o relatório.

- O modelo de relatório ajuda você a ler e avaliar somente os resultados relevantes para toda a organização.

Pré-requisitos e limitações

Pré-requisitos

- E Conta da AWS para hospedar serviços e ferramentas de segurança, gerenciados como uma conta membro de uma organização em AWS Organizations. Nesse padrão, essa conta é chamada de conta de segurança.
- Na conta de segurança, você deve ter uma sub-rede privada com acesso de saída à Internet. Para obter instruções, consulte VPC com servidores em sub-redes privadas e NAT na documentação da Amazon Virtual Private Cloud (Amazon VPC). Você pode estabelecer acesso à Internet usando um gateway NAT provisionado em uma sub-rede pública.
- Acesso à conta AWS Organizations de gerenciamento ou a uma conta que tenha delegado permissões de administrador para CloudFormation. Para obter instruções, consulte Registrar um administrador delegado na CloudFormation documentação.
- Habilite o acesso confiável entre AWS Organizations CloudFormation e. Para obter instruções, consulte Habilitar acesso confiável com AWS Organizations na CloudFormation documentação.

Limitações

- O alvo Contas da AWS deve ser gerenciado como uma organização em AWS Organizations. Se você não estiver usando AWS Organizations, você pode atualizar o CloudFormation modelo IAM-ProwlerExecRole .yaml e o script prowler_scan.sh para seu ambiente. Em vez disso, você fornece uma lista Conta da AWS IDs e regiões nas quais deseja executar o script.
- O CloudFormation modelo foi projetado para implantar a instância Amazon Elastic Compute Cloud (Amazon EC2) em uma sub-rede privada com acesso de saída à Internet. O AWS Systems Manager Agente (Agente SSM) requer acesso de saída para alcançar o ponto final do AWS Systems Manager serviço, e você precisa de acesso de saída para clonar o repositório de código e instalar dependências. Se quiser usar uma sub-rede pública, você deve modificar o modelo prowler-resources.yaml para associar um endereço IP elástico à instância. EC2

Versões do produto

- Prowler versão 4.0 ou posterior

Arquitetura

O diagrama mostra o seguinte processo:

1. Usando o Gerenciador de Sessões, um recurso do AWS Systems Manager, o usuário se autentica na EC2 instância e executa o script prowler_scan.sh. Esse script de shell executa as etapas de 2 a 8.
2. A EC2 instância assume a função do `ProwlerEC2Role` IAM, que concede permissões para acessar o bucket do S3 e assumir as funções `ProwlerExecRole` do IAM nas outras contas da organização.
3. A EC2 instância assume a função `ProwlerExecRole` do IAM na conta de gerenciamento da organização e gera uma lista das contas na organização.
4. A EC2 instância assume a função do `ProwlerExecRole` IAM nas contas dos membros da organização (chamadas de contas de carga de trabalho no diagrama de arquitetura) e realiza uma avaliação de segurança em cada conta. As descobertas são armazenadas como arquivos CSV e HTML na EC2 instância.

   > **Note**
   >
   > Os arquivos HTML são uma saída da avaliação do Prowler. Devido à natureza do HTML, eles não são concatenados, processados ou usados diretamente nesse padrão. No entanto, eles podem ser úteis para a análise de relatórios de contas individuais.

5. A EC2 instância processa todos os arquivos CSV para remover erros conhecidos e esperados e consolida as descobertas restantes em um único arquivo CSV.
6. A EC2 instância empacota os resultados individuais da conta e os resultados agregados em um arquivo zip.
7. A EC2 instância carrega o arquivo zip no bucket do S3.
8. Uma EventBridge regra detecta o upload do arquivo e usa um tópico do Amazon SNS para enviar um e-mail ao usuário notificando-o de que a avaliação foi concluída.
9. O usuário baixa o arquivo zip do bucket do S3. O usuário importa os resultados para o modelo do Excel e revisa os resultados.

Ferramentas

Serviços da AWS

- O Amazon Elastic Compute Cloud (Amazon EC2) fornece capacidade de computação escalável no. Nuvem AWS Você poderá iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala. Esse padrão usa o Session Manager, um recurso do Systems Manager.

Outras ferramentas

- O Prowler é uma ferramenta de linha de comando de código aberto que ajuda você a avaliar, auditar e monitorar suas contas quanto à adesão às melhores práticas de segurança e a outras AWS estruturas e padrões de segurança.

Repositório de código

O código desse padrão está disponível na Avaliação de Segurança de GitHub Várias Contas por meio do repositório Prowler. O repositório de código contém os seguintes arquivos:

- prowler_scan.sh — Esse script bash é usado para iniciar uma avaliação de segurança múltipla do Prowler, Contas da AWS em paralelo. Conforme definido em Prowler-resources.yaml CloudFormationtemplate, esse script é implantado automaticamente na pasta na instância. `usr/local/prowler` EC2
- Prowler-resources.yaml — Você usa esse CloudFormation modelo para criar uma pilha na conta de segurança na organização. Esse modelo implanta todos os recursos necessários para essa conta a fim de oferecer suporte à solução. Essa pilha deve ser implantada antes do modelo IAM-ProwlerExecRole .yaml. Não recomendamos que você implante esses recursos em uma conta que hospeda workloads críticas de produção.

> **Note**
>
> Se essa pilha for excluída e reimplantada, você deverá reconstruir o conjunto de `ProwlerExecRole` pilhas para reconstruir as dependências entre contas entre as funções do IAM.

- IAM- ProwlerExecRole .yaml — Você usa esse CloudFormation modelo para criar um conjunto de pilhas que implanta a função `ProwlerExecRole` do IAM em todas as contas da organização, incluindo a conta de gerenciamento.
- prowler-report-template.xlsm — Você usa esse modelo do Excel para processar as descobertas do Prowler. As tabelas dinâmicas no relatório fornecem recursos de pesquisa, gráficos e descobertas consolidadas.

Épicos

Preparar-se para implantação

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de códigos.	1. Em uma interface da linha de comando, altere seu diretório de trabalho para o local em que você deseja armazenar os arquivos de amostra. 2. Digite o comando:	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/aws-samples/multi-account-security-assessment-via-prowler.git`	
Consulte os modelos.	1. No repositório clonado, abra os arquivos Prowler-resources.yaml e IAM- .yaml. ProwlerExecRole 2. Analise os recursos criados por esses modelos e ajuste-os conforme necessário para seu ambiente. Para obter mais informações, consulte Trabalhando com modelos na CloudFormation documentação. 3. Salve e feche os arquivos Prowler-resources.yaml e IAM- .yaml. ProwlerExecRole	AWS DevOps

Crie as CloudFormation pilhas

Tarefa	Descrição	Habilidades necessárias
Provisione recursos na conta de segurança.	Usando o modelo prowler-resources.yaml, você cria uma CloudFormation pilha que implanta todos os recursos necessários na conta de	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	segurança. Para obter instruções, consulte Criação de uma pilha na CloudForm ation documentação. Observe o seguinte ao implantar esse modelo: 1. Na página Especificar modelo, escolha O modelo está pronto e, em seguida, carregue o arquivo prowler-resources.yaml. 2. Na página Specify stack details (Especificar detalhes da pilha), na caixa Stack name (Nome da pilha), insira `Prowler-Resources` . 3. Na seção Parameters (Parâmetros), insira o seguinte: • `VPCId`: selecione uma VPC na conta. • `SubnetId`: selecione uma sub-rede privada que tenha acesso à Internet. Observação: se você selecionar uma sub-rede pública, a EC2 instância não receberá um endereço IP público porque o CloudFormation modelo, por padrão, não	

Tarefa	Descrição	Habilidades necessárias

	provisiona e anexa um endereço IP elástico.
	• `InstanceType` : selecione um tamanho de instância com base no número de avaliações paralelas:
	  • Para 10, escolha `r6i.large` .
	  • Para 12, escolha `r6i.xlarge` .
	  • Para 14 a 18 anos, escolha `r6i.2xlarge` .
	• `InstanceImageId` : deixe o padrão para o Amazon Linux.
	• `KeyPairName` : se você estiver usando SSH para acessar, especifique o nome de um par de chaves existente.
	• `PermittedSSHInbound` : se você estiver usando SSH para acesso, especifique um bloco CIDR permitido. Se você não estiver usando SSH, mantenha o valor padrão de `127.0.0.1` .
	• `BucketName` : o valor padrão é `prowler-output-`	

Tarefa	Descrição	Habilidades necessárias
	`<accountID>-<region>` . Você pode modificar isso conforme necessário. Se você especificar um valor personalizado, a ID da conta e a região serão automaticamente anexados ao valor especificado. • `EmailAddress` : especifique um endereço de e-mail para uma notificação do Amazon SNS quando o Prowler concluir a avaliação e carregar o arquivo .zip no bucket do S3. Nota: a configuração da assinatura do SNS deve ser confirmada antes que o Prowler conclua a avaliação ou uma notificação não será enviada. • `IAMProwlerEC2Role` : mantenha o padrão, a menos que suas convenções de nomenclatura exijam um nome diferente para esse perfil do IAM.	

Tarefa	Descrição	Habilidades necessárias
	• `IAMProwlerExecRole` — Mantenha o padrão, a menos que outro nome seja usado ao implantar o arquivo IAM- ProwlerExecRole .yaml. • `Parallelism` : especifique o número de avaliações paralelas a serem realizadas. Certifique-se de que o valor no parâmetro `InstanceType` suporte esse número de avaliações paralelas. • `FindingOutput` : se você quiser excluir os resultados da aprovação , selecione `FailOnly`. Isso reduz significativamente o tamanho da saída e se concentra nas verificações que talvez precisem ser resolvidas. Se você quiser incluir resultados de aprovação , selecione `FailAndPass` . 4. Na página Revisar, selecione Os seguintes recursos exigem recursos: [AWS::IAM::Role] e escolha Criar pilha.	

Tarefa	Descrição	Habilidades necessárias
	5. Depois que a pilha for criada com sucesso, no CloudFormation console, na guia Saídas, copie o `ProwlerEC2Role` Amazon Resource Name (ARN). Você usa esse ARN posteriormente ao implantar o arquivo IAM- ProwlerEx ecRole .yaml.	

Tarefa	Descrição	Habilidades necessárias
Provisione o perfil do IAM nas contas dos membros.	Na conta AWS Organizations de gerenciamento ou em uma conta com permissões de administrador delegado para CloudFormation, use o modelo IAM- ProwlerExecRole .yaml para criar um CloudForm ation conjunto de pilhas. O conjunto de pilhas implanta o perfil `ProwlerExecRole` do IAM para todas as contas-membro da organização. Para obter instruções, consulte Criar um conjunto de pilhas com permissões gerenciad as pelo serviço na documenta ção. CloudFormation Observe o seguinte ao implantar esse modelo: 1. Em Preparar modelo, escolha O modelo está pronto e, em seguida, carregue o arquivo IAM-ProwlerExecRole .yaml. 2. Na página Especificar StackSet detalhes, nomeie o conjunto `IAM-Prowl erExecRole` de pilhas. 3. Na seção Parameters (Parâmetros), insira o seguinte: • `AuthorizedARN` : insira o ARN `ProwlerEC`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`2Role` , que você copiou ao criar a pilha `Prowler-Resources` . • `ProwlerExecRoleNam e` : mantenha o valor padrão de `ProwlerEx ecRole` , a menos que outro nome tenha sido usado ao implantar o arquivo Prowler-r esources.yaml. 4. Em Permissions (Permissõ es), escolha Service-managed permissions (Permissões gerenciadas pelo serviço). 5. Na página Set deploymen t options (Definir opções de implantação) em Deployment targets (Destinos da implantaç ão), escolha Deploy to organization (Implantar na organização) e aceite todos os padrões. Nota: se você quiser que as pilhas sejam implantad as em todas as contas dos membros simultaneamente, defina Máximo de contas simultâneas e Tolerância a falhas como um valor alto, como `100`.	

Tarefa	Descrição	Habilidades necessárias
	6. Em Regiões de implantação, escolha Região da AWS onde a EC2 instância do Prowler está implantada. Como os recursos do IAM são globais e não regionais, isso implanta o perfil do IAM em todas as regiões ativas. 7. Na página de revisão, selecione Eu reconheço que AWS CloudFormation posso criar recursos do IAM com nomes personalizados e, em seguida, escolha Criar StackSet. 8. Monitore a guia Instâncias de pilha (para o status da conta individual) e a guia Operações (para o status geral) para determinar quando a implantação será concluída.	

Tarefa	Descrição	Habilidades necessárias
Provisione o perfil do IAM na conta de gerenciamento.	Usando o modelo IAM-ProwlerExecRole .yaml, você cria uma CloudFormation pilha que implanta a função do `ProwlerExecRole` IAM na conta de gerenciamento da organização. O conjunto de pilhas que você criou anteriormente não implanta o perfil do IAM na conta de gerenciamento. Para obter instruções, consulte Criação de uma pilha na CloudFormation documentação. Observe o seguinte ao implantar esse modelo: 1. Na página Especificar modelo, escolha O modelo está pronto e, em seguida, carregue o arquivo IAM-ProwlerExecRole .yaml. 2. Na página Specify stack details (Especificar detalhes da pilha), na caixa Stack name (Nome da pilha), insira `IAM-ProwlerExecRole` . 3. Na seção Parameters (Parâmetros), insira o seguinte: • `AuthorizedARN` : insira o ARN `ProwlerEC2Role` , que você	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	copiou ao criar a pilha `Prowler-Resources` . • `ProwlerExecRoleName` : mantenha o valor padrão de `ProwlerExecRole` , a menos que outro nome tenha sido usado ao implantar o arquivo Prowler-resources.yaml. 4. Na página Revisar, selecione Os seguintes recursos exigem recursos: [AWS::IAM::Role] e escolha Criar pilha.	

Realize a avaliação de segurança do Prowler

Tarefa	Descrição	Habilidades necessárias
Execute a verificação.	1. Faça login na conta de segurança na organização. 2. Usando o Gerenciador de Sessões, conecte-se à EC2 instância do Prowler que você provisionou anteriormente. Para obter instruções, consulte Conectar-se à instância do Linux usando o Session Manager. Se você não conseguir se conectar, consulte a seção Solução de problemas desse padrão.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	3. Navegue até `usr/local/prowler` e abra o arquivo prowler_scan.sh.
	4. Revise e modifique os parâmetros e variáveis ajustáveis neste script conforme necessário para seu ambiente. Para obter mais informações sobre as opções de personalização, consulte os comentários no início do script.
	
	Por exemplo, em vez de obter uma lista de todas as contas dos membros da organização a partir da conta de gerenciamento, você pode modificar o script para especificar Conta da AWS IDs ou Regiões da AWS que deseja verificar , ou pode referenciar um arquivo externo que contenha esses parâmetro s.
	5. Salve e feche o arquivo prowler_scan.sh.
	6. Insira os comandos a seguir. Isso executa o script prowler_scan.sh.
	
	`sudo -i`
	`screen`	

Tarefa	Descrição	Habilidades necessárias

	`cd /usr/local/prowler`
	`./prowler_scan.sh`
	
	Observe o seguinte:
	• O comando screen permite que o script continue em execução caso a conexão atinja o tempo limite ou você perca o acesso ao console.
	• Após o início da digitalização, você pode forçar a separação da tela pressionando Ctrl+A D. A tela se separa e você pode fechar a conexão da instância e permitir que a avaliação continue.
	• Para retomar uma sessão desanexada, conecte-se à instância, insira `sudo -i` e depois `screen -r`.
	• Para monitorar o progresso das avaliações de contas individuais, você pode navegar até o diretório `usr/local/prowler` e inserir o comando `tail -f output/stdout-<account-id>` .	

Tarefa	Descrição	Habilidades necessárias
	7. Aguarde até que o Prowler conclua as verificações em todas as contas. O script avalia várias contas ao mesmo tempo. Quando a avaliação for concluída em todas as contas, você receberá uma notificação se tiver especificado um endereço de e-mail ao implantar o arquivo Prowler-resources.yaml.	

Tarefa	Descrição	Habilidades necessárias
Recupere as descobertas de Prowler.	1. Baixe o arquivo `prowler-output-<assessDate>.zip` do bucket `prowler-output-<accountID>-<region>` . Para obter instruções, consulte Baixar um objeto na documentação do Amazon S3. 2. Exclua todos os objetos no bucket, incluindo o arquivo que você baixou. Essa é uma prática recomendada para otimização de custos e para garantir que você possa excluir a `Prowler-Resources` CloudFormation pilha a qualquer momento. Para obter instruções, consulte Excluir objetos na documentação do Amazon S3.	AWS geral
Pare a EC2 instância.	Para evitar o faturamento enquanto a instância estiver ociosa, interrompa a EC2 instância que executa o Prowler. Para obter instruções, consulte Pare e inicie suas instâncias na EC2 documentação da Amazon.	AWS DevOps

Crie um relatório das descobertas

Tarefa	Descrição	Habilidades necessárias
Importe as descobertas.	1. No Excel, abra o prowler-report-templatearquivo.xlsx e escolha a planilha Prowler CSV. 2. Exclua todos os dados de amostra, incluindo a linha do cabeçalho. Se você for perguntado se deseja excluir a consulta associada aos dados que estão sendo removidos, escolha Não. A exclusão da consulta pode afetar a funcionalidade das tabelas dinâmicas no modelo do Excel. 3. Extraia o conteúdo do arquivo zip que você baixou do bucket do S3. 4. No Excel, abra o prowler-fullorgresults-accessdeniedfilteredarquivo.txt. Recomendamos que você use esse arquivo porque os erros mais comuns e não acionáveis já foram removidos, como `Access Denied` erros relacionados a tentativas de varredura de recursos. AWS Control Tower Se você quiser as descobertas não filtradas, abra o arquivo prowler-	AWS geral

Tarefa	Descrição	Habilidades necessárias
	fullorgresults.txt em vez disso. 5. Selecione a coluna A. 6. Se você estiver usando o Windows, digite Ctrl+C ou, se estiver usando o macOS, digite Cmd+C. Isso copia todos os dados para a área de transferência. 7. No modelo de relatório do Excel, na planilha Prowler CSV, selecione a célula A1. 8. Se você estiver usando o Windows, digite Ctrl+V ou, se estiver usando o macOS, digite Cmd+V. Isso irá colar as descobertas no relatório. 9. Confirme se todas as células que contêm dados colados foram seleciona das. Caso contrário, selecione a coluna A. 10. Na guia Dados, escolha Texto em colunas. 11. No assistente, faça o seguinte: • Para a etapa 1, escolha Delimitado. • Para a etapa 2, para Delimitadores, escolha Ponto e vírgula. No painel Visualização de dados,	

Tarefa	Descrição	Habilidades necessárias
	confirme se os dados estão sendo separados em colunas. • Para a etapa 3, escolha Concluir. 12. Confirme se os dados de texto estão delimitados em várias colunas. 13. Salve o relatório do Excel com um novo nome. 14. Pesquise e exclua quaisquer erros `Access Denied` nas descobertas. Para obter instruções sobre como removê-los programaticamente, consulte Remoção programática de erros na seção Informações adicionais.	

Tarefa	Descrição	Habilidades necessárias
Finalize o relatório.	1. Escolha a planilha Descobertas e, em seguida, selecione a célula A17. Essa célula é o cabeçalho da tabela dinâmica. 2. Na faixa de opções, em PivotTable Ferramentas, escolha Analisar e, em Atualizar, escolha Atualizar tudo. Isso atualiza as tabelas dinâmicas com o novo conjunto de dados. 3. Por padrão, o Excel não exibe Conta da AWS números corretamente. Para corrigir a formatação do número, faça o seguinte: • Na planilha de Descobertas, abra o menu de contexto (clique com o botão direito) da coluna A e escolha Formatar células. • Escolha Número e, em Casas decimais, insira `0`. • Escolha OK. Observação: Se um Conta da AWS número começar com um ou mais zeros, o Excel removerá automaticamente os zeros. Se você ver um número de conta com menos de 12 dígitos	AWS geral

Tarefa	Descrição	Habilidades necessárias
	no relatório, os dígitos que faltam são zeros no início do número. 4. (Opcional) Você pode recolher campos para facilitar a leitura das descobertas. Faça o seguinte: • Na planilha Descobertas, se você mover o cursor para a linha entre as linhas 18 e 19 (o espaço entre o cabeçalho crítico e a primeira descoberta), o ícone do cursor mudará para uma pequena seta apontando para baixo. • Clique para seleciona r todos os campos de descoberta. • Abra o menu de contexto (clique com o botão direito do mouse), localize Expandir/ Recolher e escolha Recolher. 5. Para obter detalhes sobre a avaliação, consulte as planilhas Descobertas, Gravidade e Aprovação.	

(Opcional) Atualize o Prowler ou os recursos no repositório de código

Tarefa	Descrição	Habilidades necessárias

Atualize o Prowler.	Se você deseja atualizar o Prowler para a versão mais recente, faça o seguinte:
	1. Conecte-se à EC2 instância do Prowler usando o Gerenciador de Sessões. Para obter instruções, consulte Conectar-se à instância do Linux usando o Session Manager
	2. Insira o comando da a seguir.
	`sudo -i`
	`pip3 install --upgrade prowler`
		AWS geral

Atualize o script prowler_scan.sh.	Se você quiser atualizar o script prowler_scan.sh para a versão mais recente no repositório, faça o seguinte: 1. Conecte-se à EC2 instância do Prowler usando o Gerenciador de Sessões. Para obter instruções, consulte Conectar-se à instância do Linux usando o Session Manager 2. Insira o comando da a seguir.	AWS geral

Tarefa	Descrição	Habilidades necessárias

	`sudo -i`
	3. Navegue até o diretório de scripts do Prowler.
	`cd /usr/local/prowler`
	4. Digite o comando a seguir para armazenar o script local para que você possa mesclar as alterações personalizadas na versão mais recente.
	`git stash`
	5. Digite o seguinte comando para obter a versão mais recente do script.
	`git pull`
	6. Digite o seguinte comando para mesclar o script personalizado com a versão mais recente do script.
	`git stash pop`
	Note
	Você pode receber avisos relacionados a qualquer arquivo	

Tarefa	Descrição	Habilidades necessárias
	gerado localmente que não esteja no GitHub repositório, como encontrar relatórios. Você pode ignorá-los, desde que o prowler_scan.sh mostre que as alterações armazenadas localmente foram mescladas novamente.	

Limpar (opcional)

Tarefa	Descrição	Habilidades necessárias
Exclua todos os recursos implantados.	Você pode deixar os recursos implantados nas contas. Se você desligar a EC2 instância quando ela não estiver em uso e mantiver o bucket do S3 vazio, isso reduzirá os custos de manutenção dos recursos para futuras verificações. Para desprovisionar todos os recursos, faça o seguinte: 1. Exclua a pilha `IAM-ProwlerExecRole` provisionada na conta de gerenciamento. Para obter instruções, consulte Como excluir uma	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	pilha na CloudFormation documentação. 2. Exclua o conjunto de pilhas `IAM-ProwlerExecRole` provisionado na conta de gerenciamento da organização ou na conta de administrador delegada. Para obter instruções, consulte Excluir um conjunto de pilhas na CloudFormation documentação. 3. Excluir todos os objetos no bucket S3 `prowler-output` . Para obter instruções, consulte Excluir objetos na documentação do Amazon S3. 4. Exclua a pilha `Prowler-Resources` provisionada na conta de segurança . Para obter instruções, consulte Como excluir uma pilha na CloudFormation documentação.	

Solução de problemas

Problema	Solução
Não é possível se conectar à EC2 instância usando o Gerenciador de Sessões.	O SSM Agent deve conseguir se comunicar com o endpoint do Session Manager. Faça o seguinte: 1. Valide que a sub-rede em que a EC2 instância está implantada tem acesso à Internet. 2. Reinicie a EC2 instância.
Ao implantar o conjunto de pilhas, o CloudFormation console solicita que você faça isso. `Enable trusted access with AWS Organizations to use service-managed permissions`	Isso indica que o acesso confiável não foi habilitado entre AWS Organizations CloudFormation e. É necessário o acesso confiável para implantar o conjunto de pilhas gerenciadas pelo serviço. Escolha o botão para habilitar o acesso confiável. Para obter mais informações, consulte Habilitar acesso confiável na CloudFormation documentação.

Recursos relacionados

AWS documentação

- Implementando controles de segurança em AWS (AWS orientação prescritiva)

Outros recursos

- Ladrão (2) GitHub

Mais informações

Removendo erros de forma programática

Se os resultados contiverem erros `Access Denied`, você deverá removê-los das descobertas. Esses erros geralmente ocorrem devido a permissões de influência externa que impedem o Prowler de avaliar um recurso específico. Por exemplo, algumas verificações falham ao revisar os buckets do S3 provisionados por meio de. AWS Control Tower Você pode extrair programaticamente esses resultados e salvar os resultados filtrados como um novo arquivo.

Os comandos a seguir removem as linhas que contêm uma única sequência de texto (um padrão) e, em seguida, enviam os resultados para um novo arquivo.

- Para Linux ou macOS (Grep)

```
grep -v -i "Access Denied getting bucket" myoutput.csv > myoutput_modified.csv
```

- Para Windows (PowerShell)

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket' -NotMatch >
 myoutput_modified.csv
```

Os comandos a seguir removem as linhas que correspondem a mais de uma sequência de texto e, em seguida, enviam os resultados para um novo arquivo.

- Para Linux ou macOS (usa um tubo de escape entre as strings de caracteres)

```
grep -v -i 'Access Denied getting bucket\|Access Denied Trying to Get' myoutput.csv >
 myoutput_modified.csv
```

- Para Windows (usa uma vírgula entre strings)

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket', 'Access
 Denied Trying to Get' -NotMatch > myoutput_modified.csv
```

Exemplos de relatório

A imagem a seguir é um exemplo da planilha de Descobertas no relatório de descobertas consolidadas da Prowler.

A imagem a seguir é um exemplo da planilha de Aprovação no relatório de descobertas consolidadas do Prowler. (Por padrão, os resultados de aprovação são excluídos da saída.)

A imagem a seguir é um exemplo da planilha de Severidade do relatório de descobertas consolidadas do Prowler.

Exclua volumes não utilizados do Amazon EBS usando e AWS ConfigAWS Systems Manager

Criado por Sankar Sangubotla (AWS)

Resumo

O ciclo de vida de um volume do Amazon Elastic Block Store (Amazon EBS) geralmente é independente do ciclo de vida da instância do Amazon Elastic Compute Cloud (Amazon EC2) à qual ele está vinculado. A menos que você selecione a opção Excluir ao encerrar no momento da execução, o encerramento da EC2 instância da Amazon separa o volume do Amazon EBS, mas não o exclui. Especialmente em ambientes de desenvolvimento e teste em que é comum iniciar e encerrar EC2 instâncias da Amazon, isso pode resultar em um grande número de volumes não utilizados do Amazon EBS. Os volumes do Amazon EBS acumulam cobranças em você Conta da AWS, independentemente de estarem sendo usados. A exclusão desses volumes pode ajudá-lo a otimizar os custos do seu Contas da AWS. Além disso, excluir volumes não utilizados do Amazon EBS é uma prática recomendada de segurança para impedir o acesso a quaisquer dados não utilizados e potencialmente confidenciais nesses volumes.

AWS Config pode ajudá-lo a corrigir manualmente ou automaticamente recursos não compatíveis. Esse padrão descreve como configurar uma AWS Config regra e uma ação de remediação automática que exclui volumes não utilizados do Amazon EBS na conta. A ação de remediação é um runbook predefinido para automação, um recurso de. AWS Systems ManagerÉ possível configurar o runbook para criar um snapshot do volume antes de excluí-lo.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Identity and Access Management Permissões (IAM) para executar o `AWSConfigRemediation-DeleteUnusedEBSVolume` runbook for Automation, um recurso do Systems Manager. Para obter mais informações, consulte Permissões obrigatórias do IAM em AWSConfigRemediation-DeleteUnusedEBSVolume.
- Um ou mais volumes do Amazon EBS não utilizados.

Limitações

- Os volumes não utilizados do Amazon EBS devem estar no estado `available`.

Arquitetura

Arquitetura de destino

1. A AWS Config regra avalia os volumes do Amazon EBS.
2. A regra retorna uma lista de recursos compatíveis e não compatíveis. Os volumes do Amazon EBS que estão no `available` estado, que são volumes não utilizados, são considerados não compatíveis.
3. AWS Config inicia automaticamente o runbook de automação.
4. Se configurado, o Systems Manager cria snapshots dos volumes não utilizados antes de excluí-los.
5. O Systems Manager exclui os volumes não utilizados do Amazon EBS.

Automação e escala

É possível aplicar essa solução em todas as contas de sua organização. Para obter mais informações, consulte Gerenciamento de regras em todas as contas da sua organização na AWS Config documentação.

Ferramentas

- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala.
- AWS Systems Manager A automação simplifica as tarefas comuns de manutenção, implantação e remediação para muitos. Serviços da AWS

Épicos

Configurar a AWS Config regra

Tarefa	Descrição	Habilidades necessárias
Crie uma função para o runbook de automação.	Crie uma função chamada de `AssumeRole` . O Systems Manager Automation usa essa função para executar o runbook. Para obter instruções, consulte Configurar o acesso a um de perfil de serviço (perfil assumido) para automações na documentação do Systems Manager.	Administrador de sistemas AWS
Ligue o AWS Config gravador.	Siga as instruções em Configuração AWS Config com o console na AWS Config documentação para garantir que ele AWS Config esteja em execução e configurado para registrar volumes do Amazon EBS.	Administrador de sistemas AWS
Execute a regra.	1. Siga as instruções em Avaliação de seus recursos na AWS Config documentação para executar a `ec2-volume-inuse-check` regra. Aguarde a avaliação antes de prosseguir. 2. Na página Regras, selecione a regra `ec2-volume-inuse-check` e em Recursos dentro do	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias
	escopo, escolha Em não conformidade. 3. Confirme se há um ou mais volumes não utilizados do Amazon EBS nos resultados da avaliação.	

Configure a correção automática de volumes não utilizados do Amazon EBS

Tarefa	Descrição	Habilidades necessárias
Adicione a ação de correção automática.	1. Na página Regras, selecione a `ec2-volume-inuse-check` regra. 2. Siga as instruções em Configurando a remediação automática na AWS Config documentação. Observe o seguinte: 3. Na seção Detalhes da ação de correção, escolha `AWSConfigRemediation-DeleteUnusedEBSVolume` . • Selecione o parâmetro Resource ID e, na lista, escolha VolumeId. Em tempo de execução, esse parâmetro é substituído pelo ID do volume não compatível do Amazon EBS.	Administrador de sistemas AWS

Tarefa	Descrição	Habilidades necessárias

	• Na seção Parâmetros forneça valores para os seguintes parâmetros:
	  • `CreateSnapshot` — (Opcional) Se configura da como`true`, a automação cria um snapshot do volume do Amazon EBS antes de ser excluído.
	  • `AutomationAssumeRole` : insira o nome do recurso da Amazon (ARN) do perfil de serviço `AssumeRole` criado anteriormente.	

Teste a correção automática da AWS Config regra.	1. No AWS Config console, na página Regras, selecione a `ec2-volume-inuse-check` regra. 2. No menu Actions (Ações), escolha Re-evaluate (Reavaliar). 3. Permita que a regra avalie os recursos não compatíveis e, em seguida, confirme se os volumes não utilizados do Amazon EBS foram excluídos.	Administrador de sistemas AWS

Solução de problemas

Problema	Solução
AWS Config não reflete com precisão o estado do recurso.	Às vezes, AWS Config não atualiza o estado dos recursos. Desligue o gravador e ligue-o novamente na página AWS Config Configura ções. O gravador captura o estado dos recursos. Para recursos recém-criados ou excluídos, pode levar algum tempo para que o gravador reflita o estado atual. Para obter mais informações sobre os estados de volume do Amazon EBS, consulte Estados de volume na documentação do Amazon EBS.

Recursos relacionados

- AWSConfigRemediation-DeleteUnusedEBSVolume caderno de corrida
- regra ec-2 volume-inuse-check
- Correção de recursos não compatíveis com regras AWSAWS Config

Implemente e gerencie AWS Control Tower controles usando AWS CDK e CloudFormation

Criado por Iker Reina Fuente (AWS) e Ivan Girardi (AWS)

Resumo

Esse padrão descreve como usar, AWS Cloud Development Kit (AWS CDK) implementar AWS CloudFormation e administrar AWS Control Tower controles preventivos, detectivos e proativos como infraestrutura como código (IaC). Um controle (também conhecido como corrimão) é uma regra de alto nível que fornece governança contínua para seu ambiente geral. AWS Control Tower Por exemplo, você pode usar controles para exigir o registro em log Contas da AWS e, em seguida, configurar notificações automáticas caso ocorram eventos específicos relacionados à segurança.

AWS Control Tower ajuda você a implementar controles preventivos, detectivos e proativos que governam seus AWS recursos e monitoram a conformidade em vários. Contas da AWS Cada controle impõe uma única regra. Neste padrão, você usa um modelo de IaC fornecido para especificar quais controles você deseja implantar em seu ambiente.

AWS Control Tower os controles se aplicam a uma unidade organizacional (OU) inteira, e o controle afeta cada um Conta da AWS dentro da OU. Portanto, quando os usuários realizam qualquer ação em qualquer conta em sua zona de pouso, a ação está sujeita aos controles que governam a UO.

A implementação de AWS Control Tower controles ajuda a estabelecer uma base de segurança sólida para sua AWS landing zone. Ao usar esse padrão para implantar os controles como IaC por meio de CloudFormation e AWS CDK, você pode padronizar os controles em sua landing zone e implantá-los e gerenciá-los com mais eficiência. Essa solução usa cdk_nag para verificar o aplicativo durante a AWS CDK implantação. Essa ferramenta verifica se o aplicativo está aderindo às AWS melhores práticas.

Para implantar AWS Control Tower controles como IaC, você também pode usar o HashiCorp Terraform em vez de. AWS CDK Para obter mais informações, consulte Implantar e gerenciar AWS Control Tower controles usando o Terraform.

Público-alvo

Esse padrão é recomendado para usuários com experiência com AWS Control Tower CloudFormation AWS CDK,, AWS Organizations e.

Pré-requisitos e limitações

Pré-requisitos

- Ativo Contas da AWS gerenciado como uma organização AWS Organizations e uma AWS Control Tower landing zone. Para obter instruções, consulte Introdução na AWS Control Tower documentação.
- AWS Command Line Interface (AWS CLI), instalado e configurado.
- Gerenciador de pacotes Node (npm), instalado e configurado para o. AWS CDK
- Pré-requisitos para. AWS CDK
- Permissões para assumir uma função existente AWS Identity and Access Management (IAM) em uma conta de implantação.
- Permissões para assumir uma função do IAM na conta de gerenciamento da organização que pode ser usada para inicializar. AWS CDK A função deve ter permissões para modificar e implantar CloudFormation recursos. Para obter mais informações, consulte Bootstrapping na documentação. AWS CDK
- Permissões para criar políticas e perfis do IAM na conta de gerenciamento da organização. Para obter mais informações, consulte Permissões necessárias para acessar recursos do IAM na documentação do IAM.

Limitações

- Esse padrão fornece instruções para implantar essa solução Contas da AWS, desde uma conta de implantação até a conta de gerenciamento da organização. Para fins de teste, você pode implantar essa solução diretamente na conta de gerenciamento, mas as instruções para essa configuração não são fornecidas explicitamente.
- Para AWS Control Tower controles, esse padrão requer o uso de identificadores globais que estejam no seguinte formato:

```
arn:<PARTITION>:controlcatalog:::control/<CONTROL_CATALOG_OPAQUE_ID>
```

  As versões anteriores desse padrão usavam identificadores regionais que não são mais suportados. Recomendamos que você migre de identificadores regionais para identificadores globais. Os identificadores globais ajudam você a gerenciar controles e expandir o número de controles que você pode usar.

> **Note**
>
> Na maioria dos casos, o valor de `<PARTITION>` é `aws`.

Versões do produto

- AWS Control Tower versão 3.2 ou posterior
- Python, versão 3.9 ou mais recente
- npm versão 8.9.0 ou mais recente

Arquitetura

Esta seção fornece uma visão geral de alto nível dessa solução e da arquitetura estabelecida pelo código de exemplo. O diagrama a seguir mostra os controles implantados nas várias contas na UO.

AWS Control Tower os controles são categorizados de acordo com seu comportamento e orientação.

Há três tipos principais de comportamentos de controle:

1. Os controles preventivos são projetados para evitar que ações ocorram. Eles são implementados com políticas de controle de serviço (SCPs) ou políticas de controle de recursos (RCPs) em AWS Organizations. O status de um controle preventivo é aplicado ou não habilitado. Os controles preventivos são suportados em todos Regiões da AWS.
2. Os controles de detetive são projetados para detectar eventos específicos quando eles ocorrem e registrar a ação. AWS CloudTrail Eles são implementados com AWS Config regras. O status de um controle detectivo é limpo, em violação, ou não habilitado. Os controles de detetive se aplicam somente àqueles Regiões da AWS suportados pelo. AWS Control Tower
3. Os controles proativos examinam os recursos que seriam provisionados AWS CloudFormation e verificam se eles estão em conformidade com as políticas e os objetivos da sua empresa. Os recursos que não estão em conformidade não serão provisionados. Eles são implementados com AWS CloudFormation ganchos. O status de um controle proativo é PASS, FAIL ou SKIP.

A orientação de controle se refere à prática recomendada de como aplicar cada controle ao seu OUs. AWS Control Tower fornece três categorias de orientação: obrigatória, altamente recomendada

e eletiva. A orientação de um controle é independente do comportamento dele. Para obter mais informações, consulte Controle de comportamento e orientação.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código. O AWS CDK kit de ferramentas é a principal ferramenta para interagir com seu AWS CDK aplicativo.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo.
- AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.

Outras ferramentas

- cdk_nag é uma ferramenta de código aberto que usa uma combinação de pacotes de regras para verificar se os AWS CDK aplicativos estão aderindo às melhores práticas.
- O npm é um registro de software executado em um ambiente Node.js e usado para compartilhar ou emprestar pacotes e gerenciar a implantação de pacotes privados.
- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub Implantar AWS Control Tower controles usando o AWS CDK repositório. Você usa o arquivo cdk.json para interagir com o AWS CDK aplicativo e usa o arquivo package.json para instalar os pacotes npm.

Práticas recomendadas

- Siga o princípio do privilégio mínimo (documentação do IAM). O exemplo de política do IAM e da política de confiança fornecido nesse padrão inclui as permissões mínimas necessárias, e as AWS CDK pilhas criadas na conta de gerenciamento são restringidas por essas permissões.
- Siga as melhores práticas para AWS Control Tower administradores (AWS Control Tower documentação).
- Siga as melhores práticas para desenvolver e implantar a infraestrutura em nuvem com a AWS CDK (AWS CDK documentação).
- Ao inicializar o AWS CDK, personalize o modelo de bootstrap para definir as políticas e as contas confiáveis que devem ter a capacidade de ler e gravar em qualquer recurso na conta de gerenciamento. Para obter mais informações, consulte Como personalizar a inicialização.
- Use ferramentas de análise de código, como cfn_nag, para verificar os modelos gerados. CloudFormation A ferramenta cfn-nag procura padrões em CloudFormation modelos que possam indicar que a infraestrutura não é segura. Você também pode usar cdk-nag para verificar seus CloudFormation modelos usando o módulo cloudformation-include.

Épicos

Prepare-se para ativar os controles

Tarefa	Descrição	Habilidades necessárias
Crie o perfil do IAM na conta de gerenciamento.	1. Crie uma política do IAM na conta de gerenciamento com as permissões definidas na política do IAM na seção de Informações adicionais. Para obter instruções, consulte Como criar políticas do IAM na documentação do IAM. Anote o nome do recurso da Amazon (ARN) da política. Veja um exemplo de ARN a seguir.	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias

	`arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`
	2. Crie um perfil do IAM na conta de gerenciamento, anexe a política de permissão do IAM que você criou na etapa anterior e anexe a política de confiança personalizada à Política de confiança na seção Informações adicionais. Para instruções, consulte Como criar um perfil usando políticas de confiança na documentação do IAM. A seguir, um exemplo do ARN para o novo perfil.
	`arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:role/<ROLE-NAME>`	

Tarefa	Descrição	Habilidades necessárias
Bootstrap AWS CDK.	1. Na conta de gerenciamento, assuma uma função que tenha permissões para inicializar. AWS CDK 2. Insira o comando a seguir, substituindo o seguinte: • `<MANAGEMENT-ACCOUNT-ID>` é o ID da conta de gerenciamento da organização. • `<AWS-CONTROL-TOWER-REGION>` é o Região da AWS local onde AWS Control Tower é implantado. Para obter uma lista completa dos códigos de região, consulte Endpoints regionais na Referência AWS geral. • `<DEPLOYMENT-ACCOUNT-ID>` é o ID da conta de implantação. • `<DEPLOYMENT-ROLE-NAME>` é o nome do perfil do IAM que você está usando na conta de implantação. • `<POLICY-NAME>` é o nome da política que você criou na conta de gerenciamento.	DevOps engenheiro, AWS geral, Python

Tarefa	Descrição	Habilidades necessárias
	`$ npx cdk bootstrap aws://<MANAGEMENT-ACCOUNT-ID>/<AWS-CONTROL-TOWER-REGION> \ --trust arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-NAME> \ --cloudformation-execution-policies arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`	
Clonar o repositório.	Em um shell bash, insira o comando a seguir. Isso clona os AWS Control Tower controles Deploy usando o AWS CDK repositório de. GitHub `git clone https://github.com/aws-samples/aws-control-tower-controls-cdk.git`	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
Edite o arquivo AWS CDK de configuração.	1. No repositório clonado, abra o arquivo constants.py. 2. No parâmetro `ACCOUNT_ID`, insira o ID da sua conta de gerenciamento. 3. No `<AWS-CONTROL-TOWER-REGION>` parâmetro, insira o Região da AWS local onde AWS Control Tower está implantado. 4. No parâmetro `ROLE_ARN`, insira o ARN do perfil criado na conta de gerenciamento. 5. Abra Todos os identificadores globais na AWS Control Tower documentação. 6. Na lista formatada em JSON, localize o controle que você deseja implementar e copie seu identificador global (também conhecido como valor {CONTROL_CATALOG_OPAQUE_ID}). Por exemplo, o identificador global para o controle AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED é. `k4izcjxhu kijhajp6ks5mjxk`	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
	7. Na `GUARDRAILS_CONFIGURATION` seção, no `Enable-Control` parâmetro, insira o identificador global que você copiou. Insira o identificador entre aspas duplas e separe vários identificadores com vírgulas. 8. Na seção `GUARDRAILS_CONFIGURATION`, no parâmetro `OrganizationalUnitIds`, insira o ID da unidade organizacional em que você deseja ativar o controle, como `ou-1111-11111111`. Insira o ID entre aspas duplas e separe vários IDs com vírgulas. Para obter mais informações sobre como recuperar a OU IDs, consulte Visualizando os detalhes de uma OU. 9. Salve e feche o arquivo constants.py. Para obter um exemplo de um arquivo constants.py atualizado, consulte a seção Informações adicionais deste padrão.	

Habilitar controles conta de gerenciamento

Tarefa	Descrição	Habilidades necessárias
Assuma um perfil do IAM na conta de implantação.	Na conta de implantação, assuma a função do IAM que tem permissões para implantar as AWS CDK pilhas na conta de gerenciamento. Para obter mais informaçõ es sobre como assumir uma função do IAM no AWS CLI, consulte Usar uma função do IAM no AWS CLI.	DevOps engenheiro, General AWS

Ative o ambiente .	Se você estiver usando Linux ou macOS:
	1. Insira o seguinte comando para criar um ambiente virtual:
	`$ python3 -m venv .venv`
	2. Depois que o ambiente virtual for criado, digite o seguinte comando para ativá-lo.
	`$ source .venv/bin/activate`
	Ou, se você estiver usando o Windows:
		DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
	1. Insira o seguinte comando para ativar um ambiente virtual. `% .venv\Scripts\activate.bat`	
Instale as dependências.	Depois que o ambiente virtual for ativado, digite o seguinte comando para executar o script install_deps.sh Esse script instala as dependências necessárias. `$ ./scripts/install_deps.sh`	DevOps engenheiro, AWS geral, Python

Implante a pilha.	Insira os comandos a seguir para sintetizar e implantar a CloudFormation pilha.
	`$ npx cdk synth`
	`$ npx cdk deploy`
		DevOps engenheiro, AWS geral, Python

Recursos relacionados

AWS documentação

- Sobre controles (AWS Control Tower documentação)
- Biblioteca de controles (AWS Control Tower documentação)
- AWS CDK Comandos do kit de ferramentas (AWS CDK documentação)
- Implemente e gerencie AWS Control Tower controles usando o Terraform (orientação AWS prescritiva)

Outros recursos

- Python

Mais informações

Exemplo de arquivo constants.py

A seguir, um exemplo de um arquivo constants.py atualizado. Esse exemplo ativa o controle AWS-GR_DISALLOW_CROSS_REGION_NETWORKING (ID global:) e o controle AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED (ID global:). **dvuaav61i5cnfazfelmvn9m6k** 50z1ot237wl8u1lv5ufau6qqo Para obter uma lista de identificadores globais IDs, consulte Todos os identificadores globais na AWS Control Tower documentação.

```
ACCOUNT_ID = 111122223333
AWS_CONTROL_TOWER_REGION = us-east-2
ROLE_ARN = "arn:aws:iam::111122223333:role/CT-Controls-Role"
GUARDRAILS_CONFIGURATION = [
    {
        "Enable-Control": {
            "dvuaav61i5cnfazfelmvn9m6k": {  # AWS-GR_DISALLOW_CROSS_REGION_NETWORKING
                "Parameters": {
                    "ExemptedPrincipalArns": ["arn:aws:iam::111122223333:role/
RoleName"]
                },
                "Tags": [{"key": "Environment", "value": "Production"}]
            },
            ...
        },
        "OrganizationalUnitIds": ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        "Enable-Control": {
            "50z1ot237wl8u1lv5ufau6qqo",  # AWS-
GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
            ...
        },
        "OrganizationalUnitIds": ["ou-2222-22222222"...],
    },
]
```

Política do IAM

O exemplo de política a seguir permite as ações mínimas necessárias para ativar ou desativar AWS Control Tower os controles ao implantar AWS CDK pilhas de uma conta de implantação na conta de gerenciamento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy",
                "ssm:GetParameters"
            ],
            "Resource": "*"
        }
    ]
}
```

Política de confiança

A política de confiança personalizada a seguir permite que um perfil do IAM específico na conta de implantação assuma o perfil do IAM na conta de gerenciamento. Substitua o seguinte:

- `<DEPLOYMENT-ACCOUNT-ID>` é o ID da conta de implantação

- <DEPLOYMENT-ROLE-NAME> é o nome do perfil na conta de implantação que tem permissão para assumir a função na conta de gerenciamento

```
{
    “Version”: “2012-10-17”,
    “Statement”: [
        {
            “Effect”: “Allow”,
            “Principal”: {
                “AWS”: “arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-
NAME>”
            },
            “Action”: “sts:AssumeRole”,
            “Condition”: {}
        }
    ]
}
```

Implemente e gerencie AWS Control Tower controles usando o Terraform

Criado por Iker Reina Fuente (AWS) e Ivan Girardi (AWS)

Resumo

Esse padrão descreve como usar AWS Control Tower controles, HashiCorp Terraform e infraestrutura como código (IaC) para implementar e administrar controles de segurança preventivos, detectivos e proativos. Um controle (também conhecido como corrimão) é uma regra de alto nível que fornece governança contínua para seu ambiente geral. AWS Control Tower Por exemplo, você pode usar controles para exigir o registro em log Contas da AWS e, em seguida, configurar notificações automáticas caso ocorram eventos específicos relacionados à segurança.

AWS Control Tower ajuda você a implementar controles preventivos, detectivos e proativos que governam seus AWS recursos e monitoram a conformidade em vários. Contas da AWS Cada controle impõe uma única regra. Neste padrão, você usa um modelo de IaC fornecido para especificar quais controles você deseja implantar em seu ambiente.

AWS Control Tower os controles se aplicam a uma unidade organizacional (OU) inteira, e o controle afeta cada um Conta da AWS dentro da OU. Portanto, quando os usuários realizam qualquer ação em qualquer conta em sua zona de pouso, a ação está sujeita aos controles que governam a UO.

A implementação de AWS Control Tower controles ajuda a estabelecer uma base de segurança sólida para sua AWS landing zone. Ao usar esse padrão para implantar os controles como IaC por meio do Terraform, você pode padronizar os controles em sua zona de pouso e implantá-los e gerenciá-los com mais eficiência.

Para implantar AWS Control Tower controles como IaC, você também pode usar AWS Cloud Development Kit (AWS CDK) em vez do Terraform. Para obter mais informações, consulte Implantar e gerenciar AWS Control Tower controles usando AWS CDKAWS CloudFormation e.

Público-alvo

Esse padrão é recomendado para usuários com experiência com AWS Control Tower Terraform e. AWS Organizations

Pré-requisitos e limitações

Pré-requisitos

- Ativo Contas da AWS gerenciado como uma organização AWS Organizations e uma AWS Control Tower landing zone. Para obter instruções, consulte Introdução na AWS Control Tower documentação.
- AWS Command Line Interface (AWS CLI), instalado e configurado.
- Uma função AWS Identity and Access Management (IAM) na conta de gerenciamento que tem permissões para implantar esse padrão. Para obter mais informações sobre as permissões necessárias e um exemplo de política, consulte Permissões de privilégio mínimo para o perfil do IAM na seção Informações adicionais deste padrão.
- Permissões para assumir o perfil do IAM na conta de gerenciamento.
- CLI do Terraform, instalada (documentação do Terraform)
- Terraform AWS Provider, configurado (documentação do Terraform).
- Backend do Terraform, configurado (documentação do Terraform)

Limitações

- Para AWS Control Tower controles, esse padrão requer o uso de identificadores globais que estejam no seguinte formato:

```
arn:<PARTITION>:controlcatalog:::control/<CONTROL_CATALOG_OPAQUE_ID>
```

  As versões anteriores desse padrão usavam identificadores regionais que não são mais suportados. Recomendamos que você migre de identificadores regionais para identificadores globais. Os identificadores globais ajudam você a gerenciar controles e expandir o número de controles que você pode usar.

> **Note**
>
> Na maioria dos casos, o valor de `<PARTITION>` é `aws`.

Versões do produto

- AWS Control Tower versão 3.2 ou posterior
- Terraform versão 1.5 ou mais recente
- Terraform AWS Provider versão 4.67 ou posterior

Arquitetura

Esta seção fornece uma visão geral de alto nível dessa solução e da arquitetura estabelecida pelo código de exemplo. O diagrama a seguir mostra os controles implantados nas várias contas na UO.

AWS Control Tower os controles são categorizados de acordo com seu comportamento e orientação.

Há três tipos principais de comportamentos de controle:

1. Os controles preventivos são projetados para evitar que ações ocorram. Eles são implementados com políticas de controle de serviço (SCPs) ou políticas de controle de recursos (RCPs) em AWS Organizations. O status de um controle preventivo é aplicado ou não habilitado. Os controles preventivos são suportados em todos Regiões da AWS.
2. Os controles de detetive são projetados para detectar eventos específicos quando eles ocorrem e registrar a ação. AWS CloudTrail Eles são implementados com AWS Config regras. O status de um controle detectivo é limpo, em violação, ou não habilitado. Os controles de detetive se aplicam somente àqueles Regiões da AWS suportados pelo. AWS Control Tower
3. Os controles proativos examinam os recursos que seriam provisionados AWS CloudFormation e verificam se eles estão em conformidade com as políticas e os objetivos da sua empresa. Os recursos que não estão em conformidade não serão provisionados. Eles são implementados com AWS CloudFormation ganchos. O status de um controle proativo é PASS, FAIL ou SKIP.

A orientação de controle é a prática recomendada de como aplicar cada controle ao seu OUs. AWS Control Tower fornece três categorias de orientação: obrigatória, altamente recomendada e eletiva. A orientação de um controle é independente do comportamento dele. Para obter mais informações, consulte Controle de comportamento e orientação.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo.

- AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.

Outras ferramentas

- HashiCorp O Terraform é uma ferramenta de infraestrutura como código (IaC) que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.

Repositório de código

O código desse padrão está disponível no repositório GitHub Implantar e gerenciar AWS Control Tower controles usando o repositório Terraform.

Práticas recomendadas

- O perfil do IAM usado para implantar essa solução devem seguir o princípio do privilégio mínimo (documentação do IAM).
- Siga as melhores práticas para AWS Control Tower administradores (AWS Control Tower documentação).

Épicos

Habilitar controles conta de gerenciamento

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Em um shell bash, insira o comando a seguir. Isso clona os AWS Control Tower controles de implantação e gerenciamento usando o repositório Terraform de. GitHub	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/aws-samples/aws-control-tower-controls-terraform.git`	
Edite o arquivo de configuração do backend do Terraform.	1. No repositório clonado, abra o arquivo backend.tf. 2. Edite o arquivo para definir a configuração do backend do Terraform. A configuração que você define nesse arquivo depende do seu ambiente. Para obter mais informações, consulte Configuração de backend (documentação do Terraform). 3. Salve e feche o arquivo backend.tf.	DevOps engenheiro, Terraform

Tarefa	Descrição	Habilidades necessárias
Edite o arquivo de configuração de provedor do Terraform.	1. No repositório clonado, abra o arquivo provider.tf. 2. Edite o arquivo para definir a configuração do provedor do Terraform. Para obter mais informações, consulte Configuração de provedor (documentação do Terraform). Defina Região da AWS como a região em que a AWS Control Tower API está disponível. 3. Salve e feche o arquivo provider.tf.	DevOps engenheiro, Terraform

Tarefa	Descrição	Habilidades necessárias
Edite o arquivo de configuração.	1. No repositório clonado, abra o arquivo variables.tfvars. 2. Abra Todos os identificadores globais na AWS Control Tower documentação. 3. Na lista formatada em JSON, localize o controle que você deseja implementar e copie seu identificador global (também conhecido como valor {CONTROL_CATALOG_OPAQUE_ID}). Por exemplo, o identificador global para o controle AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED é. `k4izcjxhu kijhajp6ks5mjxk` 4. Na `controls` seção, no `control_names` parâmetro, insira o identificador global que você copiou. 5. Na seção `controls`, no parâmetro `organizational_unit_ids` , insira o ID da unidade organizacional em que você deseja ativar o controle, como `ou-1111-11111111` . Insira o ID entre aspas duplas e separe	DevOps engenheiro, AWS geral, Terraform

Tarefa	Descrição	Habilidades necessárias
	vários IDs com vírgulas. Para obter mais informaçõ es sobre como recuperar a OU IDs, consulte Visualiza ndo os detalhes de uma OU. 6. Salve e feche o arquivo variables.tfvars. Para obter um exemplo de um arquivo variables.tfvars atualizado, consulte a seção Informaçõ es adicionais deste padrão.	
Provisione o perfil do IAM na conta de gerenciamento.	Na conta de gerenciam ento, assuma o perfil do IAM que tem permissões para implantar o arquivo de configuração do Terraform . Para obter mais informaçõ es sobre as permissões necessárias e um exemplo de política, consulte Permissõe s de privilégio mínimo para o perfil do IAM na seção Informações adicionais. Para obter mais informações sobre como assumir uma função do IAM no AWS CLI, consulte Usar uma função do IAM no AWS CLI.	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias

Implantar o arquivo de configuração	1. Insira o seguinte comando para inicializar o Terraform.
	`$ terraform init -upgrade`
	2. Insira o comando a seguir para visualizar as alteraçõe s em comparação com o estado atual.
	`$ terraform plan -var-file="variabl es.tfvars"`
	3. Revise as alterações de configuração no plano do Terraform e confirme que você deseja implement ar essas alterações na organização.
	4. Insira o seguinte comando para implantar os recursos.
	`$ terraform apply -var-file="variabl es.tfvars"`
		DevOps engenheiro, AWS geral, Terraform

(Opcional) Desative os controles na conta AWS Control Tower de gerenciamento

Tarefa	Descrição	Habilidades necessárias
Execute o comando `destroy`.	Digite o comando a seguir para remover os recursos implantados por esse padrão.	DevOps engenheiro, AWS geral, Terraform

Tarefa	Descrição	Habilidades necessárias
	`$ terraform destroy -var-file="variables.tfvars"`	

Solução de problemas

Problema	Solução
Erro `Error: creating ControlTower Control ValidationException: Guardrail <control ID> is already enabled on organizational unit <OU ID>`	O controle que você está tentando ativar já está habilitado na OU de destino. Esse erro pode ocorrer se um usuário habilitar manualmente o controle por meio do AWS Management Console, por meio de AWS Control Tower ou por completo AWS Organizations. Para implantar o arquivo de configuração do Terraform, você pode usar uma das opções a seguir. Opção 1: atualize o arquivo de estado atual do Terraform Você pode importar o recurso para o arquivo de estado atual do Terraform. Quando você executar o comando `apply` novamente, o Terraform ignorará esse recurso. Faça o seguinte para importar o recurso para o estado atual do Terraform: 1. Na conta AWS Control Tower de gerenciamento, insira o seguinte comando para recuperar uma lista dos nomes de recursos da Amazon (ARNs) para o OUs, onde `<root-ID>` está a raiz da organização. Para obter mais informações sobre como

Problema	Solução

	recuperar esse ID, consulte Visualizar detalhes sobre a organização.
	
	`aws organizations list-organizational-units-for-parent --parent-id <root-ID>`
	
	2. Para cada OU retornada na etapa anterior, digite o comando a seguir, onde <OU-ARN> é o ARN da OU.
	
	`aws controltower list-enabled-controls --target-identifier <OU-ARN>`
	
	3. Copie ARNs e execute a importação do Terraform no módulo necessário para que ele seja incluído no estado do Terraform . Para obter instruções, consulte Importar (documentação do Terraform).
	4. Repita as etapas em Implantar a configuração na seção Épicos.
	
	Opção 2: desative o controle
	
	Se você estiver trabalhando em um ambiente que não seja de produção, poderá desativar o controle no console. Reative-o repetindo as etapas em Implantar a configuração na seção Epics. Essa abordagem não é recomendada para ambientes de produção porque há um período em que o controle será desativado. Se quiser usar essa opção em um ambiente de produção, você pode implementar controles temporários, como aplicar temporariamente um SCP em AWS Organizations.

Recursos relacionados

AWS documentação

- Sobre controles (AWS Control Tower documentação)
- Biblioteca de controles (AWS Control Tower documentação)
- Implemente e gerencie AWS Control Tower controles usando AWS CDK e AWS CloudFormation (AWS orientação prescritiva)

Outros recursos

- Terraforma
- Documentação da CLI do Terraform

Mais informações

Exemplo de arquivo variables.tfvars

Veja a seguir um exemplo de um arquivo variables.tfvars atualizado. Esse exemplo ativa o controle AWS-GR_ENCRYPTED_VOLUMES (ID global:) e o controle AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED (ID global:`503uicglhjkokaajywfpt6ros`). `50z1ot237wl8u1lv5ufau6qqo` Para obter uma lista de identificadores globais IDs, consulte Todos os identificadores globais na AWS Control Tower documentação.

O exemplo a seguir também ativa controles que têm parâmetros como CT.S3.PV.5 (ID global:**`7mo7a2h2ebsq71l8k6uzr96ou`**) e CT.SECRETSMANAGER.PV.1 (ID global:). `dvhe47fxg5o6lryqrq9g6sxg4` Para obter uma lista de controles com parâmetros, consulte Controles com parâmetros na AWS Control Tower documentação.

```
controls = [
    {
        control_names = [
            "503uicglhjkokaajywfpt6ros", # AWS-GR_ENCRYPTED_VOLUMES
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
```

```
        control_names = [
            "50z1ot237wl8u1lv5ufau6qqo", # AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111"...],
    },
]

controls_with_params = [
  {
    control_names = [
      { "7mo7a2h2ebsq71l8k6uzr96ou" = { # CT.S3.PV.5
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
          "ExemptedResourceArns" : [],
        }
      } },
      { "dvhe47fxg5o6lryqrq9g6sxg4" = { # CT.SECRETSMANAGER.PV.1
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      ...
    ],
    organizational_unit_ids = ["ou-1111-11111111"...]
  },
  {
    control_names = [
      { "dvuaav61i5cnfazfelmvn9m6k" = { # AWS-GR_DISALLOW_CROSS_REGION_NETWORKING
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      { "41ngl8m5c4eb1myoz0t707n7h" = { # AWS-GR_DISALLOW_VPC_INTERNET_ACCESS
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      ...
    ],
    organizational_unit_ids = ["ou-2222-22222222"...]
  }
]
```

Permissões de privilégio mínimo para o perfil do IAM

Esse padrão exige que você assuma uma função do IAM na conta de gerenciamento. A melhor prática é assumir um perfil com permissões temporárias e limitar as permissões de acordo com o princípio do privilégio mínimo. O exemplo de política a seguir permite as ações mínimas necessárias para ativar ou desativar AWS Control Tower os controles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Implemente um pipeline que detecte simultaneamente problemas de segurança em vários produtos de código

Criado por Benjamin Morris (AWS), Dina Odum (AWS), Isaiah Schisler (AWS), Sapeksh Madan (AWS) e Tim Hahn (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais.

O Simple Code Scanning Pipeline (SCSP) fornece a criação em dois cliques de um pipeline de análise de código que executa ferramentas de segurança de código aberto padrão do setor em paralelo. Isso permite que os desenvolvedores verifiquem a qualidade e a segurança de seu código sem precisar instalar ferramentas ou mesmo entender como executá-las. Isso ajuda a reduzir vulnerabilidades e configurações incorretas nos resultados do código. Também reduz a quantidade de tempo que sua organização gasta instalando, pesquisando e configurando ferramentas de segurança.

Antes do SCSP, a digitalização do código usando esse conjunto específico de ferramentas exigia que os desenvolvedores localizassem, instalassem e configurassem manualmente as ferramentas de análise de software. Mesmo instaladas localmente, all-in-one ferramentas, como o Automated Security Helper (ASH), exigem a configuração de um contêiner Docker para serem executadas. No entanto, com o SCSP, um conjunto de ferramentas de análise de código padrão do setor é executado automaticamente no. Nuvem AWS Com essa solução, você usa o Git para enviar seus resultados de código e, em seguida, recebe uma saída visual com at-a-glance informações sobre as falhas nas verificações de segurança.

Pré-requisitos e limitações

- Um ativo Conta da AWS
- Um ou mais resultados de código que você deseja verificar em busca de problemas de segurança
- AWS Command Line Interface (AWS CLI), instalado e configurado
- Python versão 3.0 ou posterior e pip versão 9.0.3 ou posterior, instalados
- Git, instalado
- Instale git-remote-codecommitem sua estação de trabalho local

Arquitetura

Pilha de tecnologias de destino

- AWS CodeCommit repositório
- AWS CodeBuild projeto
- AWS CodePipeline encanamento
- Bucket do Amazon Simple Storage Service (Amazon S3)
- AWS CloudFormation modelo

Arquitetura de destino

O SCSP para análise estática de código é um DevOps projeto desenvolvido para fornecer feedback de segurança sobre o código entregue.

1. No AWS Management Console, faça login no alvo Conta da AWS. Confirme se você está no Região da AWS local em que deseja implantar o pipeline.
2. Use o CloudFormation modelo no repositório de código para implantar a pilha SCSP. Isso cria um novo CodeCommit repositório e CodeBuild projeto.

   > **Note**
   >
   > Como opção alternativa de implantação, você pode usar um CodeCommit repositório existente fornecendo o Amazon Resource Name (ARN) do repositório como parâmetro durante a implantação da pilha.

3. Clone o repositório na sua estação de trabalho local e, em seguida, adicione todos os arquivos às respectivas pastas no repositório clonado.
4. Use o Git para adicionar, confirmar e enviar os arquivos para o CodeCommit repositório.
5. Enviar para o CodeCommit repositório inicia um trabalho. CodeBuild O CodeBuild projeto usa as ferramentas de segurança para escanear os resultados do código.
6. Revise a saída do pipeline. As ferramentas de segurança que detectaram problemas de nível de erro resultarão em ações malsucedidas no pipeline. Corrija esses erros ou os suprima como falsos positivos. Analise os detalhes da saída da ferramenta nos detalhes da ação no bucket S3 do pipeline CodePipeline ou no repositório S3.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodeCommité um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.

Outras ferramentas

Para obter uma lista completa das ferramentas que o SCSP usa para escanear os resultados do código, consulte o arquivo readme do SCSP em. GitHub

Repositório de código

O código desse padrão está disponível no repositório Simple Code Scanning Pipeline (SCSP) em. GitHub

Épicos

Implemente o SCSP

Tarefa	Descrição	Habilidades necessárias
Crie a CloudFormation pilha.	1. Faça login no AWS Management Console. 2. No console, confirme que você está na região de destino em que deseja implantar a solução. Para obter mais informaçõ es, consulte Choosing a Region.	AWS DevOps, administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	3. Escolha o link a seguir. Isso abre o assistente de criação rápida de pilha em CloudFormation. https://console.aws.amazon.com/cloudformation/casa? #/ stacks/create/review?templateURL=https://proservetools.s3.amazonaws.com/cft/scsp -Pipeline-stack.template.json&StackName = SimpleCodeScanPipeline 4. No assistente de criação rápida de pilha, revise as configurações de parâmetros da sua pilha e faça as modificações necessárias para seu caso de uso. 5. Selecione Eu reconheço que a AWS CloudFormation pode criar recursos do IAM e, em seguida, escolha Create stack. Isso cria um CodeCommit repositório, um CodePipeline pipeline, várias definições de CodeBuild tarefas e um bucket S3. As execuções de compilação e os resultados da verificação são copiados para esse bucket. Depois que	

Tarefa	Descrição	Habilidades necessárias
	a CloudFormation pilha for completamente implantada, o SCSP estará pronto para uso.	

Use o pipeline

Tarefa	Descrição	Habilidades necessárias
Examine os resultados da verificação.	1. No console do Amazon S3, em Buckets, escolha o bucket simplecoscanpipeline-deleteresourcespipelineresso. 2. Escolha o diretório scan_results e, em seguida, escolha a pasta com o carimbo de data da verificação mais recente. 3. Examine os arquivos de log nessa pasta para analisar quaisquer problemas detectados pelas ferramentas de segurança usadas no pipeline. As ferramentas de segurança que detectarem problemas de nível de erro resultarão em `failed` ações em andamento. Eles precisam ser corrigidos ou suprimidos se forem falsos positivos.	Desenvolvedor de aplicativos, AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	Note Você também pode ver detalhes da saída da ferramenta (para digitalizações aprovadas e reprovadas) no CodePipeline console, na seção Detalhes da ação.	

Solução de problemas

Problema	Solução
HashiCorp O Terraform ou AWS CloudFormation os arquivos não estão sendo escaneados.	Certifique-se de que os arquivos do Terraform (.tf) e CloudFormation (.yml, .yaml ou .json) sejam colocados nas pastas apropriadas no repositório clonado. CodeCommit
O `git clone` comando está falhando.	Verifique se você instalou `git-remote-codecommit` e se sua CLI tem acesso às AWS credenciais que têm permissões para ler o repositório. CodeCommit
Um erro de simultaneidade, como`Project-level concurrent build limit cannot exceed the account-level concurrent build limit of 1 .`	Execute novamente o pipeline escolhendo o botão Release Change no CodePipeline console. Esse é um problema conhecido que parece ser mais comum nas primeiras vezes em que o pipeline é executado.

Recursos relacionados

Forneça feedback sobre o projeto SCSP.

Mais informações

PERGUNTAS FREQUENTES

O projeto SCSP é o mesmo que o Automated Security Helper (ASH)?

Não. Use ASH quando quiser uma ferramenta CLI que execute ferramentas de varredura de código usando contêineres. O Automated Security Helper (ASH) é uma ferramenta projetada para reduzir a probabilidade de uma violação de segurança em um novo código, infraestrutura ou configuração de recursos do IAM. ASH é um utilitário de linha de comando que pode ser executado localmente. O uso local exige que um ambiente de contêiner esteja instalado e operacional no sistema.

Use o SCSP quando quiser um pipeline de configuração mais fácil do que o ASH. O SCSP não requer instalações locais. O SCSP foi projetado para executar verificações individualmente em um pipeline e exibir os resultados por ferramenta. O SCSP também evita grande parte da sobrecarga com a configuração do Docker e é independente do sistema operacional (SO).

O SCSP é apenas para equipes de segurança?

Não, qualquer pessoa pode implantar o pipeline para determinar quais partes do código estão falhando nas verificações de segurança. Por exemplo, usuários que não são de segurança podem usar o SCSP para verificar seu código antes de revisar com suas equipes de segurança.

Posso usar o SCSP se estiver trabalhando com outro tipo de repositório, como GitLab GitHub, ou Bitbucket?

Você pode configurar um repositório git local para apontar para dois repositórios remotos diferentes. Por exemplo, você pode clonar um GitLab repositório existente, criar uma instância SCSP (especificando CloudFormation as pastas Terraform e AWS Config Rules Development Kit (AWS RDK), se necessário) e, em seguida, usar `git remote add upstream <SCSPGitLink>` para apontar o repositório local para o repositório SCSP também. CodeCommit Isso permite que as alterações de código sejam enviadas primeiro para o SCSP, validadas e, depois que quaisquer atualizações adicionais forem feitas para abordar as descobertas, enviadas para o repositório GitLab GitHub, ou Bitbucket. Para obter mais informações sobre vários controles remotos, consulte Enviar confirmações para um repositório Git adicional (postagem no blog).AWS

> **Note**
>
> Tenha cuidado com desvios, como evitar fazer alterações por meio de interfaces da web.

Contribuindo e adicionando suas próprias ações

A configuração do SCSP é mantida como um GitHub projeto, que contém o código-fonte do aplicativo SCSP AWS Cloud Development Kit (AWS CDK) . Para adicionar verificações adicionais ao pipeline, o AWS CDK aplicativo precisa ser atualizado e, em seguida, sintetizado ou implantado no destino em Conta da AWS que o pipeline será executado. Para fazer isso, comece clonando o GitHub projeto SCSP e, em seguida, localize o arquivo de definição da pilha na pasta. `lib`

Se houver uma verificação adicional que você gostaria de adicionar, a `StandardizedCodeBuildProject` classe no AWS CDK código facilita muito a adição de ações. Forneça o nome, a descrição `install` e/ou `build` os comandos. AWS CDK cria o CodeBuild projeto usando valores padrão sensatos. Além de criar o projeto de construção, você precisa adicioná-lo às CodePipeline ações no estágio de construção. Ao criar uma nova verificação, a ação deve ser tomada `FAIL` se a ferramenta de verificação detectar problemas ou falhar na execução. A ação deve ser tomada `PASS` se a ferramenta de digitalização não detectar nenhum problema. Para ver um exemplo de configuração de uma ferramenta, revise o código da `Bandit` ação.

Para obter mais informações sobre entradas e saídas esperadas, consulte a documentação do repositório.

Se você adicionar ações personalizadas, precisará implantar o SCSP usando `cdk deploy` ou`cdk synth + CloudFormation deploy`. Isso ocorre porque o CloudFormation modelo de pilha de criação rápida é mantido pelos proprietários do repositório.

Implemente controles de acesso baseados em atributos de detetive para sub-redes públicas usando AWS Config

Criado por Alberto Menendez (AWS)

Resumo

As arquiteturas de rede de borda distribuída dependem da segurança de borda da rede que funciona junto com as cargas de trabalho em suas nuvens privadas virtuais ()VPCs. Isso fornece escalabilidade sem precedentes em comparação com a abordagem centralizada mais comum. Embora a implantação de sub-redes públicas em contas de workload possa oferecer benefícios, ela também introduz novos riscos de segurança, pois aumenta a superfície de ataque. Recomendamos que você implante somente recursos do Elastic Load Balancing, como Application Load Balancers ou gateways NAT nas sub-redes públicas desses. VPCs O uso de balanceadores de carga e gateways NAT em sub-redes públicas dedicadas ajuda a implementar um controle refinado do tráfego de entrada e saída.

Recomendamos que você implemente controles preventivos e de detetive para limitar os tipos de recursos que podem ser implantados em sub-redes públicas. Para obter mais informações sobre o uso do controle de acesso baseado em atributos (ABAC) para implantar controles preventivos para sub-redes públicas, consulte Implantar controles de acesso preventivos baseados em atributos para sub-redes públicas. Embora sejam eficazes na maioria das situações, esses controles preventivos podem não abordar todos os casos de uso possíveis. Portanto, esse padrão se baseia na abordagem ABAC e ajuda a configurar alertas sobre recursos não compatíveis que são implantados em sub-redes públicas. A solução verifica se as interfaces de rede elástica pertencem a um recurso que não é permitido em sub-redes públicas.

Para conseguir isso, esse padrão usa regras AWS Config personalizadas e ABAC. A regra personalizada processa a configuração de uma interface de rede elástica sempre que ela é criada ou modificada. Em um alto nível, essa regra executa duas ações para determinar se a interface de rede é compatível:

1. Para determinar se a interface de rede está no escopo da regra, a regra verifica se a sub-rede tem AWS tags específicas que indicam que é uma sub-rede pública. Por exemplo, essa tag pode ser`IsPublicFacing=True`.
2. Se a interface de rede for implantada em uma sub-rede pública, a regra verificará quem AWS service (Serviço da AWS) criou esse recurso. Se o recurso não for um recurso do Elastic Load Balancing ou um gateway NAT, ele marcará o recurso como não compatível.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- AWS Config, configurado na conta de carga de trabalho
- Permissões para implantar os recursos necessários na conta de carga de trabalho
- Uma VPC com sub-redes públicas
- Tags aplicadas corretamente para identificar as sub-redes públicas de destino
- (Opcional) Uma organização em AWS Organizations
- (Opcional) Uma conta de segurança central que é o administrador delegado de AWS Config e AWS Security Hub

Arquitetura

Arquitetura de destino

O diagrama ilustra o seguinte:

1. Quando um recurso de interface de elastic network (`AWS::EC2::NetworkInterface`) é implantado ou modificado, AWS Config captura o evento e a configuração.
2. AWS Config compara esse evento com a regra personalizada usada para avaliar a configuração.
3. A AWS Lambda função associada a essa regra personalizada é invocada. A função avalia o recurso e aplica a lógica especificada para determinar se a configuração do recurso é `COMPLIANT` `NON_COMPLIANT` ou`NOT_APPLICABLE`.
4. Se for determinado que um recurso é`NON_COMPLIANT`, AWS Config envia um alerta por meio do Amazon Simple Notification Service (Amazon SNS).

> **Note**
>
> Se essa conta for uma conta de membro em AWS Organizations, você poderá enviar dados de conformidade para uma conta de segurança central por meio de AWS Config ou AWS Security Hub.

Lógica de avaliação da função Lambda

O diagrama a seguir mostra a lógica aplicada pela função Lambda para avaliar a conformidade da interface de rede elástica.

Automação e escala

Esse padrão é uma solução de detetive. Você também pode complementá-lo com uma regra de remediação para resolver automaticamente quaisquer recursos não compatíveis. Para obter mais informações, consulte Correção de recursos não compatíveis com regras. AWS Config

Você pode escalar essa solução da seguinte forma:

- Impondo a aplicação das AWS tags correspondentes que você estabelece para identificar sub-redes voltadas para o público. Para obter mais informações, consulte Políticas de tags na AWS Organizations documentação.
- Configurar uma conta de segurança central que aplique a regra AWS Config personalizada a cada conta de carga de trabalho na organização. Para obter mais informações, consulte Automatizar a conformidade da configuração em grande escala AWS (postagem no AWS blog).
- Integração AWS Config com AWS Security Hub para capturar, centralizar e notificar em grande escala. Para obter mais informações, consulte Configuração AWS Config na AWS Security Hub documentação.

Ferramentas

- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo.
- O Elastic Load Balancing (ELB) distribui o tráfego de entrada de aplicativos ou de rede em vários destinos. Por exemplo, você pode distribuir o tráfego entre instâncias, contêineres e endereços IP do Amazon Elastic Compute Cloud (Amazon EC2) em uma ou mais zonas de disponibilidade.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Práticas recomendadas

Para obter mais exemplos e melhores práticas para o desenvolvimento de AWS Config regras personalizadas, consulte o Repositório de AWS Config Regras oficial em GitHub.

Épicos

Implante a solução

Tarefa	Descrição	Habilidades necessárias
Criar a função do Lambda.	1. Faça login no e AWS Management Console, em seguida, abra o AWS Lambda console. 2. Na página Functions (Funções), escolha Create function (Criar função). 3. Selecione Criar do zero. 4. No painel Informações básicas, em Nome da função, insira um nome. 5. Em Runtime, selecione Python 3.12. 6. Deixe a arquitetura definida como x86_64. 7. Escolha a opção Criar função. 8. Escolha a guia Código.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	9. No explorador de arquivos, escolha lambda_function.py. 10. Cole o código de amostra fornecido na seção Informações adicionais desse padrão na guia lambda_function.py. Personalize o código de amostra para identificar qualquer lógica de avaliação personalizada na `evaluate_change_notification_compliance` função. 11. Escolha Implantar.	

Tarefa	Descrição	Habilidades necessárias
Adicione permissões à função de execução da função Lambda.	1. Selecione Funções no painel de navegação. 2. Escolha a função que você acabou de criar. 3. Escolha Configuration (Configuração) e depois Permissions (Permissões). 4. Escolha o nome da função para abrir a função no console AWS Identity and Access Management (IAM). 5. Em Políticas de permissões, escolha Adicionar permissões e, em seguida, escolha Criar política embutida. 6. Escolha JSON. 7. Cole a política a seguir no editor de políticas. Isso permite que a função Lambda: • Veja os detalhes das tags de sub-rede. • Envie o resultado da conformidade de volta para AWS Config. `{ "Version": "2012-10-17", "Statement": [ {`	AWS geral

Tarefa	Descrição	Habilidades necessárias
	<pre>"Action": ["config:PutEvaluations", "ec2:DescribeSubnets"], "Resource": "*", "Effect": "Allow" }] }</pre> 8. Escolha Próximo. 9. Insira um nome para a política e escolha Create policy (Criar política).	
Recupere a função Lambda Amazon Resource Name (ARN).	1. Abra o console do lambda. 2. Selecione Funções no painel de navegação. 3. Escolha a função que você acabou de criar. 4. Na seção Visão geral da função, em ARN da função, copie o valor.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Crie a regra AWS Config personalizada.	1. Abra o console de AWS Config. 2. Na página Rules (Regras), selecione Add rule (Adicionar regra). 3. Na página Especificar tipo de regra, escolha Criar regra personalizada do Lambda e, em seguida, escolha Avançar. 4. Na página Configurar regra, faça o seguinte: a. Insira um nome e uma descrição. b. Para a AWS Lambda função ARN, cole o ARN que você copiou anteriormente. c. Para Tipo de gatilho, escolha Quando a configuração muda. d. Em Escopo das alterações, selecione Recursos. e. Em Tipo de recurso, escolha AWS EC2 NetworkInterface. f. Escolha Próximo. 5. Na página Revisar e criar, verifique sua regra e escolha Salvar.	AWS geral

Tarefa	Descrição	Habilidades necessárias
Configure as notificações.	1. Siga as instruções em Criação de um tópico do Amazon SNS para criar um tópico do Amazon SNS. 2. Siga as instruções em Assinatura de um tópico do Amazon SNS para configurar um endpoint que receba notificações para o tópico do Amazon SNS. 3. Siga as instruções em Como posso ser notificado quando um AWS recurso não está em conformidade usando AWS Config para configurar uma EventBridge regra personalizada da Amazon para seus recursos não compatíveis.	AWS geral

Testar a solução

Tarefa	Descrição	Habilidades necessárias
Crie um recurso compatível.	1. Use as instruções a seguir para criar um dos recursos compatíveis em uma sub-rede pública: • Crie um gateway NAT • Conceitos básicos de Network Load Balancers • Criar um Application Load Balancer	AWS geral

Tarefa	Descrição	Habilidades necessárias
	2. Depois que o recurso é criado, a regra AWS Config personalizada avalia as interfaces de rede elástica associadas ao recurso. Ele marca essas interfaces de rede como `COMPLIANT`. Você pode visualizar os recursos em AWS Config seguindo estas etapas: a. Abra o console de AWS Config. b. Na página Regras, escolha sua regra. c. Na página de detalhes da regra, vá até a parte inferior da página. d. Em Recursos no escopo, selecione Compatível. Confirme se você vê as interfaces IDs de rede que foram criadas. e. Para obter mais detalhes sobre a configuração da interface de rede, escolha a ID do recurso.	

Tarefa	Descrição	Habilidades necessárias
Crie um recurso não compatível.	1. Use as instruções a seguir para criar um recurso não compatível em uma sub-rede pública: • Inicie uma EC2 instância da Amazon • Criação de uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS) • Crie um VPC endpoint 2. Depois que o recurso é criado, a regra AWS Config personalizada avalia as interfaces de rede elástica associadas ao recurso. Ele marca essas interfaces de rede como `NON_COMPLIANT` . Você pode visualizar os recursos em AWS Config seguindo estas etapas: a. Abra o console de AWS Config. b. Na página Regras, escolha sua regra. c. Na página de detalhes da regra, vá até a parte inferior da página. d. Em Recursos no escopo, selecione NonCompliant. Confirme se você vê as	AWS geral

Tarefa	Descrição	Habilidades necessárias
	interfaces IDs de rede que foram criadas. e. Para obter mais detalhes sobre a configuração da interface de rede, escolha a ID do recurso. 3. Confirme se você recebeu a notificação no endpoint que você configurou no Amazon SNS.	
Crie um recurso que não seja aplicável.	1. Em uma sub-rede privada, crie qualquer recurso que exija uma interface de rede elástica. 2. Depois que o recurso é criado, a regra AWS Config personalizada avalia as interfaces de rede elástica associadas ao recurso. Ele marca essas interfaces de rede como `NOT_APPLICABLE`. Esses recursos não são mostrados no AWS Config console.	AWS geral

Recursos relacionados

AWS documentação

- Configuração AWS Config
- AWS Config regras personalizadas
- ABAC para AWS
- Implemente controles de acesso preventivos baseados em atributos para sub-redes públicas

Outros AWS recursos

- Automatize a conformidade da configuração em grande escala em AWS
- Arquiteturas de inspeção distribuídas com Gateway Load Balancer

Mais informações

Veja a seguir uma amostra da função Lambda fornecida para fins de demonstração.

```
import boto3
import json
import os

# Init clients
config_client = boto3.client('config')
ec2_client = boto3.client('ec2')

def lambda_handler(event, context):

    # Init values
    compliance_value = 'NOT_APPLICABLE'
    invoking_event = json.loads(event['invokingEvent'])
    configuration_item = invoking_event['configurationItem']

    status = configuration_item['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']

    # First check if the event configuration applies. Ex. resource event is not delete
    if (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope:
        compliance_value = evaluate_change_notification_compliance(configuration_item)


    config_client.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
```

```
            },
        ],
        ResultToken=event['resultToken'])

# Function with the logs to evaluate the resource
def evaluate_change_notification_compliance(configuration_item):
    is_in_scope = is_in_scope_subnet(configuration_item['configuration']['subnetId'])

    if (configuration_item['resourceType'] != 'AWS::EC2::NetworkInterface') or not
 is_in_scope:
        return 'NOT_APPLICABLE'

    else:
        alb_condition = configuration_item['configuration']['requesterId'] in ['amazon-
elb']
        nlb_condition = configuration_item['configuration']['interfaceType'] in
 ['network_load_balancer']
        nat_gateway_condition = configuration_item['configuration']['interfaceType'] in
 ['nat_gateway']

        if alb_condition or nlb_condition or nat_gateway_condition:
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

# Function to check if elastic network interface is in public subnet
def is_in_scope_subnet(eni_subnet):

    subnet_description = ec2_client.describe_subnets(
        SubnetIds=[eni_subnet]
    )

    for subnet in subnet_description['Subnets']:
        for tag in subnet['Tags']:
            if tag['Key'] == os.environ.get('TAG_KEY') and tag['Value'] ==
 os.environ.get('TAG_VALUE'):
                return True

    return False
```

Implemente controles de acesso preventivos baseados em atributos para sub-redes públicas

Criado por Joel Alfredo Nunez Gonzalez (AWS) e Samuel Ortega Sancho (AWS)

Resumo

Em arquiteturas de rede centralizadas, a inspeção e as nuvens privadas virtuais de borda (VPCs) concentram todo o tráfego de entrada e saída, como o tráfego de e para a Internet. No entanto, isso pode criar gargalos ou fazer com que os limites das Service Quotas da AWS sejam atingidos. A implantação da segurança de ponta da rede junto com as cargas de trabalho VPCs fornece uma escalabilidade sem precedentes em comparação com a abordagem centralizada mais comum. Isso é chamado de arquitetura de borda distribuída.

Embora a implantação de sub-redes públicas em contas de workload possa oferecer benefícios, ela também introduz novos riscos de segurança, pois aumenta a superfície de ataque. Recomendamos que você implante somente recursos do Elastic Load Balancing (ELB), como Application Load Balancers ou gateways NAT nas sub-redes públicas desses. VPCs O uso de balanceadores de carga e gateways NAT em sub-redes públicas dedicadas ajuda a implementar um controle refinado do tráfego de entrada e saída.

O controle de acesso por atributo (ABAC) é a prática de criar permissões minuciosas com base nos atributos do usuário, como departamento, cargo e nome da equipe. Para obter mais informações, consulte ABAC para a AWS. O ABAC pode fornecer barreiras de proteção para sub-redes públicas em contas de workload. Isso ajuda as equipes de aplicativos a serem ágeis, sem comprometer a segurança da infraestrutura.

Esse padrão descreve como ajudar a proteger sub-redes públicas implementando o ABAC por meio de uma política de controle de serviços (SCP) no AWS Organizations e políticas no AWS Identity and Access Management (IAM). É possível aplicar o SCP a uma conta membro de uma organização ou a uma unidade organizacional (UO). Essas políticas ABAC permitem que os usuários implantem gateways NAT nas sub-redes de destino e os impeçam de implantar outros recursos do Amazon Elastic Compute Cloud (Amazon EC2), como instâncias e interfaces de rede elástica. EC2

Pré-requisitos e limitações

Pré-requisitos

- Uma organização no AWS Organizations

- Acesso administrativo à conta raiz do AWS Organizations
- Na organização, uma conta de membro ativa ou OU para testar o SCP

Limitações

- O SCP nessa solução não impede que os serviços da AWS que usam um perfil vinculada a serviços implantem recursos nas sub-redes de destino. Exemplos desses serviços são Elastic Load Balancing (ELB), Amazon Elastic Container Service (Amazon ECS) e Amazon Relational Database Service (Amazon RDS). Para obter mais informações, consulte Efeitos do SCP sobre permissões na documentação do AWS Organizations. Implemente controles de segurança para detectar essas exceções.

Arquitetura

Pilha de tecnologias de destino

- SCP aplicado a uma conta da AWS ou OU no AWS Organizations
- Os seguintes perfis do IAM:
  - `AutomationAdminRole`: usado para modificar tags de sub-rede e criar recursos de VPC após a implementação do SCP
  - `TestAdminRole`: usado para testar se o SCP está impedindo que outras entidades principais do IAM, incluindo aqueles com acesso administrativo, executem as ações reservadas para o `AutomationAdminRole`

Arquitetura de destino

1. Você cria o perfil do IAM `AutomationAdminRole` na conta de destino. Esse perfil tem permissões para gerenciar recursos de rede. Observe as seguintes permissões que são exclusivas para esse perfil:
   - Essa função pode criar VPCs e publicar sub-redes.
   - Esse perfil pode modificar as atribuições de tags para as sub-redes de destino.
   - Esse perfil pode gerenciar suas próprias permissões.
2. No AWS Organizations, você aplica o SCP à conta ou OU da AWS de destino. Para ver um exemplo de política, consulte Informações adicionais sobre esse padrão.

3. Um usuário ou uma ferramenta no pipeline de CI/CD pode assumir a função `AutomationAdminRole` de aplicar a tag `SubnetType` às sub-redes de destino.
4. Ao assumir outros perfis do IAM, os diretores autorizados do IAM em sua organização podem gerenciar gateways NAT nas sub-redes de destino e outros recursos de rede permitidos na conta da AWS, como tabelas de rotas. Você pode usar políticas do IAM para conceder permissões. Para obter mais informações, consulte Gerenciamento de identidade e acesso do Amazon VPC.

Automação e escala

Para ajudar a proteger as sub-redes públicas, as respectivas tags da AWS devem ser aplicadas. Depois de aplicar o SCP, os gateways NAT são o único tipo de EC2 recurso da Amazon que usuários autorizados podem criar em sub-redes que têm a tag. `SubnetType:IFA` (`IFA`significa ativos voltados para a Internet.) O SCP impede a criação de outros EC2 recursos da Amazon, como instâncias e interfaces de rede elásticas. Recomendamos que você use um pipeline de CI/CD que assuma a `AutomationAdminRole` função de criar recursos de VPC para que essas tags sejam aplicadas adequadamente às sub-redes públicas.

Ferramentas

Serviços da AWS

- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Organizations é um serviço de gerenciamento de contas que ajuda você a consolidar várias contas AWS em uma organização que você cria e gerencia de maneira centralizada. No AWS Organizations, você pode implementar políticas de controle de serviços (SCPs), que são um tipo de política que você pode usar para gerenciar permissões na sua organização.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda a iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Épicos

Aplique o SCP

Tarefa	Descrição	Habilidades necessárias
Crie um perfil de administrador de teste.	Na conta AWS de destino, crie um perfil do IAM chamado `TestAdminRole` . Anexe a política de IAM gerenciada pela AdministratorAccessAWS à nova função. Para obter instruções, consulte Criar um perfil para delegar permissões a um usuário do IAM na documentação do IAM.	Administrador da AWS
Crie o perfil de administrador de automação.	1. Na conta AWS de destino, crie um perfil do IAM chamado `AutomationAdminRole` . 2. Anexe a política de IAM gerenciada pela AdministratorAccessAWS à nova função. Veja a seguir um exemplo de política de confiança que você poderia usar para testar a função da conta `000000000000` . `{ "Version": "2012-10-17", "Statement": [ {`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	"Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::000000000000:root"] }, "Action": "sts:AssumeRole", "Condition": {} }] }	
Crie e anexe o SCP.	1. Ao usar o código de exemplo fornecido na seção Informações adicionais, crie uma política de controle de segurança. Para obter instruções, consulte Como criar um SCP na documentação do AWS Organizations. 2. Anexe o SCP à conta ou OU da AWS de destino. Para obter instruções, consulte Anexar e desanexar políticas de controle de serviços na documentação do AWS Organizations.	Administrador da AWS

Teste o SCP

Tarefa	Descrição	Habilidades necessárias
Crie uma VPC ou sub-rede.	1. Assuma o perfil `TestAdminRole` na conta de destino da AWS. 2. Tente criar uma VPC ou uma nova sub-rede pública em uma VPC existente. Para obter instruções, consulte Criar uma VPC, sub-redes e outros recursos de VPC na documentação da VPC da Amazon VPC. Você não deveria ser capaz de criar esses recursos. 3. Assuma o perfil `AutomationAdminRole` e repita a etapa anterior. Agora você deveria poder criar recursos de rede.	Administrador da AWS
Gerenciar tags.	1. Assuma o perfil `TestAdminRole` na conta de destino da AWS. 2. Adicione uma tag `SubnetType:IFA` a uma sub-rede pública disponível. Você deve ser capaz de adicionar essa tag. Para obter instruções sobre como adicionar tags por meio da AWS Command Line Interface (AWS CLI), consulte create-tags	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	na AWS CLI Command Reference. 3. Sem alterar suas credencia is, tente modificar a tag `SubnetType:IFA` atribuída a essa sub-rede. Você não deve conseguir modificar essa tag. 4. Assuma o perfil `AutomationAdminRol e` e repita as etapas anteriores. Essa função deve ser capaz de adicionar e modificar essa tag.	

Tarefa	Descrição	Habilidades necessárias
Implante recursos nas sub-redes de destino.	1. Assumir a função `TestAdminRole` . 2. Para uma sub-rede pública que tenha a `SubnetType:IFA` tag, tente criar uma EC2 instância. Para obter instruções, consulte Iniciar uma instância na EC2 documentação da Amazon. Nessa sub-rede, você não deve ser capaz de criar, modificar ou excluir nenhum EC2 recurso da Amazon, exceto gateways NAT. 3. Crie um gateway NAT privado na mesma sub-rede. Para obter instruções, consulte Criar um gateway NAT na documentação da Amazon VPC. Você deve ser capaz de criar, modificar ou excluir gateways NAT nessa sub-rede.	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
Gerencie a AutomationAdminRole função.	1. Assumir a função `TestAdminRole`. 2. Tente modificar a função `AutomationAdminRole`. Para obter instruções, consulte Modificação de uma função na documentação do IAM. Você não deve ser capaz de modificar essa função. 3. Assuma o perfil `AutomationAdminRole` e repita a etapa anterior. Agora você deveria poder modificar a função.	Administrador da AWS

Limpeza

Tarefa	Descrição	Habilidades necessárias
Limpe os recursos implantados.	1. Separe o SCP da conta da AWS ou da OU. Para obter instruções, consulte Separar um SCP na documentação do AWS Organizations. 2. Exclua a SCP. Para obter instruções, consulte Excluir um SCP (Documentação do AWS Organizations). 3. Exclua a função `AutomationAdminRole` e a função `TestAdmin`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	`Role` . Para obter instruções, consulte Como excluir perfis na documentação do IAM. 4. Exclua todos os recursos de rede, como VPCs sub-redes, que você criou para essa solução.	

Recursos relacionados

Documentação da AWS

- Fixação e desmontagem SCPs
- Criando, atualizando e excluindo SCPs
- Implemente controles de acesso baseados em atributos de detetive para sub-redes públicas usando o AWS Config
- Controles de detecção
- Referência de autorização do serviço
- Marcar recursos da AWS
- O que é ABAC para a AWS?

Referências adicionais AWS

- Proteger tags de recursos usadas para autorização usando uma política de controle de serviços no AWS Organizations (publicação no blog da AWS)

Mais informações

A política de controle de serviço a seguir é um exemplo que você pode usar para testar essa abordagem em sua organização.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyVPCActions",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateVPC",
        "ec2:CreateRoute",
        "ec2:CreateSubnet",
        "ec2:CreateInternetGateway",
        "ec2:DeleteVPC",
        "ec2:DeleteRoute",
        "ec2:DeleteSubnet",
        "ec2:DeleteInternetGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:*"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "AllowNATGWOnIFASubnet",
      "Effect": "Deny",
      "NotAction": [
        "ec2:CreateNatGateway",
        "ec2:DeleteNatGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition": {
        "ForAnyValue:StringEqualsIfExists": {
          "aws:ResourceTag/SubnetType": "IFA"
        },
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
```

```
      "Sid": "DenyChangesToAdminRole",
      "Effect": "Deny",
      "NotAction": [
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AutomationAdminRole"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "allowbydefault",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Implemente as automações de segurança para a AWS WAF solução usando o Terraform

Criado pelo Dr. Rahul Sharad Gaikwad (AWS) e Tamilselvan P (AWS)

Resumo

AWS WAF é um firewall de aplicativos da web que ajuda a proteger os aplicativos contra explorações comuns usando regras personalizáveis, que você define e implanta nas listas de controle de acesso à web ()ACLs. Configurar AWS WAF regras pode ser um desafio, especialmente para organizações que não têm equipes de segurança dedicadas. Para simplificar esse processo, a Amazon Web Services (AWS) oferece a AWS WAF solução Security Automations for, que implanta automaticamente uma única ACL da web com um conjunto de AWS WAF regras que filtra ataques baseados na web. Durante a implantação do Terraform, você pode especificar quais atributos de proteção incluir. Depois de implantar essa solução, AWS WAF inspeciona as solicitações da web para CloudFront distribuições existentes da Amazon ou Application Load Balancers e bloqueia todas as solicitações que não correspondam às regras.

A AWS WAF solução Security Automations for pode ser implantada usando de AWS CloudFormation acordo com as instruções no Guia de Implementação de Automações de AWS WAF Segurança. Esse padrão fornece uma opção alternativa de implantação para organizações que usam o HashiCorp Terraform como sua ferramenta preferida de infraestrutura como código (IaC) para provisionar e gerenciar sua infraestrutura em nuvem. Quando você implanta essa solução, o Terraform aplica automaticamente as alterações na nuvem e implanta e configura as AWS WAF configurações e os recursos de proteção.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS.
- AWS Command Line Interface (AWS CLI) versão 2.4.25 ou posterior, instalada e configurada com as permissões necessárias. Para obter mais informações, consulte Introdução (AWS CLI documentação).
- Terraform versão 1.1.9 ou posterior, instalado e configurado. Para obter mais informações, consulte Instalar o Terraform (documentação do Terraform).

Arquitetura

Arquitetura de destino

Esse padrão implanta as automações de segurança para AWS WAF a solução. Para obter mais informações sobre a arquitetura de destino, consulte Visão geral da arquitetura no Guia de AWS WAF Implementação de Automações de Segurança. Para obter mais informações sobre as AWS Lambda automações nessa implantação, o analisador de log de aplicativos, o analisador de AWS WAF log, o analisador de listas de IP e o manipulador de acesso, consulte Detalhes do componente no Guia de Implementação de Automações de Segurança. AWS WAF

Implantação do Terraform

Quando você executa o `terraform apply`, o Terraform faz o seguinte:

1. O Terraform cria funções AWS Identity and Access Management (IAM) e funções Lambda com base nas entradas do arquivo testing.tfvars.
2. O Terraform cria regras de AWS WAF ACL e conjuntos de IP com base nas entradas do arquivo testing.tfvars.
3. O Terraform cria buckets do Amazon Simple Storage Service (Amazon S3), regras AWS Glue da Amazon, tabelas de banco de dados e grupos de trabalho do EventBridge Amazon Athena com base nas entradas do arquivo testing.tfvars.
4. O Terraform implanta a AWS CloudFormation pilha para provisionar os recursos personalizados.
5. O Terraform cria os recursos do Amazon API Gateway com base nas entradas fornecidas do arquivo testing.tfvars.

Automação e escala

Você pode usar esse padrão para criar AWS WAF regras para várias Contas da AWS e implantar Regiões da AWS a AWS WAF solução Security Automations for em todo o seu Nuvem AWS ambiente.

Ferramentas

Serviços da AWS

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.

- AWS WAFé um firewall de aplicativo web que ajuda você a monitorar solicitações HTTP e HTTPS que são encaminhadas para seus recursos protegidos de aplicativos web.

Outros serviços

- Git é um sistema de controle de versão distribuído e de código aberto.
- HashiCorp O Terraform é um aplicativo de interface de linha de comando que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.

Repositório de código

O código desse padrão está disponível no repositório GitHub AWS WAF Automation Using Terraform.

Práticas recomendadas

- Coloque arquivos estáticos em buckets separados do Amazon S3.
- Evite variáveis de codificação permanente.
- Limite o uso de scripts personalizados.
- Adote uma convenção de nomenclatura.

Épicos

Configure sua estação de trabalho local.

Tarefa	Descrição	Habilidades necessárias
Instale o Git.	Siga as instruções em Conceitos básicos (site do Git) para instalar o Git na sua estação de trabalho local.	DevOps engenheiro
Clonar o repositório.	Na sua estação de trabalho local, digite o seguinte comando para clonar o repositório de código:	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`git clone https://github.com/aws-samples/aws-waf-automation-terraform-samples.git`	
Atualize as variáveis.	1. Navegue até o diretório clonado digitando o seguinte comando: `cd terraform-aws-waf-automation` 2. Em qualquer editor de texto, abra o arquivo testing.tfvars. 3. Atualize os valores das variáveis no arquivo testing.tfvars. 4. Salve e feche o arquivo.	DevOps engenheiro

Forneça a arquitetura de destino usando o Terraform

Tarefa	Descrição	Habilidades necessárias
Inicialize a configuração do Terraform.	Digite o comando a seguir para inicializar seu diretório de trabalho que contém os arquivos de configuração do Terraform: `terraform init`	DevOps engenheiro
Visualize o plano do Terraform.	Insira o comando da a seguir. O Terraform avalia	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	os arquivos de configuração para determinar o estado de destino dos recursos declarados. Em seguida, ele compara o estado de destino com o estado atual e cria um plano: `terraform plan -var-file ="testing.tfvars"`	
Verificar o plano.	Revise o plano e confirme se ele configura a arquitetura necessária em seu destino Conta da AWS.	DevOps engenheiro
Implante a solução.	1. Insira o comando a seguir para aplicar o plano: `terraform apply -var-file="testing.tfvars"` 2. Digite `yes` para confirmar. O Terraform cria, atualiza ou destrói a infraestrutura para atingir o estado de destino declarado nos arquivos de configuração. Para obter mais informações sobre a sequência, consulte Implantação do Terraform na seção Arquitetura desse padrão.	DevOps engenheiro

Validar e limpar

Tarefa	Descrição	Habilidades necessárias
Verifique as alterações.	1. No console do Terraform , verifique se as saídas correspondem aos resultados esperados. 2. Faça login no AWS Management Console. 3. Verifique se as saídas no console do Terraform foram implantadas com sucesso em seu. Conta da AWS	DevOps engenheiro
(Opcional) Limpe a infraestrutura.	Se deseja remover todos os recursos e as alterações de configuração feitas por essa solução, faça o seguinte: 1. No console do Terraform, insira o seguinte comando: `terraform destroy -var-file="testing .tfvars”` 2. Digite `yes` para confirmar.	DevOps engenheiro

Solução de problemas

Problema	Solução
Erro `WAFV2 IPSet: WAFOptimisticLockException`	Se você receber esse erro ao executar o comando `terraform destroy`, deverá excluir manualmente os conjuntos de IP.

Problema	Solução
	Para obter instruções, consulte Excluindo um conjunto de IPs (AWS WAF documentação).

Recursos relacionados

AWS referências

- Guia de AWS WAF implementação de automações de segurança
- Automações de segurança para AWS WAF (Biblioteca de AWS soluções)
- Automações de segurança para perguntas frequentes AWS WAF

Referências do Terraform

- Configuração de back-end do Terraform
- Terraform AWS Provider - Documentação e uso
- Terraform AWS Provider (GitHub repositório)

Detecte instâncias de banco de dados Amazon RDS e Aurora que têm certificados CA expirados

Criado por Stephen DiCato (AWS) e Eugene Shifer (AWS)

Resumo

Como prática recomendada de segurança, é recomendável criptografar dados em trânsito entre servidores de aplicativos e bancos de dados relacionais. Você pode usar SSL ou TLS para criptografar uma conexão com uma instância ou cluster de banco de dados (DB). Esses protocolos ajudam a fornecer confidencialidade, integridade e autenticidade entre um aplicativo e um banco de dados. O banco de dados usa um certificado de servidor, que é emitido por uma autoridade de certificação (CA) e é usado para realizar a verificação da identidade do servidor. O SSL ou o TLS verificam a autenticidade do certificado validando sua assinatura digital e garantindo que ela não tenha expirado.

No AWS Management Console, o Amazon Relational Database Service (Amazon RDS) e o Amazon Aurora fornecem notificações sobre instâncias de banco de dados que exigem atualizações de certificados. No entanto, para verificar essas notificações, você deve fazer login em cada uma delas Conta da AWS e navegar até o console de serviço em cada uma Região da AWS. Essa tarefa se torna mais complexa se você precisar avaliar a validade do certificado em muitos Contas da AWS que são gerenciados como uma organização em AWS Organizations.

Ao provisionar a infraestrutura como código (IaC) fornecida nesse padrão, você pode detectar certificados de CA expirados para todas as instâncias de banco de dados Amazon RDS e Aurora em sua organização. Conta da AWS AWS O AWS CloudFormationmodelo fornece uma AWS Config regra, uma AWS Lambda função e as permissões necessárias. Você pode implantá-lo em uma única conta como uma pilha ou implantá-lo em toda a AWS organização como um conjunto de pilhas.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Se você estiver implantando em um único Conta da AWS:
  - Certifique-se de ter permissões para criar CloudFormation pilhas.
  - Ative AWS Config na conta de destino.
  - (Opcional) Ative AWS Security Hub na conta de destino.

- Se você estiver implantando em uma AWS organização:
  - Certifique-se de ter permissões para criar conjuntos de CloudFormation pilhas.
  - Ative o Security Hub com AWS Organizations integração.
  - Ative AWS Config nas contas em que você está implantando essa solução.
  - Designe um Conta da AWS para ser o administrador delegado do Security Hub AWS Config e do Security Hub.

Limitações

- Se você estiver implantando em uma conta individual que não tem o Security Hub ativado, você pode usar AWS Config para avaliar as descobertas.
- Se você estiver implantando em uma organização que não tem um administrador delegado para AWS Config o Security Hub, você deve fazer login nas contas individuais dos membros para ver as descobertas.
- Se você usa AWS Control Tower para gerenciar e governar as contas em sua organização, implante o IaC nesse padrão usando Personalizações para AWS Control Tower (cFct). O uso do CloudFormation console criará um desvio de configuração a partir das AWS Control Tower grades de proteção e exigirá que você inscreva novamente as unidades organizacionais () OUs ou as contas gerenciadas.
- Alguns Serviços da AWS não estão disponíveis em todos Regiões da AWS. Para ver a disponibilidade da região, consulte a página de endpoints e cotas do serviço e escolha o link para o serviço.

Arquitetura

Implantação em um indivíduo Conta da AWS

O diagrama de arquitetura a seguir mostra a implantação dos AWS recursos em um único Conta da AWS. Ele é implementado usando um CloudFormation modelo diretamente no CloudFormation console. Se o Security Hub estiver ativado, você poderá visualizar os resultados em um AWS Config ou no Security Hub. Se o Security Hub não estiver ativado, você poderá visualizar os resultados somente no AWS Config console.

O diagrama mostra as seguintes etapas:

1. Você cria uma CloudFormation pilha. Isso implanta uma função Lambda e AWS Config uma regra. Tanto a regra quanto a função são configuradas com as permissões AWS Identity and Access Management (IAM) necessárias para publicar avaliações de recursos AWS Config e registros.
2. A AWS Config regra opera no modo de avaliação de detetive e é executada a cada 24 horas.
3. O Security Hub recebe todas as AWS Config descobertas.
4. Você pode ver as descobertas no Security Hub ou no AWS Config, dependendo da configuração da conta.

Implantação em uma organização AWS

O diagrama a seguir mostra a avaliação da expiração do certificado em várias contas gerenciadas por meio de AWS Organizations AWS Control Tower e. Você implanta o CloudFormation modelo por meio do cFct. Os resultados da avaliação são centralizados no Security Hub na conta do administrador delegado. O AWS CodePipeline fluxo de trabalho descrito no diagrama mostra as etapas em segundo plano que ocorrem durante a implantação do cFCT.

O diagrama mostra as seguintes etapas:

1. Dependendo da configuração do cFCT, na conta de gerenciamento, você envia o IaC para um AWS CodeCommit repositório ou carrega um arquivo compactado (ZIP) do IaC em um bucket do Amazon Simple Storage Service (Amazon S3).
2. O pipeline cFct descompacta o arquivo, executa as verificações cfn-nag (GitHub) e o implanta como um conjunto de pilhas. CloudFormation
3. Dependendo da configuração especificada no arquivo de manifesto cFct, CloudFormation StackSets implanta pilhas em contas individuais ou especificadas. OUs Isso implanta uma função Lambda e AWS Config uma regra nas contas de destino. Tanto a regra quanto a função são configuradas com as permissões do IAM necessárias para publicar avaliações de recursos AWS Config e registros.
4. A AWS Config regra opera no modo de avaliação de detetive e é executada a cada 24 horas.
5. AWS Config encaminha todas as descobertas para o Security Hub.
6. As descobertas do Security Hub são agregadas na conta do administrador delegado.
7. Você pode ver as descobertas no Security Hub na conta de administrador delegado.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo. Uma AWS Config regra define suas configurações ideais para um recurso e AWS Config pode avaliar se seus AWS recursos estão em conformidade com as condições em suas regras.
- AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas. As personalizações para AWS Control Tower (cFct) ajudam você a personalizar sua AWS Control Tower landing zone e a se manter alinhado com as melhores práticas. AWS As personalizações são implementadas com CloudFormation modelos e políticas de controle de serviços ()SCPs.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS. Também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança.

Outras ferramentas

- Python é uma linguagem de programação de computador de uso geral.

Repositório de código

O código desse padrão está disponível no repositório GitHub Detectar instâncias do Amazon RDS com certificados CA expirados.

Práticas recomendadas

Recomendamos que você siga as melhores práticas dos seguintes recursos:

- Melhores práticas para unidades organizacionais com AWS Organizations (blog de operações e migrações AWS na nuvem)
- Orientação para estabelecer uma base inicial usando AWS Control Tower on AWS (Biblioteca de AWS soluções)
- Orientação para criar e modificar AWS Control Tower recursos (AWS Control Tower documentação)
- Considerações sobre a implantação do cFCT (documentação)AWS Control Tower

Épicos

Analise a solução e o código

Tarefa	Descrição	Habilidades necessárias
Determine sua estratégia de implantação.	Analise a solução e o código para determinar como você os implantará em seu AWS ambiente. Determine se você fará a implantação em uma única conta ou AWS organizaç ão.	Proprietário do aplicativo, General AWS
Clonar o repositório.	Insira o comando a seguir para clonar o repositório Detect Amazon RDS com certificados CA expirados. `git clone https://github.com/aws-samples/config-rds-ca-expiry.git`	Desenvolvedor do aplicativo, proprietário do aplicativo

Tarefa	Descrição	Habilidades necessárias
Valide a versão do Python.	1. Navegue até o diretório de nível superior no repositório clonado. `cd config-rds-ca-expiry` 2. Abra config-rds-ca-expiry.yaml. 3. No `CertExpirationCheckLambdaFunction` recurso, confirme se a versão do Python é compatível com seu destino. Regiões da AWS Por padrão, essa função usa o Python 3.12. Para obter mais informações, consulte AWS Lambda adiciona suporte ao Python 3.12. Se necessário, atualize a versão do Python. 4. Salve e feche config-rds-ca-expiry.yaml.	Desenvolvedor do aplicativo, proprietário do aplicativo

Implante a solução

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	Implante o CloudFormation modelo em seu AWS ambiente. Execute um destes procedimentos:	Desenvolvedor de aplicativos, administrador da AWS, AWS geral

Tarefa	Descrição	Habilidades necessárias
	• Se você estiver implantando em uma única Conta da AWS, siga as instruções em Criação de uma pilha. • Se você estiver implantando em uma organização que não é gerenciada por AWS Control Tower, siga as instruções em Criar um conjunto de pilhas. • Se você estiver implantando em uma organização gerenciada por AWS Control Tower, consulte as instruções em Crie suas próprias personalizações.	
Verificar a implantação.	No CloudFormation console, verifique se a pilha ou o conjunto de pilhas foi implantado com êxito.	Administrador da AWS, proprietário do aplicativo

Analise as descobertas

Tarefa	Descrição	Habilidades necessárias
Veja as conclusões da AWS Config regra.	No Security Hub, faça o seguinte para ver uma lista de descobertas individuais: 1. Abra o console do Security Hub. 2. No painel de navegação, selecione Descobertas.	Administrador da AWS, administrador de sistemas da AWS, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
	3. Na caixa Adicionar filtros, adicione os seguintes filtros: • O status de conformidade é `FAILED` • O título é `rds-has-expiring-ca` 4. Escolha Aplicar. No Security Hub, faça o seguinte para ver uma lista do total de descobertas agrupadas por Conta da AWS: 1. Abra o console do Security Hub. 2. No painel de navegação, escolha Insights. 3. Escolha Criar insight. 4. Para selecionar o atributo de agrupamento do insight: a. Escolha a caixa de pesquisa para exibir as opções de filtro. b. Escolha Agrupar por. c. Selecione AwsAccountId. d. Escolha Aplicar. 5. Na caixa Adicionar filtros, adicione os seguintes filtros: • O título é `rds-has-expiring-ca`	

Tarefa	Descrição	Habilidades necessárias
	• O status de conformidade é `FAILED` 6. Escolha Criar insight. 7. Insira um Nome do insight e escolha Criar insight. Em AWS Config, para ver uma lista de descobertas, siga as instruções em Exibindo informações de conformidade e resultados da avaliação na AWS Config documentação.	

Solução de problemas

Problema	Solução
CloudFormation falha na criação ou exclusão do conjunto de pilhas	Quando AWS Control Tower implantado, ele impõe as proteções necessárias e assume o controle sobre agregadores e regras. AWS Config Isso inclui evitar quaisquer alteraçõe s diretas. CloudFormation Para implantar ou remover adequadamente esse CloudFormation modelo, incluindo todos os recursos associado s, você deve usar o cFct.
O cFct falha ao excluir o modelo CloudForm ation	Se o CloudFormation modelo persistir mesmo depois de fazer as alterações necessárias no arquivo de manifesto e remover os arquivos de modelo, confirme se o arquivo de manifesto contém o `enable_stack_set_deletion` parâmetro e se o valor está definido como. `false` Para obter mais informações, consulte

Problema	Solução
	Excluir um conjunto de pilhas na documentação do cFct.

Recursos relacionados

- Usando SSL/TLS para criptografar uma conexão com uma instância de banco de dados ou cluster (documentação do Amazon RDS)
- AWS Config Regras personalizadas (AWS Config documentação)

Gere dinamicamente uma política do IAM com o IAM Access Analyzer usando Step Functions

Criado por Thomas Scott (AWS), Adil El Kanabi (AWS), Koen van Blijderveen (AWS) e Rafal Pawlaszek (AWS)

Resumo

Aviso: não AWS CodeCommit está mais disponível para novos clientes. Os clientes existentes do AWS CodeCommit podem continuar usando o serviço normalmente. Saiba mais.

Privilégio mínimo é a prática recomendada de segurança para conceder as permissões mínimas necessárias para executar uma tarefa. Implementar o acesso com privilégios mínimos em uma conta já ativa da Amazon Web Services (AWS) pode ser um desafio, pois você não quer impedir acidentalmente que os usuários realizem suas tarefas alterando suas permissões. Antes de implementar mudanças na política AWS Identity and Access Management (IAM), você precisa entender as ações e os recursos que os usuários da conta estão executando.

Esse padrão foi projetado para ajudá-lo a aplicar o princípio do acesso com privilégios mínimos, sem bloquear ou diminuir a produtividade da equipe. Ele descreve como usar o IAM Access Analyzer e AWS Step Functions gerar dinamicamente uma política up-to-date do IAM para sua função, com base nas ações que estão sendo executadas atualmente na conta. A nova política foi projetada para permitir a atividade atual, mas remover quaisquer privilégios elevados e desnecessários. Você pode personalizar a política gerada definindo regras de permissão e negação, e a solução integra suas regras personalizadas.

Esse padrão inclui opções para implementar a solução com AWS Cloud Development Kit (AWS CDK) o HashiCorp CDK for Terraform (CDKTF). É possível então associar a nova política à função usando um pipeline de integração e entrega contínuas (CI/CD). Se você tiver uma arquitetura de várias contas, poderá implantar essa solução em qualquer conta em que queira gerar políticas atualizadas do IAM para as funções, aumentando a segurança de todo o seu Nuvem AWS ambiente.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS com uma AWS CloudTrail trilha ativada.
- Permissões do IAM para o seguinte:

  - Crie e implante fluxos de trabalho do Step Functions. Para obter mais informações, consulte Ações, recursos e chaves de condição para AWS Step Functions (documentação do Step Functions).
  - Crie AWS Lambda funções. Para obter mais informações, consulte Função de execução e permissões de usuário (documentação do Lambda).
  - Crie perfis do IAM. Para obter mais informações, consulte Criar uma função para delegar permissões a um usuário do IAM (documentação do IAM).
- NPM instalado. Para obter mais informações, consulte Como baixar e instalar o Node.js e o npm (documentação do npm).
- Se você estiver implantando essa solução com AWS CDK (Opção 1):
  - AWS CDK Kit de ferramentas, instalado e configurado. Para obter mais informações, consulte Instalar o AWS CDK (AWS CDK documentação).
- Se você estiver implantando essa solução com o CDKTF (Opção 2):
  - CDKTF, instalado e configurado. Para obter mais informações, consulte Instalar o CDK for Terraform (documentação do CDKTF).
  - Terraform, instalado e configurado. Para obter mais informações, consulte Introdução (documentação do Terraform).
- AWS Command Line Interface (AWS CLI) instalado e configurado localmente para o seu Conta da AWS. Para obter mais informações, consulte Instalando ou atualizando a versão mais recente do AWS CLI (AWS CLI documentação).

Limitações

- Esse padrão não aplica a nova política do IAM ao perfil. No final dessa solução, a nova política do IAM é armazenada em um AWS CodeCommit repositório. Você pode usar um pipeline de CI/CD para aplicar políticas às funções em sua conta.

Arquitetura

Arquitetura de destino

1. Uma regra de EventBridge evento regular da Amazon inicia um fluxo de trabalho de Step Functions. Você define esse cronograma de regeneração como parte da configuração dessa solução.

2. No fluxo de trabalho do Step Functions, uma função Lambda gera os intervalos de datas a serem usados ao analisar a atividade da conta nos CloudTrail registros.
3. A próxima etapa do fluxo de trabalho chama a API IAM Access Analyzer para começar a gerar a política.
4. Usando o Amazon Resource Name (ARN) da função que você especifica durante a configuração, o IAM Access Analyzer analisa os CloudTrail registros de atividades dentro da taxa de data especificada. Com base na atividade, o IAM Access Analyzer gera uma política do IAM que permite somente as ações e serviços usados pela função durante o intervalo de datas especificado. Quando essa etapa for concluída, ela gerará uma ID de trabalho.
5. A próxima etapa do fluxo de trabalho verifica o ID do trabalho a cada 30 segundos. Quando o ID do trabalho é detectado, essa etapa usa o ID do trabalho para chamar a API IAM Access Analyzer e recuperar a nova política do IAM. O IAM Access Analyzer retorna a política como um arquivo JSON.
6. A próxima etapa do fluxo de trabalho coloca o arquivo <IAM role name>/policy.json em um bucket do Amazon Simple Storage Service (Amazon S3). Você define esse bucket do S3 como parte da configuração dessa solução.
7. Uma notificação de eventos do Amazon S3 inicia uma função do Lambda.
8. A função Lambda recupera a política do bucket do S3, integra as regras personalizadas que você define nos arquivos allow.json e deny.json e, em seguida, envia a política atualizada para. CodeCommit Você define o CodeCommit repositório, a ramificação e o caminho da pasta como parte da configuração dessa solução.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- AWS CDK O Toolkit é um kit de desenvolvimento em nuvem de linha de comando que ajuda você a interagir com seu AWS Cloud Development Kit (AWS CDK) aplicativo.
- AWS CloudTrailajuda você a auditar a governança, a conformidade e o risco operacional do seu Conta da AWS.
- AWS CodeCommité um serviço de controle de versão que ajuda você a armazenar e gerenciar repositórios Git de forma privada, sem precisar gerenciar seu próprio sistema de controle de origem.

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los. Esse padrão usa o IAM Access Analyzer, um recurso do IAM, para analisar seus CloudTrail registros e identificar ações e serviços que foram usados por uma entidade do IAM (usuário ou função) e, em seguida, gerar uma política do IAM com base nessa atividade.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios. Nesse padrão, você usa integrações de serviços do AWS SDK em Step Functions para chamar ações de API de serviço do seu fluxo de trabalho.

Outras ferramentas

- O CDK for Terraform (CDKTF) ajuda você a definir infraestrutura como código (IaC) usando linguagens de programação comuns, como Python e Typescript.
- O Lerna é um sistema de compilação para gerenciar e publicar vários TypeScript pacotes JavaScript ou pacotes do mesmo repositório.
- O Node.js é um ambiente de tempo de JavaScript execução orientado a eventos projetado para criar aplicativos de rede escaláveis.
- O npm é um registro de software executado em um ambiente Node.js e usado para compartilhar ou emprestar pacotes e gerenciar a implantação de pacotes privados.

Repositório de código

O código desse padrão está disponível no repositório do GitHub Automated IAM Access Analyzer Role Policy Generator.

Épicos

Preparar-se para implantação

Tarefa	Descrição	Habilidades necessárias
Clone o repositório.	O comando a seguir clona o repositório Role Policy Generator (GitHub) do Automated IAM Access Analyzer. `git clone https://github.com/aws-samples/automated-iam-access-analyzer.git`	Desenvolvedor de aplicativos
Instale o Lerna.	O comando a seguir instala o Lerna. `npm i -g lerna`	Desenvolvedor de aplicativos

Configure as dependências.	O comando a seguir instala as dependências do repositório.
	`cd automated-iam-access-analyzer/`
	`npm install && npm run bootstrap`
		Desenvolvedor de aplicativos

Crie o código.	O comando a seguir testa, cria e prepara os pacotes zip das funções do Lambda.
	`npm run test:code`
	`npm run build:code`
	`npm run pack:code`
		Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias
Construa as estruturas.	O comando a seguir cria os aplicativos de síntese da infraestrutura, tanto para o CDKTF quanto AWS CDK para o CDKTF. `npm run build:infra`	
Configure todas as permissões personalizadas.	Na pasta repo do repositório clonado, edite os arquivos allow.json e deny.json para definir quaisquer permissões personalizadas para a função. Se os arquivos allow.json e deny.json contiverem a mesma permissão, a permissão deny será aplicada.	Administrador da AWS, desenvolvedor de aplicativos

Opção 1 — Implantar a solução usando AWS CDK

Tarefa	Descrição	Habilidades necessárias
Implante a AWS CDK pilha.	O comando a seguir implanta a infraestrutura por meio de AWS CloudFormation. Defina os seguintes parâmetros: • `<NAME_OF_ROLE>` : o ARN do perfil do IAM para a qual você está criando uma nova política. • `<TRAIL_ARN>` — O ARN da CloudTrail trilha na qual	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	a atividade da função é armazenada.
	• <CRON_EXPRESSION_TO_RUN_SOLUTION> : a expressão Cron que define o cronograma de regeneração da política. O fluxo de trabalho do Step Functions é executado nesse cronograma.
	• <TRAIL_LOOKBACK> : o período, em dias, para relembrar a trilha ao avaliar as permissões da função.
	
	`cd infra/cdk`
	`cdk deploy –-parameters roleArn=<NAME_OF_ROLE> \`
	`–-parameters trailArn=<TRAIL_ARN> \`
	`--parameters schedule=<CRON_EXPRESSION_TO_RUN_SOLUTION> \`
	`[ --parameters trailLookBack=<TRAIL_LOOKBACK> ]`
	
	Note
	Os colchetes indicam parâmetros opcionais.	

Tarefa	Descrição	Habilidades necessárias
(Opcional) Aguarde a nova política.	Se a trilha não contiver uma quantidade razoável de atividades históricas para a função, espere até ter certeza de que há atividade registrad a suficiente para que o IAM Access Analyzer gere uma política precisa. Se a função estiver ativa na conta por um período suficiente, esse período de espera talvez não seja necessário.	Administrador da AWS
Revise manualmente a política gerada.	No seu CodeCommit repositór io, revise o arquivo.json <ROLE_ARN>gerado para confirmar se as permissões de permissão e negação são apropriadas para a função.	Administrador da AWS

Opção 2 – Implantar a solução usando CDKTF

Tarefa	Descrição	Habilidades necessárias
Sintetize o modelo do Terraform.	O comando a seguir sintetiza o modelo do Terraform. `lerna exec cdktf synth --scope @aiaa/tfm`	Desenvolvedor de aplicativos
Implante o modelo do Terraform.	O comando a seguir navega até o diretório que contém a infraestrutura definida pelo CDKTF.	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	`cd infra/cdktf`
	
	O comando a seguir implanta a infraestrutura no destino Conta da AWS. Defina os seguintes parâmetros:
	
	• `<account_ID>` : o ID da conta de destino.
	• `<region>`- O alvo Região da AWS.
	• `<selected_role_ARN>` : o ARN do perfil do IAM para a qual você está criando uma nova política.
	• `<trail_ARN>` — O ARN da CloudTrail trilha na qual a atividade da função é armazenada.
	• `<schedule_expression>` : a expressão Cron que define o cronograma de regeneração da política. O fluxo de trabalho do Step Functions é executado nesse cronograma.
	• `<trail_look_back>` : o período, em dias, para relembrar a trilha ao avaliar as permissões da função.
	
	`TF_VAR_accountId=< account_ID> \`	

Tarefa	Descrição	Habilidades necessárias
	TF_VAR_region=<reg ion> \ TF_VAR_roleArns=<s elected_role_ARN> \ TF_VAR_trailArn=<t rail_ARN> \ TF_VAR_schedule=<s chedule_expression> \ [TF_VAR_trailLookBa ck=<trail_look_bac k>] \ cdktf deploy **Note** Os colchetes indicam parâmetros opcionais.	
(Opcional) Aguarde a nova política.	Se a trilha não contiver uma quantidade razoável de atividades históricas para a função, espere até ter certeza de que há atividade registrada suficiente para que o IAM Access Analyzer gere uma política precisa. Se a função estiver ativa na conta por um período suficiente, esse período de espera talvez não seja necessário.	Administrador da AWS
Revise manualmente a política gerada.	No seu CodeCommit repositório, revise o arquivo.json <ROLE_ARN>gerado para confirmar se as permissões de permissão e negação são apropriadas para a função.	Administrador da AWS

Recursos relacionados

AWS recursos

- Endpoints e cotas do IAM Access Analyzer
- Configurando o AWS CLI
- Começando com o AWS CDK
- Permissões de privilégio mínimo

Outros recursos

- CDK para Terraform (site do Terraform)

Habilite a Amazon GuardDuty condicionalmente usando modelos AWS CloudFormation

Criado por Ram Kandaswamy (AWS)

Resumo

Você pode habilitar a Amazon GuardDuty em uma conta da Amazon Web Services (AWS) usando um AWS CloudFormation modelo. Por padrão, se já GuardDuty estiver habilitado quando você tentar usá-lo CloudFormation para ativá-lo, a implantação da pilha falhará. No entanto, você pode usar condições em seu CloudFormation modelo para verificar se já GuardDuty está habilitado. CloudFormation suporta o uso de condições que comparam valores estáticos; ele não suporta o uso da saída de outra propriedade de recurso dentro do mesmo modelo. Para obter mais informações, consulte Condições na CloudFormation documentação.

Nesse padrão, você usa um recurso CloudFormation personalizado apoiado por uma AWS Lambda função para habilitar condicionalmente, GuardDuty caso ainda não esteja habilitado. Se GuardDuty estiver habilitada, a pilha captura o status e o registra na seção de saída da pilha. Se não GuardDuty estiver habilitado, a pilha o habilita.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Uma função AWS Identity and Access Management (IAM) que tem permissões para criar, atualizar e excluir CloudFormation pilhas
- AWS Command Line Interface (AWS CLI), instalado e configurado

Limitações

Se GuardDuty tiver sido desativado manualmente para um Conta da AWS ou Região da AWS, esse padrão não é ativado GuardDuty para essa conta ou região de destino.

Arquitetura

Pilha de tecnologias de destino

O padrão é usado CloudFormation para infraestrutura como código (IaC). Você usa um recurso CloudFormation personalizado apoiado por uma função Lambda para obter a capacidade dinâmica de habilitação de serviços.

Arquitetura de destino

O diagrama de arquitetura de alto nível a seguir mostra o processo de habilitação GuardDuty por meio da implantação de um CloudFormation modelo:

1. Você implanta um CloudFormation modelo para criar uma CloudFormation pilha.
2. A pilha cria um perfil do IAM e uma função do Lambda.
3. A função do Lambda assume o perfil do IAM.
4. Se ainda não GuardDuty estiver habilitado no destino Conta da AWS, a função Lambda o habilita.

Automação e escala

Você pode usar o AWS CloudFormation StackSet recurso para estender essa solução para vários Contas da AWS Regiões da AWS e. Para obter mais informações, consulte Trabalhando com AWS CloudFormation StackSets na CloudFormation documentação.

Ferramentas

- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- GuardDutyA Amazon é um serviço contínuo de monitoramento de segurança que analisa e processa registros para identificar atividades inesperadas e potencialmente não autorizadas em seu AWS ambiente.
- AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus AWS recursos controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

Épicos

Crie o CloudFormation modelo e implante a pilha

Tarefa	Descrição	Habilidades necessárias
Crie o CloudFormation modelo.	1. Copie o código no CloudFormation modelo na seção Informações adicionais. 2. Cole o código em um editor de textos. 3. Salve o arquivo como `sample.yaml` na sua estação de trabalho.	AWS DevOps
Crie a CloudFormation pilha.	1. No AWS CLI, insira o seguinte comando. Isso cria uma nova CloudFormation pilha usando o `sample.yaml` arquivo. Para obter mais informações, consulte Criação de uma pilha na CloudFormation documentação. `aws cloudformation create-stack \ --stack-name guardduty-cf-stack \ --template-body file://sample.yaml` 2. Confirme se o valor a seguir aparece no AWS CLI, indicando que a pilha foi criada com sucesso. A quantidade de tempo	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	necessária para criar a pilha pode variar. `"StackStatus": "CREATE_COMPLETE",`	
Valide se GuardDuty está habilitado para o. Conta da AWS	1. Faça login no AWS Management Console e abra o GuardDuty console. 2. Verifique se o GuardDuty serviço está ativado.	Administrador de nuvem, administrador da AWS
Configure contas ou regiões adicionais.	Conforme necessário para seu caso de uso, use o CloudFormation StackSet recurso para estender essa solução para vários Contas da AWS Regiões da AWS e. Para obter mais informaçõ es, consulte Trabalhando com AWS CloudFormation StackSets na CloudFormation documentação.	Administrador de nuvem, administrador da AWS

Recursos relacionados

Referências

- AWS CloudFormation documentação
- AWS Lambda referência de tipo de recurso
- CloudFormation tipo de recurso: AWS: :IAM: :Role
- CloudFormation tipo de recurso: AWS:GuardDuty: :Detector
- Quatro maneiras de recuperar qualquer propriedade AWS de serviço usando AWS CloudFormation (postagem do blog)

Tutoriais e vídeos

- Simplifique seu gerenciamento de infraestrutura usando AWS CloudFormation (Tutorial)
- Use AWS Security Hub a Amazon GuardDuty e proteja várias contas (AWS re:Invent 2020)
- Práticas recomendadas para criação AWS CloudFormation(AWS re:Invent 2019)
- Detecção de ameaças em AWS: uma introdução à Amazon GuardDuty (AWS re:INFORCE 2019)

Mais informações

CloudFormation modelo

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  rLambdaLogGroup:
    Type: 'AWS::Logs::LogGroup'
    DeletionPolicy: Delete
    Properties:
      RetentionInDays: 7
      LogGroupName: /aws/lambda/resource-checker
  rLambdaCheckerLambdaRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Sub 'resource-checker-lambda-role-${AWS::Region}'
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: /
      Policies:
        - PolicyName: !Sub 'resource-checker-lambda-policy-${AWS::Region}'
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Sid: CreateLogGroup
                Effect: Allow
                Action:
                  - 'logs:CreateLogGroup'
                  - 'logs:CreateLogStream'
```

```
                - 'logs:PutLogEvents'
                - 'iam:CreateServiceLinkedRole'
                - 'cloudformation:CreateStack'
                - 'cloudformation:DeleteStack'
                - 'cloudformation:Desc*'
                - 'guardduty:CreateDetector'
                - 'guardduty:ListDetectors'
                - 'guardduty:DeleteDetector'
              Resource: '*'
  resourceCheckerLambda:
    Type: 'AWS::Lambda::Function'
    Properties:
      Description: Checks for resource type enabled and possibly name to exist
      FunctionName: resource-checker
      Handler: index.lambda_handler
      Role: !GetAtt
        - rLambdaCheckerLambdaRole
        - Arn
      Runtime: python3.13
      MemorySize: 128
      Timeout: 180
      Code:
        ZipFile: |
          import boto3
          import os
          import json
          from botocore.exceptions import ClientError
          import cfnresponse


          guardduty=boto3.client('guardduty')
          cfn=boto3.client('cloudformation')


          def lambda_handler(event, context):
              print('Event: ', event)
              if 'RequestType' in event:
                if event['RequestType'] in ["Create","Update"]:
                    enabled=False
                    try:
                      response=guardduty.list_detectors()
                      if "DetectorIds" in response and len(response["DetectorIds"])>0:
                        enabled="AlreadyEnabled"
```

```
                      elif "DetectorIds" in response and
 len(response["DetectorIds"])==0:
                        cfn_response=cfn.create_stack(
                          StackName='guardduty-cfn-stack',
                          TemplateBody='{ "AWSTemplateFormatVersion": "2010-09-09",
 "Description": "A sample template",    "Resources": { "IRWorkshopGuardDutyDetector": {
  "Type": "AWS::GuardDuty::Detector",    "Properties": {   "Enable": true  }   } } }'
                          )
                        enabled="True"
                    except Exception as e:
                        print("Exception: ",e)
                    responseData = {}
                    responseData['status'] = enabled
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
 "CustomResourcePhysicalID" )
                elif event['RequestType'] == "Delete":
                    cfn_response=cfn.delete_stack(
                            StackName='guardduty-cfn-stack')
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, {})
  CheckResourceExist:
    Type: 'Custom::LambdaCustomResource'
    Properties:
      ServiceToken: !GetAtt
        - resourceCheckerLambda
        - Arn
Outputs:
  status:
    Value: !GetAtt
      - CheckResourceExist
      - status
```

Opção de código alternativa para o recurso do Lambda

O CloudFormation modelo fornecido usa código embutido para referenciar o recurso Lambda, para facilitar a referência e a orientação. Como alternativa, você pode colocar o código Lambda em um bucket do Amazon Simple Storage Service (Amazon S3) e referenciá-lo no modelo. CloudFormation O código embutido não oferece suporte a dependências ou bibliotecas de pacotes. Você pode apoiá-los colocando o código Lambda em um bucket do Amazon S3 e referenciando-o no modelo. CloudFormation

Substitua as linhas de código a seguir:

```
Code:
```

```
        ZipFile: |
```

com as linhas de código a seguir:

```
Code:
      S3Bucket: <bucket name>
      S3Key: <python file name>
      S3ObjectVersion: <version>
```

A `S3ObjectVersion` propriedade pode ser omitida se você não estiver usando o versionamento em seu bucket do Amazon S3. Para obter mais informações, consulte Uso de versionamento em buckets do Amazon S3 na documentação do Amazon S3.

Suporte para criptografia de dados transparente no Amazon RDS para SQL Server

Criado por Ranga Cherukuri (AWS)

Resumo

Esse padrão descreve como implementar a criptografia transparente de dados (TDE) no Amazon Relational Database Service (Amazon RDS) para SQL Server para criptografar dados em repouso.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma instância de banco de dados do Amazon RDS para SQL Server

Versões do produto

O Amazon RDS oferece atualmente suporte a TDE para as seguintes versões e edições do SQL Server:

- SQL Server 2016 Enterprise Edition
- SQL Server 2017 Enterprise Edition
- SQL Server 2019 Standard e Enterprise Edition
- SQL Server 2022 Standard e Enterprise Editions

Para obter as informações mais recentes sobre versões e edições suportadas, consulte Suporte para criptografia de dados transparente no SQL Server na documentação do Amazon RDS.

Arquitetura

Pilha de tecnologia

- Amazon RDS para SQL Server

Arquitetura

Ferramentas

- O Microsoft SQL Server Management Studio (SSMS) é um ambiente integrado para o gerenciamento de uma infraestrutura do SQL Server. Ele fornece uma interface de usuário e um grupo de ferramentas com editores de scripts avançados que interagem com o SQL Server.

Épicos

Crie um grupo de opções no console do Amazon RDS

Tarefa	Descrição	Habilidades necessárias
Abra o console do Amazon RDS.	Faça login no Console de Gerenciamento da AWS e abra o console do Amazon RDS.	Desenvolvedor, DBA
Crie um grupo de opções.	No painel de navegação, escolha Grupos de opções, Criar grupo. Escolha sqlserver-ee como mecanismo de banco de dados e selecione a versão do mecanismo.	Desenvolvedor, DBA
Adicione a opção TRANSPARENT_DATA_ENCRYPTION.	Edite o grupo de opções que você criou e adicione a opção chamada `TRANSPARENT_DATA_ENCRYPTION` .	Desenvolvedor, DBA

Associe o grupo de opções à instância de banco de dados

Tarefa	Descrição	Habilidades necessárias
Escolha a instância de banco de dados.	No console do Amazon RDS, no painel de navegação,	Desenvolvedor, DBA

Tarefa	Descrição	Habilidades necessárias
	escolha Bancos de dados e selecione a instância de banco de dados que você deseja associar ao grupo de opções.	
Associe o grupo de opções à instância de banco de dados.	Escolha Modificar e, em seguida, use a configuração do grupo de opções para associar a instância de banco de dados SQL Server ao grupo de opções que você criou anteriormente.	Desenvolvedor, DBA
Implemente as alterações.	Aplicar as alterações imediatamente ou durante a próxima janela de manutenção.	Desenvolvedor, DBA

Obtenha o nome do certificado.	Obtenha o nome padrão do certificado usando a consulta a seguir.
	`USE [master]`
	`GO`
	`SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECertificate%'`
	`GO`
		Desenvolvedor, DBA

Crie a chave de criptografia do banco de dados

Tarefa	Descrição	Habilidades necessárias
Conectar a uma instância de banco de dados do Amazon	Para obter instruções, consulte Usando SSMS na	Desenvolvedor, DBA

Tarefa	Descrição	Habilidades necessárias
RDS para SQL Server usando SSMS.	documentação da Micro Focus.	

Crie a chave de criptografia do banco de dados usando o certificado padrão.	Crie uma chave de criptografia de banco de dados usando o nome do certificado padrão que você obteve anteriormente. Use a seguinte consulta T-SQL para criar uma chave de criptografia de banco de dados. Você pode especificar o algoritmo AES_256 em vez de AES_128.
	`USE [Databasename]`
	`GO`
	`CREATE DATABASE`
	`ENCRYPTION KEY`
	`WITH ALGORITHM = AES_128`
	`ENCRYPTION BY SERVER`
	`CERTIFICATE [certificatename]`
	`GO`
		Desenvolvedor, DBA

Ative a criptografia no banco de dados.	Use a consulta T-SQL a seguir para habilitar a criptografia do banco de dados.
	`ALTER DATABASE [Database Name]`
	`SET ENCRYPTION ON`
	`GO`
		Desenvolvedor, DBA

Tarefa	Descrição	Habilidades necessárias
Consulte o status da criptografia.	Use a consulta T-SQL a seguir para verificar o estado da criptografia. `SELECT DB_NAME(database_id) AS DatabaseName, encryption_state, percent_complete FROM sys.dm_database_encryption_keys`	Desenvolvedor, DBA

Recursos relacionados

- Suporte para criptografia de dados com transparência no SQL Server (na documentação do Amazon RDS).
- Trabalhando com grupos de opções (documentação do Amazon RDS)
- Modificando uma instância de banco de dados Amazon RDS (documentação do Amazon RDS)
- Criptografia de dados transparente para SQL Server (documentação da Microsoft)
- Usando SSMS (documentação da Microsoft)

Garanta que os balanceadores de carga da AWS usem protocolos receptores seguros (HTTPS, SSL/TLS)

Criado por Chandini Penmetsa (AWS) e Purushotham G K (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), o Elastic Load Balancing distribui automaticamente o tráfego de entrada do aplicativo em vários destinos, como instâncias do Amazon Elastic Compute Cloud (EC2Amazon), contêineres, endereços IP e funções do AWS Lambda. Os balanceadores de carga usam receptores para definir as portas e os protocolos que o balanceador de carga usa para aceitar o tráfego dos usuários. Os balanceadores de carga de aplicativos tomam decisões de roteamento na camada do aplicativo e usam o. HTTP/HTTPS protocols. Network Load Balancers make routing decisions at the transport layer and use the Transmission Control Protocol (TCP), Transport Layer Security (TLS), User Datagram Protcol (UDP), or TCP_UDP protocols. Classic Load Balancers make routing decisions at either the transport layer, using TCP or Secure Sockets Layer (SSL) protocols, or at the application layer, using HTTP/HTTPS

Sua organização pode ter um requisito de segurança ou conformidade de que os balanceadores de carga aceitem tráfego de usuários somente em protocolos seguros, como HTTPS ou SSL/TLS.

Esse padrão fornece um controle de segurança que usa uma EventBridge regra da Amazon para monitorar as `CreateListener` chamadas de `ModifyListener` API para Application Load Balancers e Network Load Balancers, e as chamadas de `CreateLoadBalancer` API `CreateLoadBalancerListeners` e para Classic Load Balancers. Se HTTP, TCP/UDP ou TCP_UDP forem usados para o protocolo de receptor do balanceador de carga, o controle invocará uma função do Lambda. A função do Lambda publica uma mensagem em um tópico do Amazon Simple Notification Service (Amazon SNS) para enviar uma notificação que contém os detalhes do balanceador de carga.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um endereço de e-mail no qual você deseja receber a notificação de violação
- Um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar o arquivo .zip do código Lambda

Limitações

- Esse controle de segurança não verifica os balanceadores de carga existentes, a menos que seja feita uma atualização nos receptores do balanceador de carga.
- Esse controle de segurança é regional e deve ser implantado nas regiões da AWS que você pretende monitorar.

Arquitetura

Pilha de tecnologias de destino

- Função do Lambda
- Tópico do Amazon SNS
- EventBridge regra

Arquitetura de destino

Automação e escala

- Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

- AWS CloudFormation — CloudFormation A AWS é um serviço que ajuda você a modelar e configurar recursos da AWS usando a infraestrutura como código.
- Amazon EventBridge — EventBridge A Amazon fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos de software como serviço (SaaS) e serviços da AWS, roteando esses dados para destinos como funções Lambda.
- AWS Lambda: o Lambda é compatível com a execução de código sem provisionar ou gerenciar servidores.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.

- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Práticas recomendadas

Certifique-se de que o tópico do SNS usado não esteja acessível ao público. Para obter mais informações, consulte a documentação da AWS.

Épicos

Faça o upload do código do Lambda

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	No console do Amazon S3, escolha ou crie um bucket do S3 com um nome exclusivo que não contenha barras iniciais. Um nome de bucket do S3 é globalmente exclusivo , e o namespace é compartil hado por todas as contas da AWS. Seu bucket do S3 precisa estar na mesma região que o balanceador de carga que está sendo avaliado.	Arquiteto de nuvem
Carregue o código do Lambda para o bucket do S3.	Faça upload do arquivo .zip do código Lambda fornecido na seção “Anexos” para o bucket S3 definido.	Arquiteto de nuvem
Implante o CloudFormation modelo da AWS.	No CloudFormation console da AWS, na mesma região da	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	AWS do bucket S3, implante o modelo fornecido na seção “Anexos”. No próximo épico, forneça os valores para os parâmetros.	

CloudFormation parâmetros

Tarefa	Descrição	Habilidades necessárias
Dê um nome ao bucket do S3.	Em seguida, informe o nome do bucket do S3 que você criou no primeiro épico.	Arquiteto de nuvem
Forneça o prefixo do Amazon S3.	Forneça a localização do arquivo .zip do código do Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `<directory>/<file-name>.zip`).	Arquiteto de nuvem
Forneça o ARN do tópico do SNS.	Forneça o tópico do SNS nome do recurso da Amazon (ARN) se você quiser usar um tópico do SNS existente para notificações de violação. Para criar um novo tópico do SNS, mantenha o valor como `None` (o valor padrão).	Arquiteto de nuvem
Forneça um endereço de e-mail.	Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Defina o nível de registro em log.	Defina o nível de registro em log e a frequência da sua função do Lambda. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo. `Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	Arquiteto de nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Faça download do modelo.	Baixe o CloudFormation modelo fornecido na seção Anexos.	Arquiteto de nuvem
Crie a pilha.	Na mesma região do bucket do S3, navegue até o console CloudFormation de serviço e implante o modelo baixado. Consulte o épico anterior para obter detalhes dos parâmetro s.	Arquiteto de nuvem
Verifique os recursos.	Depois que a pilha for completamente criada, navegue até a guia Recursos e verifique os recursos. O	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	modelo criará os seguintes recursos: • EventBridge regra • Função do Lambda • Função de execução do Lambda • Permissão de invocação do Lambda	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o modelo é implantado com êxito, se um novo tópico do SNS tiver sido criado, uma mensagem de e-mail de assinatura será enviada para o endereço de e-mail fornecido nos parâmetros. Você deve confirmar essa assinatura de e-mail para receber notificações de violação.	Arquiteto de nuvem

Solução de problemas

Problema	Solução
Falha na criação da pilha. Ocorreu um erro enquanto GetObject. Código de erro S3: PermanentRedirect. Mensagem de erro do S3:	Certifique-se de que a região do bucket do S3 e a região em que a pilha está sendo implantada sejam as mesmas.

Problema	Solução
O bucket está nesta região: xx-xxxx-1. Use essa região para repetir a solicitação.	
Falha na criação da pilha. O parâmetro de runtime do python3.6 não é mais compatíve l com a criação ou atualização de funções do AWS Lambda.	Atualize o modelo baixado na linha 186 do Python versão 3.6 para 3.9.

Recursos relacionados

- Criação de uma pilha no console da AWS CloudFormation
- AWS Lambda
- O que é um Classic Load Balancer?
- O que é um Application Load Balancer?
- O que é um Network Load Balancer?
- Práticas recomendadas para trabalhar com funções do AWS Lambda
- CloudFormation Melhores práticas da AWS

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Garanta que a criptografia para dados em repouso do Amazon EMR esteja habilitada no lançamento

Criado por Priyanka Chaudhary (AWS)

Resumo

Esse padrão fornece um controle de segurança para monitorar a criptografia de clusters do Amazon EMR na Amazon Web Services (AWS).

A criptografia de dados ajuda a impedir que usuários não autorizados leiam dados em um cluster e em sistemas de armazenamento físico de dados associados. Isso inclui dados que podem ser interceptados enquanto viajam pela rede, conhecidos como dados em trânsito, e dados que são salvos em mídia persistente, conhecidos como dados em repouso. Dados em repouso no Amazon Simple Storage Service (Amazon S3) podem ser criptografados de duas maneiras.

- Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
- Criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), configuradas com políticas adequadas ao Amazon EMR.

Esse controle de segurança monitora as chamadas de API e inicia um evento Amazon CloudWatch Events em RunJobFlow. O gatilho invoca o AWS Lambda, que executa um script do Python. A função recupera o ID do cluster do EMR da entrada JSON do evento e determina se há uma violação de segurança executando as seguintes verificações.

1. Verifique se um cluster do EMR está associado a uma configuração de segurança específica do Amazon EMR.
2. Se uma configuração de segurança específica do Amazon EMR estiver associada ao cluster do EMR, verifique se Encryption-at-Rest está ativada.
3. Se não Encryption-at-Rest estiver ativado, envie uma notificação do Amazon Simple Notification Service (Amazon SNS) que inclua o nome do cluster EMR, detalhes da violação, região da AWS, conta da AWS e o Lambda Amazon Resource Name (ARN) do qual essa notificação foi originada.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket S3 para o arquivo .zip do código Lambda
- Um endereço de e-mail no qual você deseja receber a notificação de violação
- O registro do Amazon EMR foi desativado para que todos os registros em log da API possam ser recuperados

Limitações

- Esse controle de detetive é regional e deve ser implantado nas regiões da AWS que você pretende monitorar.

Versões do produto

- Versão 4.8.0 do Amazon EMR e superior

Arquitetura

Pilha de tecnologias de destino

- Amazon EMR
- Evento Amazon CloudWatch Events
- Função do Lambda
- Amazon SNS

Arquitetura de destino

Automação e escala

Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

Ferramentas

- CloudFormationA AWS é um serviço que ajuda você a modelar e configurar recursos da AWS usando a infraestrutura como código.
- A Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- O Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de estruturas de big data.
- O AWS Lambda é compatível com a execução de código sem provisionar ou gerenciar servidores.
- O Amazon S3 é um serviço de armazenamento de objetos altamente escalável que pode ser usado para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- O Amazon SNS é um serviço da Web que coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

- Os EMREncryption AtRest arquivos.zip e EMREncryption AtRest .yml desse projeto estão disponíveis como anexo.

Épicos

Definir o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	No console do Amazon S3, escolha ou crie um bucket do S3 com um nome exclusivo que não contenha barras iniciais. Um nome de bucket do S3 é globalmente exclusivo , e o namespace é compartil hado por todas as contas da AWS. Seu bucket do S3	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	precisa estar na mesma região que o cluster do Amazon EMR que está sendo avaliado.	

Carregar o código do Lambda para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Carregue o código do Lambda para o bucket do S3.	Faça upload do arquivo .zip do código Lambda fornecido na seção “Anexos” para o bucket S3 definido.	Arquiteto de nuvem

Implemente o CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo da AWS.	No CloudFormation console da AWS, na mesma região do seu bucket do S3, implante o CloudFormation modelo da AWS que é fornecido como anexo a esse padrão. No próximo épico, forneça os valores para os parâmetros. Para obter mais informaçõ es sobre a implantação de CloudFormation modelos da AWS, consulte a seção “Recursos relacionados”.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Dê um nome ao bucket do S3.	Em seguida, informe o nome do bucket do S3 que você criou no primeiro épico.	Arquiteto de nuvem
Forneça a chave do Amazon S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, <diretório>/<nome do arquivo>.zip).	Arquiteto de nuvem
Forneça um endereço de e-mail.	Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS.	Arquiteto de nuvem
Defina o nível de registro em log.	Defina o nível de registro e a frequência da sua função do Lambda. “Info” (Informaç ões) designa mensagens informativas detalhadas sobre o progresso do aplicativ o. “Error” (Erro) designa eventos de erro que ainda podem permitir que o aplicativ o continue em execução. “Warning” (Aviso) designa situações potencialmente prejudiciais.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail fornecido. Você deve confirmar essa assinatura de e-mail para receber notificações de violação.	Arquiteto de nuvem

Recursos relacionados

- Criação de uma pilha no console da AWS CloudFormation
- AWS Lambda
- Opções de criptografia do Amazon EMR

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Certifique-se de que um perfil do IAM esteja associado a uma EC2 instância

Criado por Mansi Suratwala (AWS)

Resumo

Esse padrão fornece um modelo de controle de CloudFormation segurança da AWS que configura a notificação automática quando ocorre uma violação do perfil do AWS Identity and Access Management (IAM) em uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Um perfil de instância é um contêiner para uma função do IAM que você pode usar para passar informações da função para uma EC2 instância quando a instância é iniciada.

O Amazon CloudWatch Events inicia essa verificação quando a AWS CloudTrail registra chamadas de EC2 API da Amazon com base nas `ReplaceIamInstanceProfileAssociation` ações `RunInstances`, `AssociateIamInstanceProfile`, e. O gatilho chama uma função do AWS Lambda, que usa um evento Amazon CloudWatch Events para verificar um perfil do IAM.

Se um perfil do IAM não existir, a função do Lambda inicia uma notificação por e-mail do Amazon Simple Notification Service (Amazon SNS) que inclui o ID da conta do Amazon Web Services (AWS) e a região da AWS.

Se existir um perfil do IAM, a função do Lambda verifica se há entradas curinga nos documentos de política. Se as entradas de curingas existirem, inicia uma notificação de violação do Amazon SNS, que ajuda você a implementar uma segurança aprimorada. A notificação contém o nome do perfil do IAM, o evento, o ID da EC2 instância, o nome da política gerenciada, a violação, o ID da conta e a região.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da ativa
- Um bucket do Amazon Simple Storage Service (Amazon S3) para o arquivo .zip do código Lambda

Limitações

- O CloudFormation modelo da AWS deve ser implantado somente para as `ReplaceIamInstanceProfileAssociation` ações `RunInstancesAssociateIamInstanceProfile`, e.
- O controle de segurança não monitora a separação dos perfis do IAM.
- O controle de segurança não verifica a modificação das políticas do IAM que estão anexadas ao perfil do IAM da EC2 instância.
- O controle de segurança não considera permissões não suportadas em nível de recurso que exijam o uso de `"Resource":*`.

Arquitetura

Pilha de tecnologias de destino

- Amazon EC2
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Arquitetura de destino

Automação e escala

Você pode usar o CloudFormation modelo da AWS várias vezes para diferentes regiões e contas da AWS. É necessário iniciar o modelo apenas uma vez para cada conta ou região.

Ferramentas

Ferramentas

- Amazon EC2 — EC2 A Amazon fornece capacidade de computação escalável (servidores virtuais) na nuvem da AWS.

- AWS CloudTrail — CloudTrail A AWS ajuda você a viabilizar a governança, a conformidade e a auditoria operacional e de risco da sua conta da AWS. As ações realizadas por um usuário, uma função ou um serviço da AWS são registradas como eventos em CloudTrail.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- AWS Lambda: o AWS Lambda é um serviço de computação que pode ser usado para executar código sem provisionamento ou gerenciamento de servidores. O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.
- Amazon S3: o Amazon S3 fornece armazenamento de objetos com alta escalabilidade que você pode usar para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- Amazon SNS: o Amazon SNS permite que aplicativos e dispositivos enviem e recebam notificações da nuvem.

Código

- Um arquivo .zip do projeto está disponível como anexo.

Épicos

Definir o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	Para hospedar o arquivo .zip do código Lambda, escolha ou crie um bucket do S3 com um nome exclusivo que não contenha barras iniciais. Um nome de bucket do S3 é globalmente exclusivo, e o namespace é compartilhado por todas as contas da AWS. Seu bucket do S3 precisa estar na mesma região da	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	EC2 instância que está sendo avaliada.	

Carregar o código do Lambda para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Carregue o código do Lambda para o bucket do S3.	Faça o upload do código do Lambda fornecido na seção Anexos para o bucket do S3. O bucket do S3 deve estar na mesma região da EC2 instância que está sendo avaliada.	Arquiteto de nuvem

Implante o CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo da AWS.	Implante o CloudFormation modelo da AWS fornecido como anexo a esse padrão. No próximo épico, forneça os valores para os parâmetros.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Dê um nome ao bucket do S3.	Em seguida, informe o nome do bucket do S3 que você criou no primeiro épico.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
Forneça a chave do S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `<directory>/<file-name>.zip`).	Arquiteto de nuvem
Forneça um endereço de e-mail.	Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS.	Arquiteto de nuvem
Defina o nível de registro em log.	Defina o nível de registro em log e a frequência da sua função do Lambda. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo. `Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail fornecido. Você deve confirmar essa assinatura de	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	e-mail para receber notificaç ões de violação.	

Recursos relacionados

- Criar um bucket do S3
- Fazer upload de arquivos em um bucket do S3
- Usar perfis de instância
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS CloudTrail

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Garanta que um cluster do Amazon Redshift seja criptografado na criação

Criado por Mansi Suratwala (AWS)

Resumo

Esse padrão fornece um CloudFormation modelo da AWS que fornece uma notificação automática quando um novo cluster do Amazon Redshift é criado sem criptografia.

O CloudFormation modelo da AWS cria um evento Amazon CloudWatch Events e uma função do AWS Lambda. O evento observa qualquer cluster do Amazon Redshift sendo criado ou restaurado a partir de um snapshot por meio da AWS. CloudTrail Se o cluster for criado sem a criptografia do AWS Key Management Service (AWS KMS) ou do modelo de segurança de hardware na nuvem (HSM) na conta da AWS, CloudWatch iniciará uma função Lambda que envia uma notificação do Amazon Simple Notification Service (Amazon SNS) informando você sobre a violação.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma nuvem privada virtual (VPC) com um grupo de sub-redes de cluster e um grupo de segurança associado.

Limitações

- O CloudFormation modelo da AWS só pode ser implantado para as `RestoreFromClusterSnapshot` ações `CreateCluster` e.

Arquitetura

Pilha de tecnologias de destino

- Amazon Redshift
- AWS CloudTrail
- Amazon CloudWatch

- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Arquitetura de destino

Automação e escala

Você pode usar o CloudFormation modelo da AWS várias vezes para diferentes regiões e contas da AWS. Você precisa executá-lo apenas uma vez em cada região ou conta.

Ferramentas

Ferramentas

- Amazon Redshift: o Amazon Redshift é um serviço de data warehouse em escala de petabytes totalmente gerenciado na nuvem. O Amazon Redshift é integrado ao seu data lake, o que permite que você use seus dados para adquirir novos insights para seus negócios e clientes.
- AWS CloudTrail — CloudTrail A AWS é um serviço da AWS que ajuda você a implementar governança, conformidade e auditoria operacional e de risco da sua conta da AWS. As ações realizadas por um usuário, função ou serviço da AWS são registradas como eventos em CloudTrail.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- AWS Lambda: o AWS Lambda oferece suporte à execução de código sem provisionar ou gerenciar servidores. O AWS Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia a milhares por segundo.
- Amazon S3: o Amazon S3 é um serviço de armazenamento de objetos altamente escalável que você pode usar para uma grande variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- Amazon SNS: o Amazon SNS é um serviço da web que coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da web e endereços de e-mail.

Código

- Um arquivo .zip do projeto está disponível como anexo.

Épicos

Definir o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	No console do Amazon S3, escolha ou crie um bucket do S3. Esse bucket do S3 hospedará o arquivo .zip do código do Lambda. Seu bucket do S3 precisa estar na mesma região do cluster do Amazon Redshift que está sendo avaliado. O nome do bucket do S3 não pode conter barras iniciais.	Arquiteto de nuvem

Carregar o código do Lambda para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Carregue o código do Lambda para o bucket do S3.	Faça o upload do código do Lambda fornecido na seção Anexos no bucket do S3. O bucket dp Amazon S3 deve estar na mesma região que o cluster do Amazon Redshift avaliado.	Arquiteto de nuvem

Implante o CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo da AWS.	Implante o CloudFormation modelo da AWS fornecido	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	como anexo a esse padrão. No próximo épico, forneça os valores para os parâmetros.	

Preencha os parâmetros no CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Dê um nome ao bucket do S3.	Em seguida, informe o nome do bucket do S3 que você criou no primeiro épico.	Arquiteto de nuvem
Forneça a chave do S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `<directory>/<file-name>.zip`).	Arquiteto de nuvem
Forneça um endereço de e-mail.	Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS.	Arquiteto de nuvem
Defina o nível de registro em log.	Defina o nível de registro em log e a frequência da sua função do Lambda. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo. `Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o modelo é implantado com sucesso, ele envia um e-mail de assinatura para o endereço de e-mail fornecido. Você deve confirmar essa assinatura de e-mail para receber notificações de violação.	Arquiteto de nuvem

Recursos relacionados

- Criar um bucket do S3
- Fazer upload de arquivos em um bucket do S3
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS CloudTrail
- Criar um cluster do Amazon Redshift

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Exporte um relatório das identidades do AWS IAM Identity Center e suas atribuições usando PowerShell

Criado por Jorge Pava (AWS), Chad Miles (AWS), Frank Allotta (AWS) e Manideep Reddy Gillela (AWS)

Resumo

Quando você usa o Centro de Identidade do AWS IAM [(sucessor do AWS autenticação única (SSO)] para gerenciar centralmente a autenticação única (SSO) a todas as suas contas e aplicativos na nuvem da Amazon Web Services (AWS), relatar e auditar essas atribuições por meio do Console de Gerenciamento da AWS pode ser entediante e demorado. Isso é especialmente verdadeiro se você estiver relatando permissões para um usuário ou grupo em dezenas ou centenas de contas da AWS.

Para muitos, a ferramenta ideal para visualizar essas informações seria em um aplicativo de planilhas, como o Microsoft Excel. Isso pode ajudar você a filtrar, pesquisar e visualizar os dados de toda a sua organização, gerenciados pelo AWS Organizations.

Esse padrão descreve como usar as ferramentas da AWS PowerShell para gerar um relatório das configurações de identidade de SSO no IAM Identity Center. O relatório é formatado como um arquivo CSV e inclui o nome da identidade (principal), o tipo de identidade (usuário ou grupo), as contas que a identidade pode acessar e os conjuntos de permissões. Depois de gerar esse relatório, você pode abri-lo em seu aplicativo preferido para pesquisar, filtrar e auditar os dados conforme necessário. A imagem a seguir mostra dados de amostra em um aplicativo de planilha.

> **Important**
>
> Como esse relatório contém informações confidenciais, é altamente recomendável que você as armazene com segurança e as compartilhe somente de forma específica. need-to-know

Pré-requisitos e limitações

Pré-requisitos

- Centro de Identidade IAM e AWS Organizations, configurados e habilitados.
- PowerShell, instalado e configurado. Para obter mais informações, consulte Instalando PowerShell (documentação da Microsoft).
- AWS Tools para PowerShell, instaladas e configuradas. Por motivos de desempenho, é altamente recomendável que você instale a versão modularizada do AWS Tools for PowerShell, chamada. `AWS.Tools` Cada serviço da AWS é compatível com seu próprio módulo individual pequeno. No PowerShell shell, insira os seguintes comandos para instalar os módulos necessários para esse padrão: `AWS.Tools.Installer` `OrganizationsSSOAdmin`,, `IdentityStore` e.

```
Install-Module AWS.Tools.Installer
Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore
```

  Para obter mais informações, consulte Instalar o AWS.Tools no Windows ou Instalar o AWS.Tools no Linux ou macOS (AWS Tools para documentação). PowerShell Se você receber um erro ao instalar os módulos, consulte a seção Solução de problemas desse padrão.
- A AWS Command Line Interface (AWS CLI) ou o AWS SDK devem ser previamente configurados com credenciais de trabalho de uma das seguintes maneiras:
  - Usar a AWS CLI `aws configure` Para obter mais informações, consulte Configuração rápida (documentação da AWS CLI).
  - Configure a AWS CLI ou o AWS Cloud Development Kit (AWS CDK) para obter acesso temporário por meio de um perfil do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Obter credenciais de perfil do IAM para acesso à CLI (documentação do Centro de Identidade IAM).
- Um perfil nomeado para a AWS CLI que salvou as credenciais de uma entidade principal do IAM que:
  - Tem acesso à conta de gerenciamento do AWS Organizations ou à conta de administrador delegado do Centro de Identidade IAM
  - `AWSSSOReadOnly` e as políticas gerenciadas pela AWS `AWSSSODirectoryReadOnly` foram aplicadas a ele?

  Para obter mais informações, consulte Uso de perfis nomeados (documentação da AWS CLI) e Políticas gerenciadas pela AWS (documentação do IAM).

Limitações

- As contas de destino da AWS devem ser gerenciadas como uma organização no AWS Organizations.

Versões do produto

- Para todos os sistemas operacionais, é recomendável usar a PowerShell versão 7.0 ou posterior.

Arquitetura

Arquitetura de destino

1. O usuário executa o script em uma linha de PowerShell comando.
2. O script assume o perfil nomeado para a AWS CLI. Isso concede acesso ao Centro de identidade IAM.
3. O script recupera as configurações de identidade de SSO do Centro de identidade IAM.
4. O script gera um arquivo CSV no mesmo diretório na estação de trabalho local em que o script é salvo.

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O Centro de Identidade do AWS IAM ajuda você a gerenciar centralmente o acesso à autenticação única (SSO) a todas as suas contas e aplicativos na nuvem da AWS.
- As ferramentas da AWS para PowerShell são um conjunto de PowerShell módulos que ajudam você a criar scripts de operações em seus recursos da AWS a partir da linha de PowerShell comando.

Outras ferramentas

- PowerShellé um programa de gerenciamento de automação e configuração da Microsoft executado em Windows, Linux e macOS.

Épicos

Gerar o relatório

Tarefa	Descrição	Habilidades necessárias
Preparar o script.	1. Copie o PowerShell script na seção Informações adicionais desse padrão. 2. Na seção `Param`, no seu ambiente da AWS, defina os valores para as seguintes variáveis: • `OutputFile` : nome do relatório. • `ProfileName` : perfil nomeado da AWS CLI que você deseja usar para gerar o relatório. • `Region`: a região da AWS na qual o Centro de Identidade IAM está implantado. Para obter uma lista completa de regiões e seus códigos, consulte Endpoints regionais. 3. Salve o script com o nome de arquivo `SSO-Report.ps1` .	Administrador de nuvem
Executar o script.	É recomendável que você execute seu script personalizado no PowerShell shell com o comando a seguir.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	`.\SSO-Report.ps1`
	
	Como alternativa, você pode executar o script de outro shell digitando o comando a seguir.
	
	`pwsh .\SSO-Report.ps1`
	
	O script gera um arquivo CSV no mesmo diretório do arquivo de script.	

Analisar os dados do relatório.	O arquivo CSV de saída tem os cabeçalhos AccountNa mePermissionSet, Principal e Tipo. Abra esse arquivo no aplicativo de planilhas de sua preferência. Você pode criar uma tabela de dados para filtrar e classificar a saída.	Administrador de nuvem

Solução de problemas

Problema	Solução
Erro `The term 'Get-<parameter>' is not recognized as the name of a cmdlet, function, script file, or operable program.`	O AWS Tools for PowerShell ou seus módulos não estão instalados. No PowerShell shell, insira os seguintes comandos para instalar o AWS Tools PowerShell e os módulos necessári os para esse padrão: `AWS.Tools.Installe r Organizations SSOAdmin`,, `IdentityS tore e`. `Install-Module AWS.Tools.Installer`

Problema	Solução
	`Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore`
Erro `No credentials specified or obtained from persisted/shell defaults`	Em Preparar o script na seção Épicos, confirme se você inseriu corretamente as variáveis `ProfileName` e `Region`. Certifique-se de que as configurações e credenciais no perfil nomeado tenham permissões suficientes para administrar o Centro de Identidade IAM.
Erro `Authenticode Issuer …` ao instalar os módulos das ferramentas da AWS	Adicione o parâmetro `-SkipPublisherCheck` no fim do comando `Install-AWSToolsModule` .

Erro `Get-ORGAccountList : Assembly AWSSDK.SSO could not be found or loaded.`	Esse erro pode ocorrer quando perfis nomeados da AWS CLI são especificados, a AWS CLI é configurado para autenticar usuários com o Centro de Identidade IAM e a AWS CLI está configurado para recuperar automaticamente tokens de autenticação atualizados. Para corrigir esse erro, faça o seguinte:
	1. Digite o comando a seguir para confirmar se os módulos `SSO` e `SSOOIDC` estão instalados.
	`Install-AWSToolsModule SSO, SSOOIDC`
	2. Insira as linhas a seguir no script abaixo do bloco `param()`.
	`Import-Module AWS.Tools.SSO`
	`Import-Module AWS.Tools.SSOOIDC`

Recursos relacionados

- Onde as definições de configuração ficam armazenadas? (Documentação da AWS CLI)
- Configurar a AWS CLI para usar o Centro de Identidade do AWS IAM (documentação da AWS CLI)
- Usar perfis nomeados (documentação da AWS CLI)

Mais informações

No script a seguir, determine se você precisa atualizar os valores dos seguintes parâmetros:

- Se você estiver usando um perfil nomeado na AWS CLI para acessar a conta na qual o Centro de Identidade IAM está configurado, atualize o valor `$ProfileName`.
- Se o Centro de Identidade IAM for implantado em uma região da AWS diferente da região padrão para sua configuração da AWS CLI ou do AWS SDK, atualize o valor `$Region` para usar a região em que o Centro de Identidade IAM está implantado.
- Se nenhuma dessas situações se aplicar, nenhuma atualização de script será necessária.

```
param (
    # The name of the output CSV file
    [String] $OutputFile  = "SSO-Assignments.csv",
    # The AWS CLI named profile
    [String] $ProfileName = "",
    # The AWS Region in which IAM Identity Center is configured
    [String] $Region      = ""
)
$Start = Get-Date; $OrgParams = @{}
If ($Region){ $OrgParams.Region = $Region}
if ($ProfileName){$OrgParams.ProfileName = $ProfileName}
$SSOParams   = $OrgParams.Clone(); $IdsParams = $OrgParams.Clone()
$AccountList = Get-ORGAccountList @OrgParams | Select-Object Id, Name
$SSOinstance = Get-SSOADMNInstanceList @OrgParams
$SSOParams['InstanceArn']       = $SSOinstance.InstanceArn
$IdsParams['IdentityStoreId']   = $SSOinstance.IdentityStoreId
$PSsets       = @{}; $Principals   = @{}
$Assignments  = @(); $AccountCount = 1; Write-Host ""
foreach ($Account in $AccountList) {
```

```
    $Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
    Write-Host "`r$Duration - Account $AccountCount of $($AccountList.Count)
 (Assignments:$($Assignments.Count))        " -NoNewline
    $AccountCount++
    foreach ($PS in Get-SSOADMNPermissionSetsProvisionedToAccountList -AccountId
 $Account.Id @SSOParams) {
        if (-not $PSsets[$PS]) {$PSsets[$PS] = (Get-SSOADMNPermissionSet @SSOParams -
PermissionSetArn $PS).Name;$APICalls++}
        $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id
        if ($AssignmentsResponse.NextToken) {$AccountAssignments =
 $AssignmentsResponse.AccountAssignments}
        else {$AccountAssignments = $AssignmentsResponse}
        While ($AssignmentsResponse.NextToken) {
            $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id -NextToken $AssignmentsResponse.NextToken
            $AccountAssignments += $AssignmentsResponse.AccountAssignments}
        foreach ($Assignment in $AccountAssignments) {
            if (-not $Principals[$Assignment.PrincipalId]) {
                $AssignmentType = $Assignment.PrincipalType.Value
                $Expression     = "Get-IDS"+$AssignmentType+" @IdsParams -"+
$AssignmentType+"Id "+$Assignment.PrincipalId
                $Principal      = Invoke-Expression $Expression
                if ($Assignment.PrincipalType.Value -eq "GROUP")
 { $Principals[$Assignment.PrincipalId] = $Principal.DisplayName }
                else { $Principals[$Assignment.PrincipalId] = $Principal.UserName }
            }
            $Assignments += [PSCustomObject]@{
                AccountName     = $Account.Name
                PermissionSet   = $PSsets[$PS]
                Principal       = $Principals[$Assignment.PrincipalId]
                Type            = $Assignment.PrincipalType.Value}
        }
    }
}
$Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
Write-Host "`r$($AccountList.Count) accounts done in $Duration. Outputting result to
 $OutputFile"
$Assignments | Sort-Object Account | Export-CSV -Path $OutputFile -Force
```

Monitorar e corrigir a exclusão programada das chaves do AWS KMS

Criado por Mikesh Khanal (AWS) e Ramya Pulipaka (AWS)

Resumo

Na nuvem da Amazon Web Services (AWS), a exclusão de uma chave do AWS Key Management Services (AWS KMS) pode resultar na perda de dados. A exclusão remove o material de chave e todos os metadados associados à chave do AWS KMS e é irreversível. Depois que uma chave do AWS KMS é excluída, não é mais possível descriptografar os dados que foram criptografados com aquela chave do AWS KMS, o que significa que os dados são irrecuperáveis.

Este padrão configura o monitoramento, com notificações, quando um aplicativo ou um usuário programa a exclusão de uma chave do AWS KMS. Se você receber essa notificação, convém cancelar a exclusão da chave do AWS KMS e reconsiderar sua decisão de excluí-la. O padrão usa o runbook de automação do AWS Systems Manager AWSConfigRemediation-CancelKeyDeletionpara facilitar o cancelamento da exclusão de uma chave do AWS KMS.

> **Note**
>
> O CloudFormation modelo do padrão deve ser implantado em todas as regiões da AWS nas quais você deseja monitorar a exclusão das chaves do AWS KMS.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Compreensão dos seguintes serviços da AWS:
  - Amazon EventBridge
  - AWS KMS
  - Amazon Simple Notification Service (Amazon SNS)
  - AWS Systems Manager

Limitações

- Qualquer personalização da solução requer conhecimento dos CloudFormation modelos da AWS e dos serviços da AWS usados nesse padrão.
- Atualmente, esta solução usa o barramento de eventos padrão e pode ser personalizada de acordo com os requisitos. Para obter mais informações sobre o barramento de eventos personalizado, consulte a documentação do AWS.

Arquitetura

Pilha de tecnologias de destino

- Amazon EventBridge
- AWS KMS
- Amazon SNS
- AWS Systems Manager
- Automação usando o seguinte:
  - AWS Command Line Interface (AWS CLI) ou AWS SDK
  - Pilha da AWS CloudFormation

Arquitetura de destino

1. A exclusão de uma chave do AWS KMS está programada.
2. O evento de exclusão programada é avaliado por uma regra. EventBridge
3. A EventBridge regra envolve o tópico do Amazon SNS.
4. A EventBridge regra inicia a automação e os runbooks do Systems Manager.
5. Os runbooks cancelam a exclusão.

Automação e escala

A CloudFormation pilha implanta todos os recursos e serviços necessários para que essa solução funcione. O padrão pode ser executado de forma independente em uma única conta ou executado usando a AWS CloudFormation StackSets para várias contas independentes ou uma organização.

```
aws cloudformation create-stack --stack-name  <stack-name>\
    --template-body file://<Full-Path-of-file> \
```

```
    --parameters ParameterKey=,ParameterValue= \
    --capabilities CAPABILITY_NAMED_IAM
```

Ferramentas

Ferramentas

- AWS CloudFormation — CloudFormation A AWS é um serviço que ajuda você a modelar e configurar seus recursos da Amazon Web Services para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos executados na AWS. Você pode usar um CloudFormation modelo para criar pilhas em uma conta da AWS em uma região da AWS. O modelo descreve todos os recursos da AWS que você deseja e CloudFormation provisiona e configura esses recursos para você.
- AWS CLI: a AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que você pode usar para interagir com serviços da AWS usando comandos no seu shell da linha de comando.
- Amazon EventBridge — EventBridge A Amazon é um serviço de ônibus de eventos sem servidor que conecta seus aplicativos a dados de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos e serviços da AWS e encaminha esses dados para destinos como o AWS Lambda. EventBridge simplifica o processo de criação de arquiteturas orientadas por eventos.
- AWS KMS: o AWS Key Management Service (AWS KMS) é um serviço gerenciado para criar e controlar chaves do AWS KMS, que são as chaves de criptografia usadas para criptografar seus dados.
- AWS SDKs — As ferramentas da AWS incluem SDKs para que você possa desenvolver e gerenciar aplicativos na AWS na linguagem de programação de sua escolha.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens de editores para assinantes (também conhecido como produtores e consumidores). Os publicadores se comunicam de maneira assíncrona com os assinantes produzindo e enviando mensagens para um tópico, que é um canal de comunicação e um ponto de acesso lógico.
- AWS Systems Manager: o AWS Systems Manager é um serviço da AWS que você pode usar para visualizar e controlar sua infraestrutura na AWS. Usando o console do Systems Manager, você pode automatizar tarefas operacionais nos recursos da AWS. O Systems Manager ajuda você a manter a segurança e a conformidade verificando suas instâncias gerenciadas e gerando relatórios (ou tomando medidas corretivas) sobre quaisquer violações de políticas detectadas.

Código

- O `alerting_ct_logs.yaml` CloudFormation modelo do projeto está anexado.

Épicos

Preparação da conta da AWS

Tarefa	Descrição	Habilidades necessárias
Instale e configure AWS CLI.	Instale a versão 2 da AWS CLI. Em seguida, defina as configurações de credencia is de segurança para uma identidade, o formato de saída padrão e a região padrão da AWS que a AWS CLI usa para interagir com a AWS. A identidade deve ter as permissões necessárias para realizar as tarefas.	Desenvolvedor, engenheiro de segurança

Implemente o CloudFormation modelo da AWS

Tarefa	Descrição	Habilidades necessárias
Faça o download do CloudFormation modelo.	Baixe o anexo para um caminho local em seu computador e extraia o arquivo do modelo `alerting_ct_logs.y aml` .	Desenvolvedor, engenheiro de segurança
Implante o modelo.	Na janela do terminal em que o perfil da conta da AWS	Desenvolvedor, engenheiro de segurança

Tarefa	Descrição	Habilidades necessárias
	foi configurado, execute o comando a seguir. `aws cloudformation create-stack --stack-name <stack_name> \ --capabilities <Value> \ --template-body file://<Full_Path> \ --parameters ParameterKey=DestinationEmailAddress,ParameterValue=<Value> \ ParameterKey=SNSTopicName,ParameterValue=<Value> \ ParameterKey=EnableRemediation ,ParameterValue=<Value> \ ParameterKey=AutomationAssumeRole, ParameterValue=<Value>` No próximo tópico, forneça valores para os parâmetros do modelo.	

Tarefa	Descrição	Habilidades necessárias
Preencha os parâmetros no modelo.	Informe os valores necessários para os parâmetros. • `DestinationEmailAddress` : o endereço de e-mail para receber um alerta quando uma chave do AWS KMS estiver programada para exclusão. • `SNSTopicName` : o nome do tópico do Amazon SNS. • `EnableRemediation` : o cancelamento da exclusão programada da chave usando um runbook do Systems Manager. Os valores permitidos são `true` e `false`. • `AutomationAssumeRole` : o nome do recurso da Amazon (ARN) da função que permite que a automação do Systems Manager realize ações em seu nome. Para obter mais informações, consulte a seção Permissões obrigatórias do IAM na AWSConfigRemediation-CancelKeyDeletiondocumentação. • `Capabilities` — Para CloudFormation que a AWS crie a pilha, você deve reconhecer explicita	Desenvolvedor, engenheiro de segurança

Tarefa	Descrição	Habilidades necessárias
	mente que seu modelo de pilha contém determinados recursos.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Verifique sua caixa de entrada de e-mail e escolha Confirmar a assinatura na mensagem de e-mail que você recebe do Amazon SNS. A janela do navegador da Web abrirá e exibirá uma confirmação de assinatura com seu ID de assinatura.	Desenvolvedor, engenheiro de segurança

Recursos relacionados

Referências

- Criação de uma regra para um serviço da AWS
- Criação de um CloudWatch alarme da Amazon para detectar o uso de uma chave do AWS KMS que está pendente de exclusão

Tutoriais e vídeos

- Como começar a usar a Amazon EventBridge
- Mergulhe na Amazon EventBridge (palestras técnicas on-line da AWS)

workshop da AWS

- Trabalhando com EventBridge regras

Mais informações

O código a seguir fornece exemplos de como estender a solução para monitorar e notificar você sobre quaisquer alterações realizadas em qualquer serviço da AWS. Os exemplos incluem padrões predefinidos e personalizados. Para obter mais informações, consulte Eventos e padrões de eventos em EventBridge.

```
EventPattern:
        source:
        - aws.kms
        detail-type:
        - AWS API Call via CloudTrail
        detail:
          eventSource:
          - kms.amazonaws.com
          eventName:
          - ScheduleKeyDeletion
```

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Identifique buckets públicos do Amazon S3 usando o Security AWS Organizations Hub

Criado por Mourad Cherfaoui (AWS), Arun Chandapillai (AWS) e Parag Nagwekar (AWS)

Resumo

Esse padrão mostra como criar um mecanismo para identificar buckets públicos do Amazon Simple Storage Service (Amazon S3) em suas contas. AWS Organizations O mecanismo funciona usando controles do padrão AWS Foundational Security Best Practices (FSBP) AWS Security Hub para monitorar os buckets do Amazon S3. Você pode usar EventBridge a Amazon para processar as descobertas do Security Hub e depois publicá-las em um tópico do Amazon Simple Notification Service (Amazon SNS). As partes interessadas em sua organização podem se inscrever no tópico e receber notificações imediatas por e-mail sobre as descobertas.

Os novos buckets do Amazon S3 e seus objetos não permitem acesso público por padrão. Você pode usar esse padrão em cenários em que você deve modificar as configurações padrão do Amazon S3 com base nos requisitos da sua organização. Por exemplo, esse pode ser um cenário em que você tem um bucket do Amazon S3 que hospeda um site público ou arquivos que todos na Internet devem ser capazes de ler do seu bucket do Amazon S3.

O Security Hub geralmente é implantado como um serviço central para consolidar todas as descobertas de segurança, incluindo aquelas relacionadas a padrões de segurança e requisitos de conformidade. Há outros Serviços da AWS que você pode usar para detectar buckets públicos do Amazon S3, mas esse padrão usa uma implantação existente do Security Hub com configuração mínima.

Pré-requisitos e limitações

Pré-requisitos

- Uma configuração AWS de várias contas com uma conta de administrador dedicada do Security Hub
- Security Hub e AWS Config, habilitado no Região da AWS que você deseja monitorar

> **Note**
>
> Você deve habilitar a agregação entre regiões no Security Hub se quiser monitorar várias regiões de uma única região de agregação.

- Permissões de usuário para acessar e atualizar a conta de administrador do Security Hub, acesso de leitura a todos os buckets do Amazon S3 na organização e permissões para desativar o acesso público (se necessário)

Arquitetura

O diagrama a seguir mostra uma arquitetura para usar o Security Hub para identificar buckets públicos do Amazon S3.

O diagrama mostra o seguinte fluxo de trabalho:

1. O Security Hub monitora a configuração dos buckets do Amazon S3 em todas as AWS Organizations contas (incluindo a conta do administrador) usando os controles S3.2 e S3.3 do padrão de segurança FSBP e detecta uma descoberta se um bucket está configurado como público.
2. A conta de administrador do Security Hub acessa as descobertas (incluindo aquelas para S3.2 e S3.3) de todas as contas de membros.
3. O Security Hub envia automaticamente todas as novas descobertas e todas as atualizações das descobertas existentes EventBridge como eventos importados do Security Hub Findings. Isso inclui eventos para descobertas das contas do administrador e do membro.
4. Uma EventBridge regra filtra as descobertas do S3.2 e do S3.3 que têm um `ComplianceStatus` de`FAILED`, um status de fluxo de trabalho de `NEW` e um `RecordState` de. `ACTIVE`
5. As regras usam os padrões de eventos para identificar eventos e enviá-los para um tópico do Amazon SNS após a correspondência.
6. Um tópico do Amazon SNS envia os eventos para seus assinantes (por e-mail, por exemplo).
7. Os analistas de segurança designados para receber as notificações por e-mail analisam o bucket Amazon S3 em questão.
8. Se o bucket for aprovado para acesso público, o analista de segurança definirá o status do fluxo de trabalho da descoberta correspondente no Security Hub como `SUPPRESSED`. Caso contrário,

o analista define o status como `NOTIFIED`. Isso elimina futuras notificações para o bucket do Amazon S3 e reduz o ruído das notificações.

9. Se o status do fluxo de trabalho estiver definido como `NOTIFIED`, o analista de segurança analisará a descoberta com o proprietário do bucket para determinar se o acesso público é justificado e está em conformidade com os requisitos de privacidade e proteção de dados. A investigação resulta na remoção do acesso público ao bucket ou na aprovação do acesso público. No último caso, o analista de segurança define o status do fluxo de trabalho como `SUPPRESSED`.

> **Note**
>
> O diagrama de arquitetura se aplica a implantações de agregação de uma única região e entre regiões. Nas contas A, B e C do diagrama, o Security Hub pode pertencer à mesma região da conta do administrador ou pertencer a regiões diferentes se a agregação entre regiões estiver ativada.

Ferramentas

- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos de software como serviço (SaaS) e. Serviços da AWS EventBridge roteia esses dados para destinos, como tópicos e AWS Lambda funções do Amazon SNS, se os dados corresponderem às regras definidas pelo usuário.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS. O Security Hub também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança. O Security Hub coleta dados de segurança de vários Contas da AWS serviços e produtos de parceiros terceirizados compatíveis e, em seguida, ajuda a analisar as tendências de segurança e identificar os problemas de segurança de maior prioridade.

Épicos

Configurar contas do Security Hub

Tarefa	Descrição	Habilidades necessárias
Ative o Security Hub nas AWS Organizations contas.	Para habilitar o Security Hub nas contas da organização em que você deseja monitorar buckets do Amazon S3, consulte as diretrizes em Designação de uma conta de administrador do Security Hub (console) e Gerenciamento de contas de membros que pertencem a uma organização na documentação do Security Hub.	Administrador da AWS
(Opcional) Habilitar a agregação entre regiões.	Se você quiser monitorar buckets do Amazon S3 em várias regiões de uma única região, configure a agregação entre regiões.	Administrador da AWS
Ative os controles do S3.2 e S3.3 para o padrão de segurança FSBP.	Você deve habilitar os controles do S3.2 e S3.3 para o padrão de segurança FSBP. 1. Para ativar os controles do S3.2, siga as instruções do [S3.2]. Os buckets do S3 devem proibir o acesso público de leitura na documentação do Security Hub. 2. Para habilitar os controles do S3.3, siga as instruçõe	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	s de [3] Os buckets do S3 devem proibir o acesso público de gravação na documentação do Security Hub.	

Configurar o ambiente

Tarefa	Descrição	Habilidades necessárias
Configure o tópico e a assinatura de e-mail do Amazon SNS.	1. Faça login no AWS Management Console e abra o console do Amazon SNS. 2. No painel de navegação, selecione Topics (Tópicos) e Create topic (Criar tópico). 3. Em Tipo, escolha Padrão. 4. Em Nome, insira um nome para o seu tópico (por exemplo, public-s3-buckets). 5. Escolha Criar tópico. 6. Na guia Subscriptions (Assinaturas) para o seu tópico, escolha Create subscription (Criar assinatura). 7. Em Protocol (Protocolo), selecione Email. 8. Em Endpoint, insira o endereço de e-mail que	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	receberá as notificações. Você pode usar o endereço de e-mail de um AWS administrador, profissional de TI ou profissional da Infosec. 9. Selecione Criar assinatura. Para criar assinaturas de e-mail adicionais, repita as etapas 6 a 8 conforme necessário.	

Tarefa	Descrição	Habilidades necessárias
Configure a EventBridge regra.	1. Abra o console de EventBridge . 2. Na seção Começar, selecione EventBridge Regra e, em seguida, escolha Criar regra. 3. Na página Definir detalhes da regra, em Nome, insira um nome para sua regra (por exemplo, public-s3-buckets). Escolha Próximo. 4. Na seção Event patter (Padrão de evento), selecione Edit pattern (Editar padrão). 5. Copie o código a seguir, cole-o no editor de código do Padrão de eventos e escolha Avançar. `{ "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Compliance": { "Status": ["FAILED"] }, "RecordState": ["ACTIVE"], "Workflow": {`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	<pre>"Status": ["NEW"] }, "ProductFields": { "ControlId": ["S3.2", "S3.3"] } } }</pre> 6. Na página Selecionar destino(s), em Selecionar um destino, selecione Tópico do SNS como o destino e, em seguida, selecione o tópico que você criou anteriormente. 7. Escolha Avançar, escolha Avançar novamente e, em seguida, escolha Criar regra.	

Solução de problemas

Problema	Solução
Eu tenho um bucket do Amazon S3 com acesso público ativado, mas não estou recebendo notificações por e-mail sobre ele.	Isso pode ocorrer porque o bucket foi criado em outra região e a agregação entre regiões não está habilitada na conta de administrador do Security Hub. Para resolver esse problema, habilite a agregação entre regiões ou implemente a solução desse padrão na região em que seu bucket do Amazon S3 reside atualmente.

Recursos relacionados

- O que AWS Security Hubé (Documentação do Security Hub)
- AWS Padrão Foundational Security Best Practices (FSBP) (documentação do Security Hub)
- AWS Security Hub scripts de ativação de várias contas (AWS Labs)
- Práticas recomendadas de segurança para o Amazon S3 (documentação do Amazon S3)

Mais informações

Fluxo de trabalho para monitorar buckets públicos do Amazon S3

O fluxo de trabalho a seguir ilustra como você pode monitorar os buckets públicos do Amazon S3 em sua organização. O fluxo de trabalho pressupõe que você concluiu as etapas no tópico Configurar o Amazon SNS e na história de assinatura de e-mail desse padrão.

1. Você recebe uma notificação por e-mail quando um bucket do Amazon S3 é configurado com acesso público.
   - Se o bucket for aprovado para acesso público, defina o status do fluxo de trabalho da descoberta correspondente como `SUPPRESSED` na conta de administrador do Security Hub. Isso impede que o Security Hub emita mais notificações para esse bucket e pode eliminar alertas duplicados.
   - Se o bucket não for aprovado para acesso público, defina o status do fluxo de trabalho da descoberta correspondente na conta de administrador do Security Hub como `NOTIFIED`. Isso impede que o Security Hub emita mais notificações para esse bucket a partir do Security Hub e pode eliminar ruído.
2. Caso o bucket possa conter dados confidenciais, desative o acesso público imediatamente até que a análise seja concluída. Se você desativar o acesso público, o Security Hub alterará o status do fluxo de trabalho para `RESOLVED`. Em seguida, envie notificações por e-mail sobre a interrupção do bucket.
3. Encontre o usuário que configurou o bucket como público (por exemplo, usando AWS CloudTrail) e inicie uma análise. A análise resulta na remoção do acesso público ao bucket ou na aprovação do acesso público. Se o acesso público for aprovado, defina o status do fluxo de trabalho da descoberta correspondente como `SUPPRESSED`.

Ingira e analise os registros de segurança da AWS no Microsoft Sentinel

Criado por Ivan Girardi (AWS) e Sebastian Wenzel (AWS)

Resumo

Esse padrão descreve como automatizar a ingestão de registros de AWS segurança, como registros, dados do Amazon AWS CloudTrail Logs, dados do Amazon VPC Flow CloudWatch Logs e descobertas da Amazon GuardDuty , no Microsoft Sentinel. Se sua organização usa o Microsoft Sentinel como um sistema de gerenciamento de eventos e informações de segurança (SIEM), isso ajuda você a monitorar e analisar centralmente os registros para detectar eventos relacionados à segurança. Assim que os registros estiverem disponíveis, eles serão automaticamente entregues a um bucket do Amazon Simple Storage Service (Amazon S3) em menos de 5 minutos. Isso pode ajudá-lo a detectar rapidamente eventos de segurança em seu AWS ambiente.

O Microsoft Sentinel ingere CloudTrail registros em um formato tabular que inclui a data e hora original de quando o evento foi gravado. A estrutura dos registros ingeridos permite recursos de consulta usando a Kusto Query Language no Microsoft Sentinel.

O padrão implanta uma solução de monitoramento e alerta que detecta falhas de ingestão em menos de 1 minuto. Também inclui um sistema de notificação que o SIEM externo pode monitorar. Você usa AWS CloudFormation para implantar os recursos necessários na conta de registro.

Público-alvo

Esse padrão é recomendado para usuários com experiência com AWS Control Tower, AWS Organizations, CloudFormation, AWS Identity and Access Management (IAM) e AWS Key Management Service (AWS KMS).

Pré-requisitos e limitações

Pré-requisitos

A seguir estão os pré-requisitos para implantar essa solução:

- Ativos Contas da AWS que são gerenciados como uma organização AWS Organizations e fazem parte de uma AWS Control Tower landing zone. A organização deve incluir uma conta dedicada para registro. Para obter instruções, consulte Criação e configuração de uma organização na AWS Organizations documentação.

- Uma CloudTrail trilha que registra eventos de toda a organização e armazena os registros em um bucket do Amazon S3 na conta de registro. Para obter instruções, consulte Criação de uma trilha para uma organização.
- Na conta de registro, permissões para assumir uma função existente do IAM que tenha as seguintes permissões:
  - Implante os recursos definidos no CloudFormation modelo fornecido.
  - Implante o CloudFormation modelo fornecido.
  - Modifique a política de AWS KMS chaves se os registros forem criptografados com uma chave gerenciada pelo cliente.
- AWS Command Line Interface (AWS CLI), instalado e configurado.
- Uma conta do Microsoft Azure com uma assinatura para usar o Microsoft Sentinel.
- Ative e configure o Microsoft Sentinel. Para obter instruções, consulte Habilitar o Microsoft Sentinel e os recursos e conteúdos iniciais na documentação do Microsoft Sentinel.
- Atenda aos pré-requisitos para configurar o conector Microsoft Sentinel S3.

Limitações

- Essa solução encaminha os registros de segurança de um bucket do Amazon S3 na conta de registro para o Microsoft Sentinel. As instruções sobre como enviar os registros para o Amazon S3 não são fornecidas explicitamente.
- Esse padrão fornece instruções para implantação em um AWS Control Tower landing zone. No entanto, o uso de não AWS Control Tower é necessário.
- Essa solução é compatível com um ambiente em que o bucket de registro do Amazon S3 é restrito às políticas de controle de serviço (SCPs), como Proibir alterações na política de bucket para buckets criados do Amazon AWS Control Tower S3 no arquivo de log.
- Esse padrão fornece instruções para o encaminhamento de CloudTrail registros, mas você pode adaptar essa solução para enviar outros registros compatíveis com o Microsoft Sentinel, como registros de Logs CloudWatch , Amazon VPC Flow Logs e. GuardDuty
- As instruções usam o AWS CLI para implantar o CloudFormation modelo, mas você também pode usar AWS Management Console o. Para obter instruções, consulte Usando o AWS CloudFormation console. Se você usar o console para implantar a pilha, implante a pilha da Região da AWS mesma forma que o bucket de registro.
- Essa solução implanta uma fila do Amazon Simple Queue Service (Amazon SQS) para entregar notificações do Amazon S3. A fila contém mensagens com os caminhos dos objetos carregados

no bucket do Amazon S3, não com dados reais. A fila usa criptografia SSE-SQS para ajudar a proteger o conteúdo das mensagens. Se quiser criptografar a fila SQS com o SSE-KMS, você pode usar uma chave KMS gerenciada pelo cliente. Para obter mais informações, consulte Criptografia em repouso no Amazon SQS.

Arquitetura

Esta seção fornece uma visão geral de alto nível da arquitetura que o código de amostra estabelece. O diagrama a seguir mostra os recursos implantados na conta de registro para ingerir registros de um bucket existente do Amazon S3 no Microsoft Sentinel.

O diagrama da arquitetura mostra as seguintes interações de recursos:

1. Na conta de registro, o Microsoft Sentinel assume uma função do IAM por meio do OpenID Connect (OIDC) para acessar registros em um bucket específico do Amazon S3 e na fila do Amazon SQS.
2. O Amazon Simple Notification Service (Amazon SNS) e o Amazon S3 usam para criptografia. AWS KMS
3. O Amazon S3 envia mensagens de notificação para a fila do Amazon SQS sempre que recebe novos registros.
4. O Microsoft Sentinel verifica se há novas mensagens no Amazon SQS. A fila do Amazon SQS usa criptografia SSE-SQS. O período de retenção de mensagens está definido para 14 dias.
5. O Microsoft Sentinel extrai mensagens da fila do Amazon SQS. As mensagens contêm o caminho dos objetos Amazon S3 carregados. O Microsoft Sentinel ingere esses objetos do bucket do Amazon S3 na conta do Microsoft Azure.
6. Um CloudWatch alarme monitora a fila do Amazon SQS. Se as mensagens não forem recebidas e excluídas da fila do Amazon SQS em 5 minutos, ele iniciará uma notificação do Amazon SNS que enviará um e-mail.

AWS Control Tower ajuda você a configurar a estrutura da unidade organizacional fundamental (OU) e centraliza CloudTrail os registros na conta de registro. Ele também implementa SCPs a obrigatoriedade de proteger o bucket de registro.

Fornecemos a arquitetura do alvo em um AWS Control Tower landing zone, mas isso não é estritamente necessário. Neste diagrama, os recursos na conta de gerenciamento refletem uma AWS Control Tower implantação e uma CloudTrail trilha que registra eventos de toda a organização.

Esse padrão se concentra na implantação de recursos na conta de registro. Se os registros armazenados no Amazon S3 em sua AWS Control Tower landing zone forem criptografados com uma chave KMS gerenciada pelo cliente, você deverá atualizar a política de chaves para permitir que o Microsoft Sentinel decifre os registros. Em um AWS Control Tower landing zone, você gerencia a política de chaves a partir da conta de gerenciamento, que é onde a chave foi criada.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los em todo o ciclo de vida em todas Contas da AWS as regiões.
- CloudWatchA Amazon ajuda você a monitorar as métricas dos seus AWS recursos e dos aplicativos em que você executa AWS em tempo real.
- AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas.
- AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- O Amazon Simple Queue Service (Amazon SQS) fornece uma fila hospedada segura, durável e disponível que ajuda a integrar e desacoplar sistemas e componentes de software distribuídos.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- O Microsoft Sentinel é um sistema SIEM nativo da nuvem que fornece orquestração, automação e resposta de segurança (SOAR).

Repositório de código

O código desse padrão está disponível nos registros de AWS segurança GitHub Ingest and Analyze no repositório Microsoft Sentinel.

Práticas recomendadas

- Siga o princípio do privilégio mínimo (documentação do IAM).
- Siga as melhores práticas para AWS Control Tower administradores (AWS Control Tower documentação).
- Siga as AWS CloudFormation melhores práticas (CloudFormation documentação).
- Use ferramentas de análise de código, como cfn_nag, para verificar os modelos gerados. CloudFormation A ferramenta cfn_nag identifica possíveis problemas de segurança em CloudFormation modelos pesquisando padrões.

Épicos

Conecte o Microsoft Sentinel ao Amazon S3

Tarefa	Descrição	Habilidades necessárias
Prepare o conector Microsoft Sentinel S3.	1. No Microsoft Sentinel, escolha Conectores de dados. 2. Na galeria de conectores de dados, escolha Amazon Web Services S3. **Note** Se você não vê o conector, instale a solução Amazon Web Services a partir do Content Hub no Microsoft Sentinel.	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
	3. No painel de detalhes do conector, escolha Abrir página do conector. 4. Na seção Configuração, copie a ID externa. Você precisará desse ID mais tarde.	

Implante a CloudFormation pilha

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Em um shell bash, insira o comando a seguir. Isso clona o Ingest e analisa os registros de AWS segurança no repositório Microsoft Sentinel. `git clone https://github.com/aws-samples/ingest-and-analyze-aws-security-logs-in-microsoft-sentinel.git`	DevOps engenheiro, General AWS
Assuma a função do IAM na conta de registro.	Na conta de registro, assuma a função do IAM que tem permissões para implantar a CloudFormation pilha. Para obter mais informações sobre como assumir uma função do IAM no AWS CLI, consulte	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
	Usar uma função do IAM no AWS CLI.	

Tarefa	Descrição	Habilidades necessárias
Implante a pilha.	Para implantar a CloudFormation pilha, digite o seguinte comando, onde: • `<Bucket name>` é o nome do bucket Amazon S3 de registro em log. • `<Sentinel external ID>` é a ID externa do conector Amazon S3 no Microsoft Sentinel. • `<Email address>` é um endereço de e-mail válido no qual você deseja receber notificações. • `<Customer managed key ARN>` é o Amazon Resource Name (ARN) da chave KMS gerenciada pelo cliente. Forneça esse parâmetro somente se os registros estiverem criptografados com uma chave KMS gerenciada pelo cliente. • `<Suffix>` é um parâmetro opcional para evitar conflitos de nomes de recursos. • `<ARN for the OIDC provider>` é o ARN do provedor OIDC, se ele já existir. Se você não fornecer esse parâmetro, CloudFormation cria o provedor OIDC.	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
	Important Se a AWS organização for monitorada com o Microsoft Code Defender, o provedor OIDC para a Microsoft já foi implantado. Você deve fornecer esse parâmetro e o ARN do provedor existente. `aws cloudformation deploy --stack-name cloudtrail-sentinel-integration \ --no-fail-on-empty-changeset \ --template-file template.yml \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM CAPABILITY_AUTO_EXPAND \ --parameter-overrides \ ControlTowerS3BucketName="<Bucket name>" \ AzureWorkspaceID="<Sentinel external ID>" \`	

Tarefa	Descrição	Habilidades necessárias
	`EmailAddress="<Email address>" \ KMSKeyArn="<Customer managed key ARN>" \ Suffix="<Suffix to avoid name conflicts>" \ OIDCProviderArn="<ARN for the OIDC provider>"`	
Copie as saídas.	Na saída da CloudFormation pilha, copie os valores de `SentinelRoleArn` e. `SentinelSQS` Você usa esses valores posteriormente para concluir a configuração no Microsoft Sentinel.	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
Modifique a política de chaves.	Se você não estiver usando uma chave KMS gerenciada pelo cliente para criptografar os registros no bucket do Amazon S3, você pode pular esta etapa. Se os registros forem criptografados com uma chave KMS gerenciada pelo cliente, modifique a política de chaves para conceder permissão ao Microsoft Sentinel para descriptografar os registros. Veja a seguir um exemplo de política de chave. Este exemplo de política permite o acesso entre contas se a chave KMS estiver em outra. Conta da AWS `{ "Version": "2012-10-17", "Id": "key-policy", "Statement": [ ... { "Sid": "Grant access to decrypt", "Effect": "Allow", "Principal": { "AWS": "<SentinelRoleArn>" }, `	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
	"Action": "kms:Decrypt", "Resource": "<KeyArn>" }] }	

Configurar o conector no Microsoft Sentinel

Tarefa	Descrição	Habilidades necessárias
Conclua a configuração no Microsoft Sentinel.	1. No Microsoft Sentinel, escolha Conectores de dados. 2. Na galeria de conectores de dados, escolha Amazon Web Services S3. 3. No painel de detalhes do conector, escolha Abrir página do conector. 4. Na seção Configuração, faça o seguinte: a. Em Função a ser adicionada, insira o `SentinelRoleArn` valor que você copiou. b. Em URL do SQS, insira o `SentinelSQS` valor que você copiou. c. Na lista Tabela de destino, escolha`AWSCloudTrail` .	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	5. Escolha Adicionar conexão.	
Envie notificações de eventos do Amazon S3 para o Amazon SQS.	Siga as instruções em Habilitar e configurar notificações de eventos usando o console do Amazon S3 para configurar o bucket de registro do Amazon S3 para enviar notificações de eventos para a fila do Amazon SQS. Se CloudTrail tiver sido configurado para toda a organização, os registros nesse bucket terão o prefixo `<OrgID>/AWSLogs/<OrgID>/` , onde `<OrgID>` está o ID da organização. Para obter mais informações, consulte Visualização de detalhes sobre sua organização.	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
Confirme se os registros foram ingeridos.	1. Espere até que os registros sejam ingeridos no Microsoft Sentinel. Isso pode demorar vários minutos. 2. No Microsoft Sentinel, abra a página do Amazon S3 Data Connector e faça o seguinte: • Confirme se o status do Amazon S3 Data Connector é. `Connected` • Verifique o volume de dados no gráfico Dados recebidos. Para obter mais informaçõ es sobre como inspecionar a atividade do conector de dados, consulte Conector de dados na documentação da Microsoft.	DevOps engenheiro

Valide a solução

Tarefa	Descrição	Habilidades necessárias
CloudWatch Compare os registros do Sentinel.	Na configuração padrão do AWS Control Tower, CloudTrail os registros são enviados para a Amazon CloudWatch e armazenados na conta AWS Control Tower	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
	de gerenciamento. Para obter mais informações, consulte Registro e monitoramento em AWS Control Tower. Use as etapas a seguir para confirmar se esses registros são automaticamente ingeridos no Microsoft Sentinel: 1. Abra o console de CloudWatch . 2. No painel de navegação à esquerda, escolha Logs e, em seguida, escolha Log Insights(Insights de log). 3. Em Selecionar grupo (s) de registros, selecione o grupo de registros em que os CloudTrail registros estão armazenados, como`aws-controltower/CloudTrailLogs` . 4. Na caixa do editor de consultas, insira`fields eventID`. 5. Selecione Executar consulta. 6. Escolha Exportar resultados e, em seguida, escolha Copiar tabela para área de transferência (CSV). 7. Cole os resultados em um editor de texto.	

Tarefa	Descrição	Habilidades necessárias

	8. Altere o formato da saída para que ela possa ser usada em uma consulta do Microsoft Sentinel. Veja a seguir um exemplo que usa a linguagem de consulta Kusto:
	`AWSCloudTrail`
	`| where AwsEventId in`
	`(`
	`'aa08b5fe-3bfb-391a-a14e-5fcebe14dab2',`
	`'9decd805-269c-451c-b75b-762f5dce59f9'`
	`)`
	9. No Microsoft Sentinel, abra a página do Amazon S3 Data Connector. Ao lado do gráfico Dados recebidos, escolha Ir para análise de registros.
	10. Na caixa do editor de consultas, insira a consulta e escolha Executar.
	11. No Microsoft Sentinel e CloudWatch, verifique se o número de entradas é o mesmo. Adapte o intervalo de tempo, se necessário.	

Recursos relacionados

AWS documentação e recursos

- AWS CLI Referência de comando (AWS CLI documentação)
- Configurar opcionalmente AWS KMS keys (AWS Control Tower documentação)
- Criptografia em repouso no Amazon SQS (documentação do Amazon SQS)
- Como faço para evitar que os destinatários da lista cancelem a inscrição de todos na lista dos meus e-mails de tópicos do Amazon SNS? (Centro de AWS conhecimento)

Documentação da Microsoft

- Conecte o Microsoft Sentinel ao Amazon Web Services para AWS ingerir dados de log de serviços
- Linguagem Kusto Query no Microsoft Sentinel

Gerencie AWS Organizations políticas como código usando o AWS CodePipeline Amazon Bedrock

Criado por Andre Cavalcante (AWS) e Mariana Pessoa de Queiroz (AWS)

Resumo

Você pode usar políticas de autorização AWS Organizations para configurar e gerenciar centralmente o acesso de diretores e recursos em suas contas de membros. As políticas de controle de serviço (SCPs) definem o máximo de permissões disponíveis para as funções e usuários AWS Identity and Access Management (IAM) em sua organização. As políticas de controle de recursos (RCPs) definem o máximo de permissões disponíveis para recursos em sua organização.

Esse padrão ajuda você a gerenciar SCPs e criar uma infraestrutura RCPs como código (IaC) que você implanta por meio de um pipeline de integração contínua e implantação contínua (CI/CD). Ao usar o AWS CloudFormation Hashicorp Terraform para gerenciar essas políticas, você pode reduzir a carga associada à criação e manutenção de várias políticas de autorização.

Esse padrão inclui os seguintes recursos:

- Você cria, exclui e atualiza as políticas de autorização usando arquivos de manifesto (`scp-management.jsonercp-management.json`).
- Você trabalha com grades de proteção em vez de políticas. Você define suas grades de proteção e seus alvos nos arquivos de manifesto.
- O pipeline, que usa AWS CodeBuild e AWS CodePipeline, mescla e otimiza as grades de proteção nos arquivos de manifesto. Para cada instrução no arquivo de manifesto, o pipeline combina as grades de proteção em um único SCP ou RCP e as aplica aos destinos definidos.
- AWS Organizations aplica as políticas às suas metas. Um destino pode ser uma Conta da AWS unidade organizacional (OU), um ambiente (que é um grupo de contas ou OUs que você define no `environments.json` arquivo) ou um grupo de contas que compartilham uma AWS tag.
- O Amazon Bedrock lê os registros do pipeline e resume todas as mudanças na política.
- O pipeline requer uma aprovação manual. O aprovador pode revisar o resumo executivo que o Amazon Bedrock preparou, o que o ajuda a entender as mudanças.

Pré-requisitos e limitações

Pré-requisitos

- Vários Contas da AWS que são gerenciados como uma organização em AWS Organizations. Para obter mais informações, consulte Criar uma organização.
- Os recursos SCP e RCP estão habilitados em. AWS Organizations Para obter mais informações, consulte Habilitando um tipo de política.
- A versão 1.9.8 ou posterior do Terraform está instalada.
- Se você não estiver implantando essa solução por meio de um pipeline do Terraform, o arquivo de estado do Terraform deverá ser armazenado em um bucket do Amazon Simple Storage Service (Amazon S3) no local em que você está implantando Conta da AWS o pipeline de gerenciamento de políticas.
- A versão 3.13.3 ou posterior do Python está instalada.

Limitações

- Você não pode usar esse padrão para gerenciar SCPs ou RCPs que foram criados fora desse pipeline de CI/CD. No entanto, você pode recriar políticas existentes por meio do pipeline. Para obter mais informações, consulte Migração de políticas existentes para o pipeline na seção Informações adicionais desse padrão.
- O número de contas e políticas em cada conta estão sujeitos às cotas e aos limites de serviço de. OUs AWS Organizations
- Esse padrão não pode ser usado para configurar políticas de gerenciamento AWS Organizations, como políticas de backup, políticas de tags, políticas de aplicativos de bate-papo ou políticas declarativas.

Arquitetura

O diagrama a seguir mostra o fluxo de trabalho do pipeline de gerenciamento de políticas e seus recursos associados.

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário confirma as alterações nos arquivos `scp-management.json` ou nos arquivos de `rcp-management.json` manifesto na ramificação principal do repositório remoto.
2. A mudança na `main` ramificação inicia a entrada do pipeline. AWS CodePipeline

3. CodePipeline inicia o `Validate-Plan` CodeBuild projeto. Este projeto usa um script Python no repositório remoto para validar as políticas e os arquivos de manifesto da política. Este CodeBuild projeto faz o seguinte:
   a. Verifica se os arquivos de manifesto SCP e RCP contêm uma instrução exclusiva IDs ()`Sid`.
   b. Usa os scripts `scp-policy-processor/main.py` e `rcp-policy-processor/main.py` Python para concatenar guardrails na pasta guardrails em uma única política RCP ou SCP. Ele combina grades de proteção que têm o mesmo `ResourceAction`, e. `Condition`
   c. Usa AWS Identity and Access Management Access Analyzer para validar a política final otimizada. Se houver alguma descoberta, o gasoduto é interrompido.
   d. Cria `scps.json` e `rcps.json` arquiva, que o Terraform usa para criar recursos.
   e. Executa o `terraform plan` comando, que cria um plano de execução do Terraform.
4. (Opcional) O `Validate-Plan` CodeBuild projeto usa o `bedrock-prompt/prompt.py` script para enviar uma solicitação para o Amazon Bedrock. Você define o prompt no `bedrock-prompt/prompt.txt` arquivo. O Amazon Bedrock usa o Anthropic Claude Sonnet 3.5 para gerar um resumo das mudanças propostas analisando os registros do Terraform e do Python.
5. CodePipeline usa um tópico do Amazon Simple Notification Service (Amazon SNS) para notificar os aprovadores de que as alterações devem ser revisadas. Se o Amazon Bedrock gerou um resumo da alteração, a notificação incluirá esse resumo.
6. Um aprovador da política aprova a ação em. CodePipeline Se o Amazon Bedrock gerou um resumo da alteração, o aprovador poderá revisar o resumo CodePipeline antes da aprovação.
7. CodePipeline inicia o `Apply` CodeBuild projeto. Este projeto usa o Terraform para aplicar as alterações de RCP e SCP em. AWS Organizations

O modelo de IaC associado a essa arquitetura também implanta os seguintes recursos que dão suporte ao pipeline de gerenciamento de políticas:

- Um bucket do Amazon S3 para armazenar CodePipeline artefatos e scripts, como e `scp-policy-processor/main.py` `bedrock-prompt/prompt.py`
- Uma chave AWS Key Management Service (AWS KMS) que criptografa os recursos criados por essa solução

Ferramentas

Serviços da AWS

- O Amazon Bedrock é um serviço de IA totalmente gerenciado que disponibiliza muitos modelos básicos de alto desempenho para uso por meio de uma API unificada.
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar as alterações de software continuamente.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Outras ferramentas

- HashiCorp O Terraform é uma ferramenta de IaC que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.

Repositório de código

O código desse padrão está disponível no organizations-policy-pipeline GitHub repositório. A seguir estão os arquivos-chave que estão contidos na `sample-repository` pasta:

- Na `environments` pasta, `environments.json` contém uma lista de ambientes. Os ambientes são um grupo de alvos e podem conter Conta da AWS IDs nossas unidades organizacionais (OUs).
- Na `rcp-management` pasta:
  - A `guardrails` pasta contém as grades de proteção individuais para seu RCPs
  - A `policies` pasta contém o indivíduo RCPs
  - O arquivo de `rcp-management.json` manifesto ajuda você a gerenciar grades de proteção completas RCPs do RCP e seus alvos associados.
- Na `scp-management` pasta:
  - A `guardrails` pasta contém as grades de proteção individuais para seu SCPs

  - A `policies` pasta contém o indivíduo SCPs
  - O arquivo de `scp-management.json` manifesto ajuda você a gerenciar as grades de proteção completas SCPs do SCP e seus alvos associados.
- A `utils` pasta contém scripts que podem ajudar você a migrar seus arquivos atuais SCPs RCPs para que você possa gerenciá-los por meio do pipeline. Para obter mais informações, consulte a seção Informações adicionais desse padrão.

Práticas recomendadas

- Antes de configurar o pipeline, recomendamos que você verifique se não atingiu os limites de suas AWS Organizations cotas.
- Recomendamos que você use a conta AWS Organizations de gerenciamento somente para tarefas que devem ser executadas nessa conta. Para obter mais informações, consulte Práticas recomendadas para a conta de gerenciamento.

Épicos

Configurar a conta de destino

Tarefa	Descrição	Habilidades necessárias
Criar um repositório.	Crie um repositório a partir do qual sua equipe de operações de segurança gerenciará as políticas. Use um dos provedores de repositórios terceirizados que oferecem Conexões de código da AWS suporte.	DevOps engenheiro
Delegar a administração de políticas.	Delegue a administração das AWS Organizations políticas à conta do membro em que você está implantando o pipeline. Para obter instruçõe s, consulte Criar uma política	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	de delegação baseada em recursos com. AWS Organizations Para ver um exemplo de política, consulte Exemplo de política de delegação baseada em recursos na seção Informações adicionais desse padrão.	
(Opcional) Ative o modelo básico.	Se você quiser gerar resumos das mudanças na política, habilite o acesso ao modelo de fundação Anthropic Claude 3.5 Sonnet no Amazon Bedrock, Conta da AWS onde você está implantando o pipeline. Para obter instruções, consulte Adicionar ou remover o acesso aos modelos da Amazon Bedrock Foundation.	AWS geral

Implante os recursos para o pipeline

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Digite o comando a seguir para clonar o organizations-policy-pipeline repositório: GitHub `git clone https://github.com/aws-samp`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`les/organizations-policy-pipeline.git`	

Tarefa	Descrição	Habilidades necessárias
Defina seu método de implantação.	1. No repositório clonado, abra o `variables.tf` arquivo. 2. Para `project_name` , insira o prefixo que você deseja aplicar aos nomes dos recursos implantados. 3. Para `provider_type` , insira o provedor do repositório remoto. Os valores válidos são fornecidos no arquivo. 4. Para `full_repo sitory_name` , insira o nome do repositório remoto. 5. Para `branch_name` , insira o nome da ramificação do Git que você usará para implantar políticas. Um empurrão ou mesclagem nessa ramificação inicia o pipeline. Normalmente, esse é o ramo principal. 6. Para `terraform _version` , insira a versão do Terraform que você está usando. 7. Para `enable_bedrock` , insira `true` se você quiser que o Amazon Bedrock resuma as alterações. Insira `false` se você não	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	quiser gerar um resumo das alterações. 8. Para `tags`, insira os pares de valores-chave que você deseja atribuir como tags aos recursos implantados. 9. Salve e feche o arquivo `variables.tf` .	

Implante o pipeline.	1. Insira o comando a seguir para criar um plano e revisar as alterações:
	`terraform plan`
	2. Insira o comando a seguir para aplicar o plano e criar a infraestrutura do pipeline:
	`terraform apply`
		DevOps engenheiro, Terraform

Conecte o repositório remoto.	Na etapa anterior, o Terraform criou uma CodeConnections conexão com o repositór io de terceiros. No console AWS Developer Tools, altere o status da conexão de `PENDING` para `AVAILABLE` . Para obter instruçõe s, consulte Atualizar uma conexão pendente.	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
Assine o tópico do Amazon SNS.	O Terraform criou um tópico do Amazon SNS. Inscreva um endpoint no tópico e confirme a assinatura para que os aprovadores recebam notificações sobre ações de aprovação pendentes no pipeline. Para obter instruções, consulte Criação de uma assinatura para um tópico do Amazon SNS.	AWS geral

Defina suas grades de proteção e políticas

Tarefa	Descrição	Habilidades necessárias
Preencha o repositório remoto.	Do repositório clonado, copie o conteúdo da `sample-repository` pasta para o seu repositório remoto. Isso inclui as `utils` pastas `environments` `rcp-management` `scp-management` ,, e.	DevOps engenheiro
Defina seus ambientes.	1. Na `environments` pasta, abra o `environments.json` arquivo. Este é o arquivo em que você define o alvo Contas da AWS e OUs para o seu RCPs SCPs e. 2. Exclua os ambientes de exemplo.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	3. Adicione seus ambientes de destino no seguinte formato: `[ { "ID": "<environment-name>", "Target": [ "<ou-name>:<ou-id>", "<account-name>:<account-id>" ] } ]` Em que: • `<environment-name>` é o nome que você atribui ao grupo OUs e às contas da AWS. Você pode usar esse nome no arquivo de manifesto para definir onde deseja aplicar suas políticas. • `<ou-name>` é o nome da OU de destino. • `<ou-id>`é a ID da OU de destino. • `<account-name>` é o nome do alvo Conta da AWS.	

Tarefa	Descrição	Habilidades necessárias
	• `<account-id>` é o ID do alvo Conta da AWS. Para ver exemplos, consulte o repositório de código-fonte. 4. Salve e feche o arquivo `environments.json` .	

Tarefa	Descrição	Habilidades necessárias
Defina suas grades de proteção.	1. Navegue até a `rcp-management/guardrails` pasta no seu repositório remoto. Essa é a pasta em que você define as grades de proteção do seu arquivo de manifesto RCP. Cada corrimão deve estar em um arquivo individual. Os arquivos de proteção podem conter uma ou mais declarações. **Note** Você pode usar a mesma grade de proteção em várias instruções nos arquivos de manifesto de e. SCPs RCPs Se você modificar a grade de proteção, todas as políticas que incluam essa grade de proteção serão afetadas. 2. Exclua qualquer exemplo de proteções que tenha sido copiado do repositório do código-fonte.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	3. Crie um novo arquivo.json e dê a ele um nome descritivo. 4. Abra o arquivo.json que você criou. 5. Defina a grade de proteção no seguinte formato: `[ { "Sid": "<guardrail-name>", "Effect": "<effect-value>", "Action": [ "<action-name>" ], "Resource": "<resource-arn>", "Condition": { "<condition-operator>": { "<condition-key>": [ "<condition-value>" ] } } } ]` Em que: • `<guardrail-name>` é um nome exclusivo para a grade de proteção.	

Tarefa	Descrição	Habilidades necessárias
	Esse nome não pode ser usado para nenhuma outra grade de proteção. • `<effect-value>` deve ser `Allow` ou`Deny`. Para obter mais informações, consulte Efeito. • `<action-name>` deve ser um nome válido de uma ação suportada pelo serviço. Para obter mais informações, consulte Ação. • `<resource-arn>` é o Amazon Resource Name (ARN) do recurso ao qual o guardrail se aplica. Você também pode usar caracteres curinga, como `*` ou`?`. Para obter mais informações, consulte Recurso. • `<condition-operator>` é um operador de condição válido. Para obter mais informações, consulte Operadores de condição. • `<condition-key>` é uma chave de contexto de condição global válida ou uma chave de contexto específica do serviço. Para obter mais	

Tarefa	Descrição	Habilidades necessárias
	informações, consulte Condição. • `<condition-value>` é o valor específico usado em uma condição para avaliar se uma grade de proteção se aplica. Para obter mais informações, consulte Condição. Por exemplo, guardrails de RCP, consulte o repositório do código-fonte. 6. Salve e feche o arquivo.json. 7. Repita essas etapas para criar quantas grades de proteção RCP forem necessárias. 8. Repita essas etapas na `scp-management/guardrails` pasta para criar quantas grades de proteção forem necessárias para o seu. SCPs Por exemplo, guardrails do SCP, consulte o repositório do código-fonte.	

Tarefa	Descrição	Habilidades necessárias
Defina suas políticas.	1. Navegue até a `rcp-management/policies` pasta no seu repositório remoto. Essa é a pasta na qual você define políticas completas para seu arquivo de manifesto RCP. Cada política deve ser um arquivo individual. **Note** Se você modificar uma política nessa pasta, as alterações na política afetarão todas as contas às quais OUs essa política é aplicada, conforme definido no arquivo de manifesto. 2. Exclua qualquer exemplo de política que tenha sido copiada do repositório de código-fonte. 3. Crie um novo arquivo.json e dê a ele um nome descritivo. 4. Abra o arquivo.json que você criou. 5. Defina o RCP. Por exemplo RCPs, consulte o repositór	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	io de código-fonte ou veja exemplos de políticas de controle de recursos na AWS Organizations documentação. 6. Salve e feche o arquivo.json. 7. Repita essas etapas para criar RCPs quantas forem necessárias. 8. Repita essas etapas na `scp-management/policies` pasta para criar SCPs quantas forem necessárias. Por exemplo SCPs, consulte o repositório de código-fonte ou veja exemplos de políticas de controle de serviços na AWS Organizations documentação.	

Use o arquivo de manifesto para gerenciar as políticas

Tarefa	Descrição	Habilidades necessárias
Configure os arquivos de manifesto.	1. Na `rcp-management` pasta, abra o `rcp-management.json` arquivo. Esse é o arquivo em que você define quais grades de proteção do RCP RCPs se aplicam totalmente aos seus ambientes de destino.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	Para ver um exemplo desse arquivo, consulte o repositório do código-fonte. 2. Exclua a declaração de exemplo. 3. Adicione uma nova declaração no seguinte formato: `[ { "SID": "<statement-name>", "Target": { "Type": "<target-type>", "ID": "<target-name>" }, "Guardrails": [ "<guardrail-name>" ], "Policy": "<policy-name>", "Comments": "<comment-text>" } ]` Em que: • `<statement-name>` é um nome exclusivo para a declaração. • `<target-type>` é o tipo de alvo em que	

Tarefa	Descrição	Habilidades necessárias

	você deseja aplicar a política. Os valores válidos são `Account`, `OU`, `Environment` ou `Tag`.
	• `<target-name>` é o identificador do alvo em que você deseja aplicar a política. Insira um dos seguintes:
	  • Para um Conta da AWS, insira o identificador como `<account-name>:<account-id>`.
	  • Para uma OU, insira o identificador como `<OU-name>:<ou-id>`.
	  • Para um ambiente, insira o nome exclusivo que você definiu no `environments.json` arquivo.
	  • Para uma tag, insira o par de valores-chave como. `<tag-key>:<tag-value>`
	• `<guardrail-name>` é o nome exclusivo da grade de proteção do RCP que você definiu na pasta. `rcp-manag`	

Tarefa	Descrição	Habilidades necessárias
	ement/guardrails` Você pode adicionar várias grades de proteção nesse elemento. Você pode deixar esse campo vazio se não quiser aplicar uma grade de proteção. • `<policy-name>` é o nome exclusivo do RCP que você definiu na `rcp-management/policies` pasta. Você pode adicionar somente uma política nesse elemento. Você pode deixar esse campo vazio se não quiser aplicar uma política. • `<comment-text>` é uma descrição que você pode inserir para fins de documentação. Esse campo não é usado durante o processamento do pipeline. Você pode deixar esse campo vazio se não quiser adicionar um comentário. 4. Repita essas etapas para adicionar quantas declarações forem necessárias RCPs para configurar sua organização.	

Tarefa	Descrição	Habilidades necessárias
	5. Salve e feche o arquivo `rcp-management.json` . 6. Na `scp-management` pasta, repita essas etapas no `scp-management.json` arquivo. Esse é o arquivo em que você define quais grades de proteção do SCP SCPs se aplicam totalmente aos seus ambientes de destino. Para ver um exemplo desse arquivo, consulte o repositório do código-fonte.	
Iniciar o pipeline.	Confirme e envie as alterações para a ramificação do repositório remoto que você definiu no `variables.tf` arquivo. Normalmente, esse é o `main` ramo. O pipeline de CI/CD é iniciado automaticamente. Se houver algum erro de pipeline, consulte a seção Solução de problemas desse padrão.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Aprove as mudanças.	Quando o `Validate-Plan` CodeBuild projeto estiver concluído, os aprovadores da política receberão uma notificação por meio do tópico do Amazon SNS que você configurou anteriormente. Faça o seguinte: 1. Abra a mensagem de notificação. 2. Se disponível, revise o resumo das mudanças na política. 3. Siga as instruções em Aprovar ou rejeitar uma ação de aprovação em CodePipeline.	AWS geral, aprovador de políticas

Tarefa	Descrição	Habilidades necessárias
Valide a implantação.	1. Faça login no AWS Organizations console na conta da qual é o administrador delegado. AWS Organizations 2. Na página Políticas de controle de serviços, confirme se as SCPs que você criou estão listadas. 3. Escolha um SCP que seja gerenciado por meio do pipeline e confirme se ele se aplica aos alvos pretendidos. 4. Na página Políticas de controle de recursos, confirme se as RCPs que você criou estão listadas. 5. Escolha um RCP que seja gerenciado por meio do pipeline e confirme se ele se aplica aos alvos pretendidos.	AWS geral

Solução de problemas

Problema	Solução
Erros de arquivo manifesto na `Validate-Plan` fase do pipeline	Uma mensagem “Erros de pipeline na fase de validação e planejamento para arquivos de manifesto” aparece na saída do pipeline se houver algum erro nos `rcp-management.json` arquivos `scp-manag`

Problema	Solução
	`ement.json` ou. Os possíveis erros incluem um nome de ambiente incorreto, campos ou SIDs valores duplicados ou inválidos. Faça o seguinte: 1. Siga as instruções em Exibir detalhes da compilação em AWS CodeBuild. 2. No registro de compilação, encontre o erro de validação. O erro fornece mais informaçõ es sobre o que causou a falha da compilaçã o. 3. Atualize o arquivo.json correspondente. 4. Confirme e envie o arquivo atualizado para o repositório remoto. O pipeline é reiniciado. 5. Monitore o status para confirmar se o erro de validação foi resolvido.

Problema	Solução
Descobertas do IAM Access Analyzer na `Validate-Plan` fase do pipeline	Uma mensagem “Descobertas no IAM Access Analyzer durante a fase de validação e planejamento” aparece na saída do pipeline se houver algum erro na proteção ou nas definições da política. Esse padrão usa o IAM Access Analyzer para validar a política final. Faça o seguinte: 1. Siga as instruções em Exibir detalhes da compilação em AWS CodeBuild. 2. No registro de compilação, encontre o erro de validação do IAM Access Analyzer. O erro fornece mais informações sobre o que causou a falha da compilação. Para obter mais informações sobre os tipos de descoberta, consulte a referência de verificação de validação de políticas do IAM. 3. Atualize o arquivo.json correspondente para a grade de proteção ou política. 4. Confirme e envie o arquivo atualizado para o repositório remoto. O pipeline é reiniciado. 5. Monitore o status para confirmar se o erro de validação foi resolvido.

Recursos relacionados

- Referência do elemento de política JSON (documentação do IAM)
- Políticas de controle de recursos (AWS Organizations documentação)
- Políticas de controle de serviços (AWS Organizations documentação)
- Adicionar ou remover o acesso aos modelos da Amazon Bedrock Foundation (documentação do Amazon Bedrock)
- Aprovar ou rejeitar uma ação de aprovação em CodePipeline (CodePipeline documentação)

Mais informações

Exemplo de política de delegação baseada em recursos

Veja a seguir um exemplo de política de delegação baseada em recursos para. AWS Organizations Ele permite que a conta de administrador delegada SCPs gerencie e RCPs para a organização. No exemplo de política a seguir, `<MEMBER_ACCOUNT_ID>` substitua pelo ID da conta em que você está implantando o pipeline de gerenciamento de políticas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegationToAudit",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<MEMBER_ACCOUNT_ID>:root"
      },
      "Action": [
        "organizations:ListTargetsForPolicy",
        "organizations:CreatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:EnablePolicyType",
        "organizations:UpdatePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Migração de políticas existentes para o pipeline

Se você já tiver SCPs ou RCPs quiser migrar e gerenciar por meio desse pipeline, poderá usar os scripts do Python na pasta `sample-repository/utils` do repositório de código. Esses scripts incluem:

- `check-if-scp-exists-in-env.py`— Esse script verifica se uma política especificada se aplica a algum destino em um ambiente específico, que você define no `environments.json` arquivo. Digite o seguinte comando para executar esse script:

  ```
  python3 check-if-scp-exists-in-env.py \
     --policy-type <POLICY_TYPE> \
     --policy-name <POLICY_NAME> \
     --env-id <ENV_ID>
  ```

  Substitua o seguinte neste comando:

  - `<POLICY_TYPE>` é `scp` ou `rcp`
  - `<POLICY_NAME>`é o nome do SCP ou RCP
  - `<ENV_ID>`é a ID do ambiente que você definiu no `environments.json` arquivo
- `create-environments.py`— Esse script cria um arquivo environments.json com base no atual SCPs e RCPs no seu ambiente. Isso exclui as políticas implantadas por meio de. AWS Control Tower Digite o comando a seguir para executar esse script, onde `<POLICY_TYPE>` está `scp` ou`rcp`:

  ```
  python create-environments.py --policy-type <POLICY_TYPE>
  ```
- `verify-policies-capacity.py`— Esse script verifica cada ambiente que você define para determinar quanta capacidade resta para cada cota AWS Organizations relacionada à política. Você define os ambientes a serem verificados no `environments.json` arquivo de entrada. Digite o comando a seguir para executar esse script, onde `<POLICY_TYPE>` está `scp` ou`rcp`:

  ```
  python verify-policies-capacity.py --policy-type <POLICY_TYPE>
  ```

Gerencie conjuntos de AWS IAM Identity Center permissões como código usando AWS CodePipeline

Criado por Andre Cavalcante (AWS) e Claison Amorim (AWS)

Resumo

AWS IAM Identity Center ajuda você a gerenciar centralmente o acesso de login único (SSO) a todos os seus aplicativos. Contas da AWS Você pode criar e gerenciar identidades de usuários no Centro de Identidade do IAM ou conectar uma fonte de identidades existente, como um domínio do Microsoft Active Directory ou um provedor de identidades (IdP) externo. O IAM Identity Center fornece uma experiência de administração unificada para definir, personalizar e atribuir acesso refinado ao seu AWS ambiente usando conjuntos de permissões. Os conjuntos de permissões se aplicam aos usuários e grupos federados do seu repositório de identidades do IAM Identity Center ou do seu IdP externo.

Esse padrão ajuda você a gerenciar os conjuntos de permissões do IAM Identity Center como código em seu ambiente de várias contas, que é gerenciado como uma organização em AWS Organizations. Com esse padrão, você pode conseguir o seguinte:

- Criar, excluir e atualizar conjuntos de permissões
- Crie, atualize ou exclua atribuições do conjunto de permissões para o alvo Contas da AWS, para as unidades organizacionais (OUs) ou para a raiz da sua organização.

Para gerenciar as permissões e atribuições do IAM Identity Center como código, essa solução implanta um pipeline de integração contínua e entrega contínua (CI/CD) que usa e. AWS CodeBuild AWS CodePipeline Você gerencia os conjuntos de permissões e as atribuições nos modelos JSON que você armazena em um repositório remoto. Quando EventBridge as regras da Amazon detectam uma alteração no repositório ou detectam modificações nas contas na UO de destino, elas iniciam uma AWS Lambda função. A função do Lambda inicia o pipeline de CI/CD que atualiza os conjuntos de permissões e as atribuições no contínuas Centro de Identidade do IAM.

Pré-requisitos e limitações

Pré-requisitos

- Um ambiente de várias contas gerenciado como uma organização em AWS Organizations. Para obter mais informações, consulte Criar uma organização.

- Centro de identidade do IAM, habilitado e configurado com uma fonte de identidade. Para obter mais informações sobre o Centro de Identidade do IAM, consulte Fundamentos.
- Uma conta de membro registrada como administrador delegado para o seguinte: Serviços da AWS
  - Centro de identidade do IAM — Para obter instruções, consulte Registrar uma conta de membro na documentação do IAM Identity Center.
  - AWS Organizations — Para obter instruções, consulte Administrador delegado para AWS Organizations. Essa conta deve ter permissões para listar e descrever contas OUs e.

> **Note**
>
> Você deve usar a mesma conta do administrador delegado para ambos os serviços.

- Permissões para implantar AWS CloudFormation pilhas na conta de administrador delegado do IAM Identity Center e na conta de gerenciamento da organização. Para obter mais informações, consulte Controle de acesso na CloudFormation documentação.
- Um bucket do Amazon Simple Storage Service (Amazon S3) na conta de administrador delegado do IAM Identity Center. Você carrega o código do artefato nesse bucket. Para obter instruções, consulte Criação de um bucket na documentação do Amazon S3.
- O ID da conta de gerenciamento da organização. Para obter instruções, consulte Como encontrar seu Conta da AWS ID.
- Um repositório em seu host de código-fonte, como GitHub.

Limitações

- Esse padrão não pode ser usado para gerenciar ou atribuir conjuntos de permissões para ambientes de conta única ou para contas que não são gerenciadas como uma organização em AWS Organizations.
- Os nomes dos conjuntos de permissões, as atribuições IDs e os tipos principais do IAM Identity Center IDs não podem ser modificados após a implantação.
- Esse padrão ajuda você a criar e gerenciar permissões personalizadas. Você não pode usar esse padrão para gerenciar ou atribuir permissões predefinidas.
- Esse padrão não pode ser usado para gerenciar um conjunto de permissões para a conta de gerenciamento da organização.

Arquitetura

Arquitetura de destino

O diagrama mostra o seguinte fluxo de trabalho:

1. Um usuário faz uma ou todas as alterações a seguir:
   - Confirma uma ou mais alterações no repositório remoto, como GitHub
   - Modifica as contas na OU em AWS Organizations
2. Se o usuário tiver confirmado uma alteração no repositório remoto na ramificação principal, o pipeline será iniciado.

   Se o usuário modificou as contas na OU, a `MoveAccount` EventBridge regra detectará a alteração e iniciará uma função Lambda na conta de gerenciamento da organização.
3. A função Lambda iniciada inicia o pipeline de CI/CD em. CodePipeline
4. CodePipeline inicia o `TemplateValidation` CodeBuild projeto. O `TemplateValidation` CodeBuild projeto usa um script Python no repositório remoto para validar os modelos do conjunto de permissões. CodeBuild valida o seguinte:
   - Os nomes do conjunto de permissões que são exclusivos.
   - A declaração de atribuição IDs (`Sid`) é exclusiva.
   - As definições de política no parâmetro `CustomPolicy` e válidas. (Essa validação usa AWS Identity and Access Management Access Analyzer.)
   - Os nomes de recursos da Amazon (ARNs) das políticas gerenciadas são válidos.
5. O grupo de `PermissionSet` ação no `Deploy` CodeBuild projeto usa AWS SDK para Python (Boto3) para excluir, criar ou atualizar os conjuntos de permissões no IAM Identity Center. Somente os conjuntos de permissões com a tag `SSOPipeline:true` são afetados. Todos os conjuntos de permissões gerenciados por meio desse pipeline têm essa tag.
6. O grupo de `Assignments` ação no `Deploy` CodeBuild projeto usa o Terraform para excluir, criar ou atualizar as atribuições no IAM Identity Center. Os arquivos de estado do back-end do Terraform são armazenados em um bucket Amazon S3 na mesma conta.
7. CodeBuild atualiza os conjuntos de permissões e as atribuições no IAM Identity Center.

Automação e escala

Como todas as novas contas em um ambiente de várias contas são movidas para uma unidade organizacional específica em AWS Organizations, essa solução é executada automaticamente e concede os conjuntos de permissões necessários a todas as contas que você especifica nos modelos de atribuição. Nenhuma automação ou ação de escalonamento adicional é necessária.

Em ambientes grandes, o número de solicitações de API para o Centro de Identidade do IAM pode fazer com que essa solução seja executada mais lentamente. O Terraform e o Boto3 gerenciam automaticamente o controle de utilização para minimizar qualquer degradação do desempenho.

Ferramentas

Serviços da AWS

- AWS CloudFormationajuda você a configurar AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em Contas da AWS e. Regiões da AWS
- AWS CodeBuildé um serviço de compilação totalmente gerenciado que ajuda você a compilar o código-fonte, executar testes de unidade e produzir artefatos prontos para implantação.
- AWS CodePipelineajuda você a modelar e configurar rapidamente os diferentes estágios de uma versão de software e automatizar as etapas necessárias para liberar alterações de software continuamente.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- AWS IAM Identity Centerajuda você a gerenciar centralmente o acesso de login único (SSO) a todos os seus Contas da AWS aplicativos e à nuvem.
- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente.
- AWS SDK para Python (Boto3)é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python com o. Serviços da AWS
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Repositório de código

O código desse padrão está disponível no repositório aws-iam-identity-center-pipeline. A pasta de modelos no repositório inclui modelos de exemplo para conjuntos de permissões e atribuições. Também inclui AWS CloudFormation modelos para implantar o pipeline de CI/CD e AWS os recursos nas contas de destino.

Práticas recomendadas

- Antes de começar a modificar o conjunto de permissões e os modelos de exercícios, recomendamos que você planeje os conjuntos de permissões para sua organização. Considere quais devem ser as permissões, a quais contas ou OUs o conjunto de permissões devem ser aplicados e quais diretores do IAM Identity Center (usuários ou grupos) devem ser afetados pelo conjunto de permissões. Os nomes dos conjuntos de permissões, a associação IDs e os tipos principais do IAM Identity Center IDs não podem ser modificados após a implantação.
- Siga o princípio do privilégio mínimo e conceda as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte Conceder privilégios mínimos e melhores práticas de segurança na documentação AWS Identity and Access Management (IAM).

Épicos

Planejar conjuntos de permissões e atribuições

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Em um shell bash, insira o comando a seguir. Isso clona o repositório aws-iam-identity-center-pipeline de. GitHub `git clone https://github.com/aws-samples/aws-iam-identity-center-pipeline.git`	DevOps engenheiro
Defina os conjuntos de permissões.	1. No repositório clonado, navegue até a pasta `templates/permissi`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	onsets e abra um dos modelos disponíveis. 2. No parâmetroName , insira um nome para o conjunto de permissões. Esse valor deve ser exclusivo e não pode ser alterado após a implantação. 3. No parâmetro Descripti on , descreva brevemente o conjunto de permissões, como o caso de uso. 4. No SessionDuration parâmetro, especifique por quanto tempo um usuário pode estar conectado a um Conta da AWS. Use o ISO-8601 duration format (formato de duração ISO-8601) (Wikipedia), como PT4H por 4 horas. Se nenhum valor for definido, o padrão no Centro de Identidade do IAM é de 1 hora. 5. No RelayState parâmetro, especifique a URL que fornece acesso rápido ao console mais apropriado para a função do usuário. 6. Personalize as políticas no conjunto de permissõe s. Todos os parâmetros	

Tarefa	Descrição	Habilidades necessárias

	a seguir são opcionais e podem ser modificados após a implantação. Você deve usar pelo menos um dos parâmetros para definir as políticas no conjunto de permissões:
	• No `ManagedPolicies` parâmetro, insira ARNs as políticas AWS gerenciadas que você deseja atribuir.
	• No parâmetro `CustomerManagedPolicies` , insira os ARNs de todas as políticas gerenciadas pelo cliente que você deseja atribuir. Não use o ARN.
	• No `PermissionBoundary` parâmetro , faça o seguinte para atribuir um limite de permissões:
	  • Se você estiver usando uma política AWS gerenciada como limite de permissões, entre `PolicyType AWS`, entre e insira o ARN da política. `Policy`
	  • Se você estiver usando uma política gerenciada pelo cliente como	

Tarefa	Descrição	Habilidades necessárias
	limite de permissõe sPolicyType , entreCustomer, entre e insira o nome da política. Policy Não use o ARN. • No parâmetro CustomPolicy , defina todas as políticas personalizadas em formato JSON que você deseja atribuir. Para obter mais informações sobre a estrutura da política JSON, consulte Visão geral de políticas JSON. 7. Salve e feche o modelo do conjunto de permissõe s. Recomendamos que você salve o arquivo com um nome que correspon da ao nome do conjunto de permissões. 8. Repita esse processo para criar quantos conjuntos de permissões forem necessári os para sua organização e exclua todos os modelos de amostra que não sejam necessários.	

Tarefa	Descrição	Habilidades necessárias
Defina as atribuições.	1. No repositório clonado, navegue até a pasta `templates/assignments` e abra `iam-identitycenter-assigments.json`. Esse arquivo descreve como você deseja atribuir os conjuntos de permissões a Contas da AWS ou OUs. 2. No parâmetro `SID`, insira um identificador para a atribuição. Esse valor deve ser exclusivo e não pode ser alterado após a implantação. 3. No parâmetro `Target`, defina as contas ou organizações nas quais você deseja aplicar o conjunto de permissões. Os valores válidos são conta IDs OUs, ou `root`. `root` atribui o conjunto de permissões a todas as contas dos membros na organização, excluindo a conta de gerenciamento. Insira os valores entre aspas duplas e separe vários identificadores com vírgulas. Conta IDs e OUs deve seguir o padrão: `{{account`	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	`_name}}:{{account_id}}` `ou{{ou_name}}:{{ou_id}}` . Se você quiser atribuir permissões recursivamente ao aninhado OUs, use o padrão OU com um curinga no final. Example: `{{ou_name}}:{{ou_id}}:*` 4. No parâmetro `PrincipalType` , insira o tipo de entidade principal do Centro de Identidade do IAM que será afetado pelo conjunto de permissões. Os valores válidos são `USER` ou `GROUP`. Esse valor não poderá ser modificado após a implantação. 5. No parâmetro `PrincipalID` , insira o nome do usuário ou grupo no armazém de identidade do Centro de Identidade do IAM que será afetado pelo conjunto de permissões. Esse valor não poderá ser modificado após a implantação. 6. No parâmetro `PermissionSetName` , insira o nome do conjunto de permissões que você deseja atribuir.	

Tarefa	Descrição	Habilidades necessárias
	7. Repita as etapas de 2 a 6 para criar quantas tarefas forem necessárias nesse arquivo. Normalmente, há uma atribuição para cada conjunto de permissões. Exclua todos os exemplos de exercícios que não sejam obrigatórios. 8. Salve e feche o arquivo `iam-identitycenter-assigments.json` .	

Implante conjuntos de permissões e atribuições

Tarefa	Descrição	Habilidades necessárias
Faça login na conta de administrador delegado do Centro de Identidade do IAM.	1. Na conta de administrador delegado do IAM Identity Center, abra o AWS CloudFormation console. 2. Implante o modelo `iam-identitycenter-pipeline.yaml` . Dê um nome bem definido e descritivo à pilha e atualize os parâmetros conforme as instruções. Para obter instruções, consulte Criação de uma pilha na CloudFormation documentação.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Implante recursos na conta AWS Organizations de gerenciamento.	1. Faça login na conta de gerenciamento da organização. 2. Abra o console de AWS CloudFormation. 3. Na barra de navegação, escolha o nome do exibido atualmente Região da AWS. Depois escolha a região `us-east-1` . Essa região é necessária para que a `MoveAccount` EventBridge regra possa detectar AWS CloudTrai l eventos associados às mudanças na organização. 4. Implante o modelo `iam-identitycenter-organization` . Dê um nome bem definido e descritivo à pilha e atualize os parâmetros conforme as instruçõe s. Para obter instruções, consulte Criação de uma pilha na CloudFormation documentação.	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
Conclua a configuração do repositório remoto.	Altere o status da Conexões de código da AWS conexão de `PENDING` para`AVAILABLE` . Essa conexão foi criada quando você implantou a CloudFormation pilha. Para obter instruções, consulte Atualizar uma conexão pendente na CodeConnections documentação.	DevOps engenheiro
Faça upload de arquivos para o repositório remoto.	Faça upload de todos os arquivos que você baixou do `aws-samples` repositório e editou nas etapas anteriores para o repositório remoto. As alterações na `main` ramificação iniciam o pipeline, que cria ou atualiza os conjuntos de permissões e as atribuições.	DevOps engenheiro

Como atualizar os conjuntos de permissões e as atribuições

Tarefa	Descrição	Habilidades necessárias
Atualize os conjuntos de permissões e as atribuições.	Quando a EventBridge regra da `MoveAccount` Amazon detectar modificações nas contas da organização, o CI/CD pipeline automatically starts and updates the permission sets. For example, if you add an account to an OU specified in the assignmen	DevOps engenheiro

Tarefa	Descrição	Habilidades necessárias
	ts JSON file, then the CI/CD pipeline aplicará o conjunto de permissões à nova conta. Se você quiser modificar os conjuntos de permissões e as atribuições implantados, atualize os arquivos JSON e, em seguida, confirme-os no repositório remoto. Observe o seguinte ao usar o pipeline de CI/CD para gerenciar conjuntos de permissões e associações implantados anteriormente: • Se você alterar o nome de um conjunto de permissões, o pipeline de CI/CD excluirá o conjunto de permissões original e criará um novo. • Esse pipeline gerencia somente conjuntos de permissões que têm a tag `SSOPipeline:true` . • Você pode ter vários conjuntos de permissões e modelos de exercícios na mesma pasta no repositório. • Se você excluir um modelo, o pipeline excluirá o conjunto de permissões ou de atribuições.	

Tarefa	Descrição	Habilidades necessárias
	• Se você excluir um bloco JSON de atribuição inteiro, o pipeline excluirá a atribuição do Centro de Identidade do IAM. • Você não pode excluir um conjunto de permissões atribuído a um Conta da AWS. Primeiro, você deve cancelar a atribuição do conjunto de permissões.	

Solução de problemas

Problema	Solução
Erros de acesso negado	Confirme se você tem as permissões necessárias para implantar os CloudFormation modelos e os recursos definidos neles. Para obter mais informações, consulte Controle de acesso na CloudFormation documentação.
Erros de pipeline na fase de validação	Esse erro aparecerá se houver algum erro no conjunto de permissões ou nos modelos de atribuição. 1. Em CodeBuild, veja os detalhes da construção. 2. No log de compilação, encontre o erro de validação que fornece mais informações sobre o que causou a falha da compilação. 3. Atualize o conjunto de permissões ou os modelos de atribuição e, em seguida, confirme-os no repositório.

Problema	Solução
	4. O pipeline de CI/CD reinicia o projeto. CodeBuild Monitore o status para confirmar se o erro de validação foi resolvido.

Recursos relacionados

- Permission sets (documentação do Centro de Identidade do IAM)

Gerenciar credenciais usando o AWS Secrets Manager

Criado por Durga Prasad Cheepuri (AWS)

Resumo

Esse padrão orienta você a usar o AWS Secrets Manager para buscar dinamicamente as credenciais do banco de dados para um aplicativo Java Spring.

No passado, quando você criava um aplicativo personalizado para recuperação de informações de um banco de dados, normalmente era necessário incorporar as credenciais (o segredo) para acessar o banco de dados diretamente no aplicativo. Quando chegou a hora de alternar credenciais, você precisava tirar tempo para atualizar a aplicação para usar novas credenciais e depois distribuir a aplicação atualizada. Se houvesse vários aplicativos compartilhando as credenciais e um deles não fosse atualizado, ele apresentaria falha. Devido a esse risco, muitos usuários optam por não alternar regularmente suas credenciais, o que, na verdade, substitui um risco por outro.

O Secrets Manager permite substituir credenciais codificadas, incluindo senhas, por uma chamada da API para recuperar o segredo por programação. Isso ajuda a garantir que o segredo não será comprometido por alguém que esteja examinando seu código, pois o segredo simplesmente não está ali. Configure também o Secrets Manager para alterar automaticamente o segredo de acordo com a programação que você especificar. Isso permite substituir segredos de longo prazo por outros de curto prazo, ajudando a reduzir de maneira significativa o risco de comprometimento. Para obter mais informações, consulte a documentação do AWS Secrets Manager.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta da AWS com acesso ao Secrets Manager
- Um aplicativo Java Spring

Arquitetura

Pilha de tecnologia de origem

- Um aplicativo Java Spring com código que acessa um banco de dados, com credenciais de banco de dados gerenciadas a partir do arquivo application.properties.

Pilha de tecnologias de destino

- Um aplicativo Java Spring com código que acessa um banco de dados, com credenciais de banco de dados gerenciadas no Secrets Manager. O arquivo application.properties contém os segredos do Secrets Manager.

Integração do Secrets Manager com um aplicativo

Ferramentas

- Secrets Manager: o AWS Secrets Manager é um serviço da AWS que facilita o gerenciamento de segredos. Os segredos podem ser credenciais de banco de dados, senhas, chaves de API de terceiros e até mesmo texto arbitrário. Você pode armazenar e controlar o acesso a esses segredos centralmente usando o console do Secrets Manager, a interface de linha de comando (CLI) do Secrets Manager ou a API Secrets Manager e. SDKs

Épicos

Armazenar o segredo no Secrets Manager

Tarefa	Descrição	Habilidades necessárias
Armazene credenciais do banco de dados em segredo no Secrets Manager.	Armazene o Amazon Relational Database Service (Amazon RDS) ou outras credenciais de banco de dados como um segredo no Secrets Manager seguindo as etapas em Criação de um segredo na documentação do Secrets Manager.	Admin do sistema
Defina permissões para o aplicativo Spring acessar o Secrets Manager.	Defina as permissões apropriadas com base em como o aplicativo Java Spring usa o Secrets Manager.	Admin do sistema

Tarefa	Descrição	Habilidades necessárias
	Para controlar o acesso ao segredo, crie uma política com base nas informações fornecidas na documenta ção do Secrets Manager, nas seções Usando políticas baseadas em identidade (políticas do IAM) e ABAC para o Secrets Manager e Usando políticas baseadas em recursos para o Secrets Manager. Siga as etapas na seção Recuperando o valor secreto na documentação do Secrets Manager.	

Atualizar o aplicativo Spring

Tarefa	Descrição	Habilidades necessárias
Adicione dependências JAR para usar o Secrets Manager.	Consulte a seção Informações adicionais para obter detalhes.	Desenvolvedor Java
Adicione os detalhes do segredo ao aplicativo Spring.	Atualize o arquivo applicati on.properties com o nome secreto, os endpoints e a região da AWS. Para obter um exemplo, consulte a seção Informações adicionais.	Desenvolvedor Java
Atualize o código de recuperação de credenciais de banco de dados em Java.	No aplicativo, atualize o código Java que busca as credenciais do banco de dados para obter esses detalhes do Secrets Manager.	Desenvolvedor Java

Tarefa	Descrição	Habilidades necessárias
	Para exemplo de código, consulte a seção Informações adicionais.	

Recursos relacionados

- Documentação do AWS Secrets Manager
- Usar políticas baseadas em identidade (políticas do IAM) e ABAC para o Secrets Manager
- Usando políticas baseadas em recursos para o Secrets Manager
- Código de exemplo

Mais informações

Adicionando dependências JAR para usar o Secrets Manager

Maven:

```
<groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-secretsmanager</artifactId>
    <version>1.11. 355 </version>
```

Gradle:

```
compile group: 'com.amazonaws', name: 'aws-java-sdk-secretsmanager', version:
 '1.11.355'
```

Atualizando o arquivo application.properties com os detalhes do segredo

```
spring.aws.secretsmanager.secretName=postgres-local
spring.aws.secretsmanager.endpoint=secretsmanager.us-east-1.amazonaws.com
spring.aws.secretsmanager.region=us-east-1
```

Atualizando o código de recuperação de credenciais de banco de dados em Java

```
String  secretName  =  env.getProperty("spring.aws.secretsmanager.secretName");
```

```
String  endpoints  =  env.getProperty("spring.aws.secretsmanager.endpoint");
String  AWS Region  =  env.getProperty("spring.aws.secretsmanager.region");
AwsClientBuilder.EndpointConfiguration  config  =  new
  AwsClientBuilder.EndpointConfiguration(endpoints, AWS Region);
AWSSecretsManagerClientBuilder  clientBuilder  =
  AWSSecretsManagerClientBuilder.standard();
clientBuilder.setEndpointConfiguration(config);
AWSSecretsManager  client  =  clientBuilder.build();

ObjectMapper  objectMapper  =  new  ObjectMapper();

JsonNode  secretsJson  =  null;

ByteBuffer  binarySecretData;

GetSecretValueRequest  getSecretValueRequest  =  new
  GetSecretValueRequest().withSecretId(secretName);

GetSecretValueResult  getSecretValueResponse  =  null;

try  {
     getSecretValueResponse  =  client.getSecretValue(getSecretValueRequest);
    }

catch  (ResourceNotFoundException  e)  {
     log.error("The requested secret "  +  secretName  +  " was not found");
    }

catch  (InvalidRequestException  e)  {
     log.error("The request was invalid due to: "  +  e.getMessage());
     }

catch  (InvalidParameterException  e)  {
     log.error("The request had invalid params: "  +  e.getMessage());
     }
if  (getSecretValueResponse  ==  null)  {
     return  null;
     }  // Decrypted secret using the associated KMS key // Depending on whether the
 secret was a string or binary, one of these fields will be populated


String secret = getSecretValueResponse.getSecretString();

if (secret != null) {
```

```
     try {
                secretsJson  =  objectMapper.readTree(secret);
           }

     catch  (IOException  e)  {
                log.error("Exception while retrieving secret values: "  +
  e.getMessage());
           }
}

else  {
     log.error("The Secret String returned is null");

     return null;

     }
     String  host  =  secretsJson.get("host").textValue();
     String  port  =  secretsJson.get("port").textValue();
     String  dbname  =  secretsJson.get("dbname").textValue();
     String  username  =  secretsJson.get("username").textValue();
     String  password  =  secretsJson.get("password").textValue();
}
```

Monitore ElastiCache clusters para grupos de segurança

Criado por Susanne Kangnoh (AWS) e Archit Mathur (AWS)

Resumo

ElastiCache A Amazon é um serviço da Amazon Web Services (AWS) que fornece uma solução de cache de alto desempenho, escalável e econômica para distribuir um armazenamento de dados na memória ou um ambiente de cache na nuvem. Ele recupera dados de armazenamentos de dados na memória de alto throughput e baixa latência. Essa funcionalidade o torna uma escolha popular para casos de uso em tempo real, como armazenamento em cache, armazenamentos de sessões, jogos, serviços geoespaciais, análises em tempo real e filas. ElastiCache oferece armazenamentos de dados Redis e Memcached, ambos com tempos de resposta inferiores a um milissegundo.

Um grupo de segurança atua como um firewall virtual para suas ElastiCache instâncias, controlando o tráfego de entrada e saída. Os grupos de segurança atuam no nível da instância e não no nível da sub-rede. Para cada grupo de segurança, adicione um conjunto de regras que controlam o tráfego de entrada para instâncias e um conjunto separado de regras que controlam o tráfego de saída. Você pode especificar regras de permissão, mas não regras de negação.

Esse padrão fornece um controle de segurança que monitora as chamadas de API e gera um evento no Amazon CloudWatch Events sobre as ModifyReplicationGroupoperações CreateReplicationGroupCreateCacheClusterModifyCacheCluster,, e. Esse evento chama uma AWS Lambda função, que executa um script Python. A função obtém o ID do grupo de replicação da entrada JSON do evento e executa as seguintes verificações para determinar se há uma violação de segurança:

- Verifica se o grupo de segurança do cluster corresponde ao grupo de segurança configurado na função do Lambda.
- Se o grupo de segurança do cluster não corresponder, a função enviará uma mensagem de violação para um endereço de e-mail fornecido por você, usando uma notificação do Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos e limitações

Pré-requisitos

- Uma AWS conta ativa.

- Um bucket do Amazon Simple Storage Service (Amazon S3) para carregar o código do Lambda fornecido.
- Um endereço de e-mail no qual você deseja receber notificações de violação.
- ElastiCache registro ativado, para acesso a todos os registros da API.

Limitações

- Esse controle de detetive é regional e deve ser implantado em cada área Região da AWS que você deseja monitorar.
- O controle é compatível com grupos de replicação que executam em uma nuvem privada virtual (VPC).

Arquitetura

Arquitetura de fluxo de trabalho

Automação e escala

- Se você estiver usando AWS Organizations, você pode usar AWS CloudFormation StackSetspara implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

AWS serviços

- A Amazon ElastiCache facilita a configuração, o gerenciamento e a escalabilidade de ambientes distribuídos de cache na memória no Nuvem AWS. Ele fornece um cache na memória de alto desempenho, redimensionável e econômico, ao mesmo tempo em que remove a complexidade associada à implantação e ao gerenciamento de um ambiente de cache distribuído. ElastiCache funciona com os mecanismos Redis e Memcached.
- AWS CloudFormationajuda você a modelar e configurar seus AWS recursos, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em vários Contas da AWS e. Regiões da AWS

- A Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. CloudWatch Os eventos ficam cientes das mudanças operacionais à medida que elas ocorrem e tomam medidas corretivas conforme necessário, enviando mensagens para responder ao ambiente, ativando funções, fazendo alterações e capturando informações de estado.
- AWS Lambdaé um serviço de computação que oferece suporte à execução de código sem provisionar ou gerenciar servidores. O Lambda executa o código somente quando necessário e escala automaticamente, desde algumas solicitações por dia a milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- O Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que coordena e gerencia o envio de mensagens entre editores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

Esse padrão inclui um anexo com dois arquivos:

- `ElastiCacheAllowedSecurityGroup.zip` é um arquivo compactado que inclui o controle de segurança (código Lambda).
- `ElastiCacheAllowedSecurityGroup.yml`é um CloudFormation modelo que implanta o controle de segurança.

Consulte a seção Tópicos para obter informações sobre como usar esses arquivos.

Épicos

Implemente o controle de segurança

Tarefa	Descrição	Habilidades necessárias
Faça upload do código para um bucket do S3.	Crie um novo bucket do S3 ou use um bucket do S3 existente para carregar o arquivo `ElastiCacheAllowed`	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`SecurityGroup.zip` anexado (código do Lambda). Esse bucket deve estar nos Região da AWS mesmos recursos que você deseja avaliar.	
Implante o CloudFormation modelo.	Abra o CloudFormation console da Região da AWS mesma forma que o bucket do S3 e implante o `ElastiCacheAllowedSecurityControl.yml` arquivo fornecido no anexo. No próximo épico, forneça valores para os parâmetros do modelo.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Dar o nome do bucket do S3.	Insira o nome do bucket do S3 que você criou ou selecionou no primeiro épico. Esse bucket do S3 contém o arquivo.zip do código Lambda e deve estar no mesmo Região da AWS formato do CloudFormation modelo e do recurso que será avaliado.	Arquiteto de nuvem
Fornecer a chave do S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	barras iniciais (por exemplo, `ElasticCacheAllowedSecurityGroup.zip` ou `controls/ElasticCacheAllowedSecurityGroup.zip`).	
Fornecer um endereço de e-mail.	Forneça um endereço de e-mail ativo no qual você deseja receber notificações de violação.	Arquiteto de nuvem
Especifique um nível de log.	Especifique o nível de registro em log e a verbosidade. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo e deve ser usado somente para depuração. `Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	Arquiteto de nuvem

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirme a assinatura por e-mail.	Quando o CloudFormation modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail que você forneceu.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	Você precisa confirmar sua assinatura para começar a receber as notificações.	

Recursos relacionados

- Criação de uma pilha no AWS CloudFormation console (AWS CloudFormation documentação)
- Amazon VPCs e ElastiCache segurança (ElastiCache documentação da Amazon)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Monitorar clusters do Amazon EMR para criptografia em trânsito na execução

Criado por Susanne Kangnoh (AWS)

Resumo

Este padrão fornece um controle de segurança que monitora os clusters do Amazon EMR na execução e envia um alerta se a criptografia em trânsito não estiver habilitada.

O Amazon EMR é um serviço da web que facilita a execução de frameworks de big data, como o Apache Hadoop, para processar e analisar dados. O Amazon EMR permite que você processe grandes quantidades de dados de forma econômica executando etapas de mapeamento e redução em paralelo.

A criptografia de dados impede que usuários não autorizados acessem ou leiam dados em repouso ou dados em trânsito. Dados em repouso se referem aos dados armazenados em mídias, como um sistema de arquivos local em cada nó, o Sistema de Arquivos Distribuído do Hadoop (HDFS) ou o Sistema de Arquivos do EMR (EMRFS) por meio do Amazon Simple Storage Service (Amazon S3). Dados em trânsito se referem aos dados que viajam pela rede e estão em trânsito entre as tarefas. A criptografia em trânsito oferece suporte a recursos de criptografia de código aberto para Apache Spark, Apache TEZ, Apache Hadoop, Apache e Presto. HBase Você habilita a criptografia criando uma configuração de segurança a partir da AWS Command Line Interface (AWS CLI), do console ou da SDKs AWS e especificando as configurações de criptografia de dados. Você pode fornecer os artefatos de criptografia para criptografia em trânsito por meio de uma das formas a seguir:

- Ao fazer o upload de um arquivo compactado de certificados no Amazon S3.
- Ao fazer referência a uma classe Java personalizada que fornece artefatos de criptografia.

O controle de segurança incluído nesse padrão monitora as chamadas de API e gera um evento Amazon CloudWatch Events sobre a RunJobFlowação. O evento chama uma função do AWS Lambda, que executa um script Python. A função obtém o ID do cluster EMR da entrada JSON do evento e executa as seguintes verificações para determinar se há uma violação de segurança:

- Verifica se o cluster EMR tem uma configuração de segurança específica do Amazon EMR.
- Se o cluster tiver uma configuração de segurança, verifique se a criptografia em trânsito está habilitada.

- Se o cluster não tiver uma configuração de segurança, enviará um alerta para um endereço de e-mail que você fornecer usando o Amazon Simple Notification Service (Amazon SNS). A notificação especifica o nome do cluster do EMR, os detalhes da violação, as informações da conta e da região da AWS e o ARN do AWS Lambda (Amazon Resource Name) do qual a notificação foi originada.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do S3 para fazer o upload do código do Lambda fornecido com este padrão.
- Um endereço de e-mail no qual você deseja receber notificações de violação.
- Log do Amazon EMR ativado, para acesso a todos os logs da API.

Limitações

- Esse controle de detecção é regional e deve ser implantado em cada região da AWS que você deseja monitorar.

Versões do produto

- Versão 4.8.0 e posterior do Amazon EMR.

Arquitetura

Arquitetura de fluxo de trabalho

Automação e escala

- Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar o modelo em várias contas que você deseja monitorar.

Ferramentas

Serviços da AWS

- Amazon EMR: o Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de Big Data, como o Apache Hadoop e o Apache Spark, na AWS, para processar e analisar grandes volumes de dados. Ao usar essas estruturas e projetos de código aberto relacionados, é possível processar dados para finalidades analíticas e workloads de inteligência de negócios. Além disso, é possível usar o Amazon EMR para transformar e mover grandes volumes de dados para dentro e fora de outros armazenamentos de dados e bancos de dados da AWS, como o Amazon S3 e o Amazon DynamoDB.
- AWS Cloudformation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em várias contas e regiões da AWS.
- Eventos do AWS Cloudwatch — A Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem as mudanças nos recursos da AWS. CloudWatch Os eventos ficam cientes das mudanças operacionais à medida que elas ocorrem e tomam medidas corretivas conforme necessário, enviando mensagens para responder ao ambiente, ativando funções, fazendo alterações e capturando informações de estado.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e escala automaticamente, desde algumas solicitações por dia a milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- AWS SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que coordena e gerencia o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

Esse padrão inclui um anexo com dois arquivos:

- `EMRInTransitEncryption.zip` é um arquivo compactado que inclui o controle de segurança (código Lambda).
- `EMRInTransitEncryption.yml`é um CloudFormation modelo que implanta o controle de segurança.

Consulte a seção Tópicos para obter informações sobre como usar esses arquivos.

Épicos

Implemente o controle de segurança

Tarefa	Descrição	Habilidades necessárias
Faça upload do código para um bucket do S3.	Crie um novo bucket do S3 ou use um bucket do S3 existente para carregar o arquivo `EMRInTransitEncryption.zip` anexado (código do Lambda). Esse bucket deve estar na mesma região da AWS que o CloudFormation modelo e os recursos que você deseja avaliar.	Arquiteto de nuvem
Implante o CloudFormation modelo.	Abra o console do Cloudformation na mesma região da AWS do bucket S3 e implante o arquivo `EMRInTransitEncryption.yml` fornecido no anexo. No próximo épico, forneça valores para os parâmetros do modelo.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Dar o nome do bucket do S3.	Insira o nome do bucket do S3 que você criou ou selecionou no primeiro épico. Esse bucket do S3 contém o arquivo.zip do código Lambda e deve estar na mesma região da AWS do CloudFormation modelo e do recurso que será avaliado.	Arquiteto de nuvem
Forneça a chave do S3.	Espeça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `EMRInTransitEncryption.zip` ou `controls/EMRInTransitEncryption.zip`).	Arquiteto de nuvem
Fornecer um endereço de e-mail.	Forneça um endereço de e-mail ativo no qual você deseja receber notificações de violação.	Arquiteto de nuvem
Especifique um nível de registro em log.	Especifique o nível de registro em log e a verbosidade para os logs do Lambda. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo e deve ser usado somente para depuração. `Error` designa eventos de erro que ainda podem permitir que o aplicativ	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	o continue em execução. `Warning` designa situações potencialmente prejudiciais.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirme a assinatura por e-mail.	Quando o CloudFormation modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail que você forneceu. Você precisa confirmar sua assinatura para começar a receber as notificações.	Arquiteto de nuvem

Recursos relacionados

- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- Opções de criptografia (documentação do Amazon EMR)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Monitore ElastiCache clusters da Amazon para criptografia em repouso

Criado por Susanne Kangnoh (AWS)

Resumo

ElastiCache A Amazon é um serviço da Amazon Web Services (AWS) que fornece uma solução de cache de alto desempenho, escalável e econômica para distribuir um armazenamento de dados na memória ou um ambiente de cache na nuvem. Ele recupera dados de armazenamentos de dados na memória de alto throughput e baixa latência. Essa funcionalidade o torna uma escolha popular para casos de uso em tempo real, como armazenamento em cache, armazenamentos de sessões, jogos, serviços geoespaciais, análises em tempo real e filas. ElastiCache oferece armazenamentos de dados Redis e Memcached, ambos com tempos de resposta inferiores a um milissegundo.

A criptografia de dados ajuda a impedir que usuários não autorizados leiam dados em um cluster e em sistemas de armazenamento de dados em cache associados. Isso inclui dados salvos em mídias persistentes, conhecidos como dados em repouso, e dados que podem ser interceptados enquanto viajam pela rede entre servidores cache e clientes, conhecidos como dados em trânsito.

Você pode ativar a criptografia em repouso ElastiCache para o Redis ao criar um grupo de replicação, definindo o AtRestEncryptionEnabledparâmetro como verdadeiro. Quando esse parâmetro está habilitado, ele criptografa o disco durante as operações de sincronização, backup e troca, além de criptografar os backups armazenados no Amazon Simple Storage Service (Amazon S3). Não é possível habilitar a criptografia em repouso em grupos de replicação existentes. Ao criar um grupo de replicação, você pode habilitar a criptografia em repouso de duas maneiras:

- Ao escolher a opção Padrão, que usa criptografia em repouso gerenciada por serviços.
- Ao usar uma chave gerenciada pelo cliente e fornecer o ID da chave ou o nome do recurso da Amazon (ARN) do AWS Key Management Service (AWS KMS).

Esse padrão fornece um controle de segurança que monitora as chamadas de API e gera um evento Amazon CloudWatch Events na CreateReplicationGroupoperação. Esse evento chama uma função do Lambda AWS, que executa um script Python. A função obtém o ID do grupo de replicação da entrada JSON do evento e executa as seguintes verificações para determinar se há uma violação de segurança:

- Verifica se a AtRestEncryptionEnabledchave existe.

- Se AtRestEncryptionEnabledexistir, verifica o valor para ver se é verdadeiro.
- Se o AtRestEncryptionEnabledvalor for definido como false, define uma variável que rastreia violações e envia uma mensagem de violação para um endereço de e-mail fornecido por você, usando uma notificação do Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Um bucket do S3 para fazer o upload do código do Lambda fornecido.
- Um endereço de e-mail no qual você deseja receber notificações de violação.
- ElastiCache registro ativado, para acesso a todos os registros da API.

Limitações

- Esse controle de detecção é regional e deve ser implantado em cada região da AWS que você deseja monitorar.
- O controle é compatível com grupos de replicação que executam em uma nuvem privada virtual (VPC).
- O controle fornece suporte a grupos de replicação que estão executando os seguintes tipos de nós:
  - R5, R4, R3
  - M5, M4, M3
  - T3, T2

Versões do produto

- ElastiCache para Redis versão 3.2.6 ou posterior

Arquitetura

Arquitetura de fluxo de trabalho

Automação e escala

- Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

Serviços da AWS

- Amazon ElastiCache — A Amazon ElastiCache facilita a configuração, o gerenciamento e a escalabilidade de ambientes distribuídos de cache na memória na nuvem da AWS. Ele fornece um cache na memória de alto desempenho, redimensionável e econômico, ao mesmo tempo em que remove a complexidade associada à implantação e ao gerenciamento de um ambiente de cache distribuído. ElastiCache funciona com os mecanismos Redis e Memcached.
- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Você pode gerenciar e provisionar pilhas em várias contas e regiões da AWS.
- Eventos do AWS Cloudwatch — A Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem as mudanças nos recursos da AWS. CloudWatch Os eventos ficam cientes das mudanças operacionais à medida que elas ocorrem e tomam medidas corretivas conforme necessário, enviando mensagens para responder ao ambiente, ativando funções, fazendo alterações e capturando informações de estado.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e escala automaticamente, desde algumas solicitações por dia a milhares por segundo. Você paga apenas pelo tempo de computação consumido. Não haverá cobranças quando o código não estiver em execução.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que coordena e gerencia o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

Esse padrão inclui um anexo com dois arquivos:

- `ElasticCache-EncryptionAtRest.zip` é um arquivo compactado que inclui o controle de segurança (código Lambda).
- `elasticache_encryption_at_rest.yml`é um CloudFormation modelo que implanta o controle de segurança.

Consulte a seção Tópicos para obter informações sobre como usar esses arquivos.

Épicos

Implemente o controle de segurança

Tarefa	Descrição	Habilidades necessárias
Faça upload do código para um bucket do S3.	Crie um novo bucket do S3 ou use um bucket do S3 existente para carregar o arquivo `ElastiCache-EncryptionAtRest.zip` anexado (código do Lambda). Esse bucket deve estar na mesma região da AWS que os recursos que você deseja avaliar.	Arquiteto de nuvem
Implante o CloudFormation modelo.	Abra o console do Cloudformation na mesma região da AWS do bucket S3 e implante o arquivo `elasticache_encryption_at_rest.yml` fornecido no anexo. No próximo épico, forneça valores para os parâmetros do modelo.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Dar o nome do bucket do S3.	Insira o nome do bucket do S3 que você criou ou selecionou no primeiro épico. Esse bucket do S3 contém o arquivo.zip do código Lambda e deve estar na mesma região da AWS do CloudFormation modelo e do recurso que será avaliado.	Arquiteto de nuvem
Fornecer a chave do S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `ElasticCache-EncryptionAtRest.zip` ou `controls/ElasticCache-EncryptionAtRest.zip`).	Arquiteto de nuvem
Fornecer um endereço de e-mail.	Forneça um endereço de e-mail ativo no qual você deseja receber notificações de violação.	Arquiteto de nuvem
Especifique um nível de log.	Especifique o nível de registro em log e a verbosidade. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo e deve ser usado somente para depuração. `Error` designa eventos de erro que ainda podem permitir que o aplicativ	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	o continue em execução. `Warning` designa situações potencialmente prejudiciais.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirme a assinatura por e-mail.	Quando o CloudFormation modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail que você forneceu. Você precisa confirmar sua assinatura para começar a receber as notificações.	Arquiteto de nuvem

Recursos relacionados

- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- Criptografia em repouso ElastiCache para Redis (documentação da Amazon ElastiCache)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Monitore pares de chaves de EC2 instância usando o AWS Config

Criado por Wassim Benhallam (AWS), Sergio Bilbao Lopez (AWS) e Vikrant Telkar (AWS)

Resumo

Ao iniciar uma instância do Amazon Elastic Compute Cloud (Amazon EC2) na Amazon Web Services (AWS) Cloud, a melhor prática é criar ou usar um par de chaves existente para se conectar à instância. O par de chaves, que consiste em uma chave pública armazenada na instância e uma chave privada fornecida ao usuário, permite acesso seguro por meio do Secure Shell (SSH) à instância e evita o uso de senhas. No entanto, às vezes, os usuários podem iniciar instâncias inadvertidamente sem anexar um par de chaves. Como os pares de chaves só podem ser atribuídos durante a execução de uma instância, é importante identificar e sinalizar rapidamente como não compatíveis todas as instâncias lançadas sem pares de chaves. Isso é particularmente útil quando se trabalha em contas ou ambientes que exigem o uso de pares de chaves para acesso de instância.

Esse padrão descreve como criar uma regra personalizada no AWS Config para monitorar pares de chaves de EC2 instância. Quando as instâncias são identificadas como não compatíveis, um alerta é enviado usando notificações do Amazon Simple Notification Service (Amazon SNS) iniciadas por meio de um evento da Amazon. EventBridge

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- O AWS Config está habilitado para a região da AWS que você deseja monitorar e configurado para registrar todos os recursos da AWS

Limitações

- Essa solução é específica para a região. Todos os recursos devem ser criados na mesma região da AWS.

Arquitetura

Pilha de tecnologias de destino

- AWS Config
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Arquitetura de destino

1. O AWS Config inicia a regra.
2. A regra invoca a função Lambda para avaliar a conformidade das instâncias. EC2
3. A função do Lambda envia o estado de conformidade atualizado para o AWS Config.
4. O AWS Config envia um evento para. EventBridge
5. EventBridge publica notificações de alteração de conformidade em um tópico do SNS.
6. O Amazon SNS envia um alerta por e-mail.

Automação e escala

A solução pode monitorar qualquer número de EC2 instâncias em uma região.

Ferramentas

Ferramentas

- AWS Config: o AWS Config é um serviço que permite avaliar, auditar e verificar as configurações dos recursos da AWS. O AWS Config monitora e registra continuamente suas configurações de recursos da AWS e permite automatizar a avaliação das configurações registradas em relação às configurações desejadas.
- Amazon EventBridge — EventBridge A Amazon é um serviço de ônibus de eventos sem servidor para conectar seus aplicativos com dados de várias fontes.
- AWS Lambda: o AWS Lambda é um serviço de computação com tecnologia sem servidor que oferece suporte à execução de código sem provisionar ou gerenciar servidores, criar uma lógica de escalabilidade de cluster com reconhecimento de workload, manter integrações de eventos ou gerenciar runtimes.

- Amazon SNS — O Amazon Simple Notification Service (Amazon SNS) é um serviço de mensagens totalmente gerenciado para comunicação (A2A) application-to-application e (A2P). application-to-person

Código

O código da função do Lambda segue anexo.

Épicos

Crie uma função Lambda para avaliar a conformidade da Amazon EC2

Tarefa	Descrição	Habilidades necessárias
Crie um perfil do AWS Identity and Access Management (IAM) para o Lambda.	No Console de Gerenciamento da AWS, escolha IAM e, em seguida, crie a função, usando o Lambda como entidade confiável e adicionando as permissões `AmazonEventBridgeFullAccess` e `AWSConfigRulesExecutionRole`. Para obter mais informações, consulte a documentação da AWS.	DevOps
Criar e implantar as funções do Lambda.	1. No console Lambda, crie uma função usando o Author from scratch, com o Python 3.6 como runtime e o perfil do IAM criado anteriormente. Anote o nome de recurso da Amazon (ARN). 2. Na guia Código, escolha `lambda_function.py`	DevOps

Tarefa	Descrição	Habilidades necessárias
	e cole o código que está anexado a esse padrão. 3. Para salvar suas alteraçõe s, selecione Implementar.	

Crie uma regra personalizada do AWS Config

Tarefa	Descrição	Habilidades necessárias
Adicione uma regra personali zada do AWS Config.	No console do AWS Config, adicione uma regra personali zada usando as seguintes configurações: • ARN: o ARN da função do Lambda criada anteriorm ente • Tipo de trigger: alterações da configuração • Escopo das mudanças: recursos • Tipo de recurso — EC2 instância da Amazon Para obter mais informações, consulte a documentação da AWS.	DevOps

Configurar notificações por e-mail quando um evento de alteração de conformidade for detectado

Tarefa	Descrição	Habilidades necessárias
Crie o tópico do SNS e inscrição	No console do Amazon SNS do Amazon, crie um tópico usando Standard como o tipo e, em seguida, crie uma assinatura usando E-mail como protocolo. Quando você o receber o e-mail de confirmação, escolha o link para confirmar a assinatura. Para obter mais informações, consulte a documentação da AWS.	DevOps
Crie uma EventBridge regra para iniciar as notificações do Amazon SNS.	No EventBridge console, crie uma regra usando as seguintes configurações: • Nome do serviço: AWS Config • Tipo de evento: alteração de conformidade das regras de configuração • Tipo de mensagem — Tipos de mensagem específicos, ComplianceChangeNotification • Nome específico da regra: o nome da sua regra do AWS Config criada anteriormente	DevOps

Tarefa	Descrição	Habilidades necessárias
	• Alvo: tópico do SNS, seu tópico criado anteriormente Para obter mais informações, consulte a documentação da AWS.	

Verifique a regra e as notificações

Tarefa	Descrição	Habilidades necessárias
Crie EC2 instâncias.	Crie duas EC2 instâncias de qualquer tipo e anexe um par de chaves e crie uma EC2 instância sem um par de chaves.	DevOps
Verificar a regra.	1. No console do AWS Config, na página Regras, selecione sua regra. 2. Para ver EC2 instância s compatíveis e não compatíveis, altere Recursos no escopo para Todos. Verifique se duas instâncias estão listadas como compatíveis e se uma instância está listada como não compatível. 3. Aguarde para receber uma notificação por e-mail do Amazon SNS sobre o	DevOps

Tarefa	Descrição	Habilidades necessárias
	estado de conformidade das EC2 instâncias.	

Recursos relacionados

- Criar uma função para delegar permissões a um serviço da AWS
- Criação de uma regra personalizada no AWS Config
- Criar um tópico do Amazon SNS
- Assinar tópico do Amazon SNS
- Crie uma regra na Amazon EventBridge

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Monitorar a atividade do usuário raiz do IAM

Criado por Mostefa Brougui (AWS)

Resumo

Cada conta da Amazon Web Services (AWS) tem um usuário raiz. Como prática recomendada de segurança para o AWS Identity and Access Management (IAM), recomendamos usar o usuário raiz para concluir as tarefas que somente o usuário raiz pode executar. Para obter a lista completa, consulte Tarefas que exigem credenciais de usuário raiz no Guia de Referência do Gerenciamento de Conta Compartilhado da AWS. Como o usuário raiz tem acesso total a todos os seus recursos e informações de faturamento da AWS, recomendamos que você não use essa conta e a monitore em busca de qualquer atividade, o que possa indicar que as credenciais do usuário raiz foram comprometidas.

Ao usar esse padrão, você configura uma arquitetura orientada por eventos que monitora o usuário raiz do IAM. Esse padrão configura uma hub-and-spoke solução que monitora várias contas da AWS, as contas spoke, e centraliza o gerenciamento e os relatórios em uma única conta, a conta hub.

Quando as credenciais do usuário raiz do IAM são usadas, a Amazon CloudWatch e a AWS CloudTrail registram a atividade no log e na trilha, respectivamente. Na conta spoke, uma EventBridge regra da Amazon envia o evento para o ônibus central de eventos na conta do hub. Na conta do hub, uma EventBridge regra envia o evento para uma função do AWS Lambda. A função usa um tópico do Amazon Simple Notification Service (Amazon SNS) que notifica você sobre a atividade do usuário raiz.

Nesse padrão, você usa um CloudFormation modelo da AWS para implantar os serviços de monitoramento e tratamento de eventos nas contas spoke. Você usa um modelo do HashiCorp Terraform para implantar os serviços de gerenciamento de eventos e notificação na conta do hub.

Pré-requisitos e limitações

Pré-requisitos

1. Permissões para implantar recursos da AWS em seu ambiente da AWS.
2. Permissões para implantar conjuntos CloudFormation de pilhas. Para obter mais informações, consulte Pré-requisitos para operações de conjunto de pilhas (documentação). CloudFormation
3. Terraform instalado e pronto para uso. Para obter mais informações, consulte Conceitos básicos – AWS (Documentação do Terraform).

4. Uma trilha existente em cada relato do spoke. Para obter mais informações, consulte Conceitos básicos da AWS CloudTrail (CloudTrail documentação).
5. A trilha está configurada para enviar eventos para o CloudWatch Logs. Para obter mais informações, consulte Envio de eventos para o CloudWatch Logs (CloudTrail documentação).
6. Suas contas hub e spoke devem ser gerenciadas pela AWS Organizations.

Arquitetura

O diagrama a seguir ilustra os componentes básicos da implementação.

1. Quando as credenciais do usuário raiz do IAM são usadas, CloudWatch CloudTrail registre a atividade no registro e na trilha, respectivamente.
2. Na conta spoke, uma EventBridge regra envia o evento para o barramento central de eventos na conta do hub.
3. Na conta do hub, uma EventBridge regra envia o evento para uma função Lambda.
4. A função do Lambda usa um tópico do Amazon SNS que notifica você sobre a atividade do usuário raiz.

Ferramentas

Serviços da AWS

- CloudFormationA AWS ajuda você a configurar recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida em todas as contas e regiões da AWS.
- CloudTrailA AWS ajuda você a auditar a governança, a conformidade e o risco operacional da sua conta da AWS.
- O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas, aplicativos e serviços da AWS para que você possa monitorá-los e arquivá-los com segurança.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, funções do Lambda, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outras contas da AWS.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.

- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- O Amazon Simple Notification Service (Amazon SNS) ajuda você a coordenar e gerenciar a troca de mensagens entre publicadores e clientes, incluindo servidores web e endereços de e-mail.

Outras ferramentas e serviços

- O Terraform é um aplicativo CLI para provisionar e gerenciar a infraestrutura e os recursos da nuvem usando código, na forma de arquivos de configuração.

Repositório de código

O código-fonte e os modelos desse padrão estão disponíveis em um GitHub repositório. Esse padrão fornece dois modelos:

- Um modelo do Terraform contendo os recursos que você implanta na conta do hub
- Um CloudFormation modelo que você implanta como uma instância de conjunto de pilhas nas contas spoke

O repositório tem a estrutura geral a seguir.

```
.
 |__README.md
 |__spoke-stackset.yaml
 |__hub.tf
 |__root-activity-monitor-module
     |__main.tf  # contains Terraform code to deploy resources in the Hub account
     |__iam      # contains IAM policies JSON files
         |__ lambda-assume-policy.json          # contains trust policy of the IAM role
 used by the Lambda function
         |__ lambda-policy.json                 # contains the IAM policy attached to
 the IAM role used by the Lambda function
     |__outputs  # contains Lambda function zip code
```

A seção Epics fornece step-by-step instruções para implantar os modelos.

Épicos

Implante recursos na conta do hub

Tarefa	Descrição	Habilidades necessárias
Clone o repositório de código de amostra.	1. Abra o repositório do AWS IAM Root User Activity Monitor. 2. Na guia Código, acima da lista de arquivos, escolha Código e copie o URL HTTPS. 3. Em uma interface da linha de comando, altere seu diretório de trabalho para o local em que você deseja armazenar os arquivos de amostra. 4. Digite o comando: `git clone <repoURL>`	AWS geral
Atualize o modelo do Terraform.	1. Recupere o ID da organização. Para obter instruções, consulte Visualização de detalhes de uma organização na conta de gerenciamento (documentação do AWS Organizations). 2. No repositório clonado, abra `hub.tf`. 3. Atualize o seguinte com os valores adequados para seu ambiente:	AWS geral

Tarefa	Descrição	Habilidades necessárias
	• `OrganizationId` : adicione o ID da sua organização. • `SNSTopicName` : adicione um nome para o tópico do Amazon SNS. • `SNSSubscriptions` : adicione o e-mail para o qual as notificações do Amazon SNS devem ser enviadas. • `Region`: adicione o código da região da AWS em que você está implantando os recursos. Por exemplo, `.eu-west-1` • `Tags`: adicione suas tags. Para obter mais informações, consulte Marcar recursos da AWS com tags (Referência geral da AWS). 4. Salve e feche o arquivo `hub.tf`.	

Tarefa	Descrição	Habilidades necessárias

Implantar os recursos na conta do hub da AWS.	1. Na interface de linha de comando do Terraform, navegue até a pasta raiz do repositório clonado e digite o comando a seguir.
	`terraform init && terraform plan`
	2. Revise a saída e confirme que você deseja criar os recursos descritos.
	3. Insira o comando da a seguir.
	`terraform apply`
	4. Quando solicitado, confirme a implantação inserindo `yes`.
		AWS geral

Implante recursos em suas contas spoke

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	1. Faça login no Console de Gerenciamento da AWS e abra o console do CloudFormation . 2. No painel de navegação, escolha StackSets. 3. Na parte superior da StackSetspágina, escolha Criar StackSet.	AWS geral

Tarefa	Descrição	Habilidades necessárias
	4. Em Permissões, escolha Permissões gerenciadas pelo serviço. CloudFormation configura automaticamente as permissões necessárias para implantação nas contas de destino gerenciadas pelo AWS Organizations. 5. Em Pré-requisito: prepare o modelo, escolha O modelo está pronto. 6. Em Especificar modelo, escolha Fazer upload de um arquivo de modelo. 7. Selecione Escolher arquivo e, em seguida, no repositório clonado, selecione `spoke-stackset.yaml` . 8. Escolha Próximo. 9. Na página Especificar StackSet detalhes, insira um nome para o conjunto de pilhas. 10. Em Parâmetros, insira o ID da conta do hub e escolha Avançar. 11. Na página Configurar StackSet opções, em Tags, adicione suas tags. 12. Em Configuração de execução, escolha Inativo	

Tarefa	Descrição	Habilidades necessárias
	e, em seguida, escolha Avançar. 13. Na página Definir opções de implantação, especifiq ue as unidades organizac ionais e as regiões nas quais você deseja implantar o conjunto de pilhas e escolha Avançar. 14. Na página de revisão, selecione Eu reconheço que a AWS CloudFormation pode criar recursos do IAM e, em seguida, escolha Enviar. CloudFormation começa a implantar seu conjunto de pilhas. Para obter mais informações e instruções, consulte Criar um conjunto de pilhas (CloudFor mation documentação).	

(Opcional) Teste as notificações

Tarefa	Descrição	Habilidades necessárias
Use as credenciais do usuário raiz.	1. Faça login em uma conta spoke ou na conta hub usando as credenciais do usuário raiz. 2. Confirme se a conta de e-mail especificada recebe	AWS geral

Tarefa	Descrição	Habilidades necessárias
	a notificação do Amazon SNS.	

Recursos relacionados

- Melhores práticas de segurança (Documentação do IAM)
- Trabalhando com StackSets (CloudFormation documentação)
- Comece agora (Documentação do Terraform)

Mais informações

GuardDutyA Amazon é um serviço contínuo de monitoramento de segurança que analisa e processa registros para identificar atividades inesperadas e potencialmente não autorizadas em seu ambiente da AWS. Como alternativa a essa solução, se você tiver ativado GuardDuty, ela poderá alertá-lo quando as credenciais do usuário raiz forem usadas. A GuardDuty descoberta é`Policy:IAMUser/RootCredentialUsage`, e a severidade padrão é Baixa. Para obter mais informações, consulte Gerenciando GuardDuty as descobertas da Amazon.

Enviar uma notificação quando um usuário do IAM for criado

Criado por Mansi Suratwala (AWS) e Sergiy Shevchenko (AWS)

Resumo

Na Amazon Web Services (AWS), você pode usar esse padrão para implantar um CloudFormation modelo da AWS para receber notificações automaticamente quando usuários do AWS Identity and Access Management (IAM) forem criados.

Usando o IAM, você pode gerenciar o acesso aos serviços e recursos da AWS com segurança. Você pode criar e gerenciar usuários e grupos da AWS e usar permissões para permitir e negar o acesso deles aos recursos da AWS.

O CloudFormation modelo cria um evento Amazon CloudWatch Events e uma função do AWS Lambda. O evento usa CloudTrail a AWS para monitorar qualquer usuário do IAM que está sendo criado na conta da AWS. Se um usuário for criado, o evento CloudWatch Events inicia uma função Lambda, que envia uma notificação do Amazon Simple Notification Service (Amazon SNS) informando sobre o evento de criação do novo usuário.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma CloudTrail trilha da AWS criada e implantada

Limitações

- O CloudFormation modelo da AWS deve ser implantado `CreateUser` somente para.

Arquitetura

Pilha de tecnologias de destino

- IAM
- AWS CloudTrail
- CloudWatch Eventos da Amazon

- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Arquitetura de destino

Automação e escala

Você pode usar o CloudFormation modelo da AWS várias vezes para diferentes regiões e contas da AWS. Você precisa executá-lo apenas uma vez em cada região ou conta. Para automatizar a implantação em várias contas, use a AWS CloudFormation StackSets. O CloudFormation modelo poderá implantar todos os recursos necessários em cada conta.

Ferramentas

Ferramentas

- IAM: o AWS Identity and Access Management (IAM) é um serviço da web que ajuda você a controlar o acesso aos recursos da AWS com segurança. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.
- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da Amazon Web Services para que você possa passar menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos que são executados na AWS. Você cria um modelo que descreve todos os recursos da AWS que você deseja e CloudFormation se encarrega de provisionar e configurar esses recursos para você.
- AWS CloudTrail — CloudTrail A AWS ajuda você a gerenciar a governança, a conformidade e a auditoria operacional e de risco da sua conta da AWS. As ações realizadas por um usuário, uma função ou um serviço da AWS são registradas como eventos em CloudTrail. Os eventos incluem ações realizadas no Console de Gerenciamento da AWS, na Interface de Linha de Comando da AWS SDKs e na AWS APIs e.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um near-real-time fluxo de eventos do sistema que descrevem as mudanças nos recursos da AWS.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia até milhares por segundo.

- Amazon S3: o Amazon Simple Storage Service (Amazon S3) serve como armazenamento para a internet. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens usando Lambda, HTTP, e-mail, notificações push móveis e mensagens de texto móveis (SMS).

Código

Um arquivo .zip do projeto está disponível como anexo.

Épicos

Crie o bucket do S3 para o script do Lambda

Tarefa	Descrição	Habilidades necessárias
Defina o bucket do S3.	Abra o console do Amazon S3, escolha ou crie um bucket do S3. Esse bucket do S3 hospedará o arquivo .zip do código do Lambda. O nome do bucket do S3 não pode conter barras iniciais.	Arquiteto de nuvem

Carregar o código do Lambda para o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Faça o upload do código do Lambda.	Faça upload do arquivo .zip do código Lambda fornecido na seção Anexos para o bucket do S3 que você definiu.	Arquiteto de nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo.	No CloudFormation console, implante o CloudFormation `createIAMuser.yaml` modelo fornecido como anexo a esse padrão. No próximo épico, forneça valores para os parâmetros do modelo.	Arquiteto de nuvem

Preencha os parâmetros no CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Dê o nome do bucket do S3.	Insira o nome do bucket do S3 que você criou ou escolheu no primeiro épico.	Arquiteto de nuvem
Forneça a chave do S3.	Forneça a localização do arquivo .zip do código Lambda em seu bucket do S3, sem barras iniciais (por exemplo, `<directory>/<file-name>.zip`).	Arquiteto de nuvem
Forneça um endereço de e-mail.	Forneça um endereço de e-mail ativo para receber notificações do Amazon SNS.	Arquiteto de nuvem
Defina o nível de registro em log.	Defina o nível de registro em log e a frequência da sua função do Lambda. `Info` designa mensagens informativas detalhadas sobre o progresso do aplicativo.	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	`Error` designa eventos de erro que ainda podem permitir que o aplicativo continue em execução. `Warning` designa situações potencialmente prejudiciais.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o modelo é implantado com sucesso, ele envia uma mensagem de e-mail de assinatura para o endereço de e-mail fornecido. Você precisa confirmar sua assinatura para começar a receber as notificações.	Arquiteto de nuvem

Recursos relacionados

- Criar uma trilha
- Criar um bucket do S3
- Fazer upload de arquivos em um bucket do S3
- Implantando um modelo CloudFormation
- Criar um usuário do IAM.
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS CloudTrail

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Impeça o acesso à Internet no nível da conta usando uma política de controle de serviços

Criado por Sergiy Shevchenko (AWS), Sean O'Sullivan (AWS) e Victor Mazeo Whitaker (AWS)

Resumo

Frequentemente, as organizações desejam limitar o acesso à Internet aos recursos da conta que devem permanecer privados. Nessas contas, os recursos em nuvens privadas virtuais (VPCs) não devem acessar a Internet de forma alguma. Muitas organizações escolhem uma arquitetura de inspeção centralizada. Para o tráfego leste-oeste (VPC para VPC) em uma arquitetura de inspeção centralizada, você precisa garantir que as contas spoke e seus recursos não tenham acesso à Internet. Para tráfego norte-sul (saída da Internet e local), você deseja permitir o acesso à Internet somente por meio da VPC de inspeção.

Esse padrão usa uma política de controle de serviço (SCP) para ajudar a impedir o acesso à Internet. Você pode aplicar esse SCP no nível da conta ou da unidade organizacional (OU). O SCP limita a conectividade com a Internet impedindo o seguinte:

- Criação ou conexão de um gateway de IPv6 internet IPv4 ou gateway que permita acesso direto à Internet à VPC
- Criar ou aceitar uma conexão de emparelhamento de VPC que pode permitir acesso indireto à Internet por meio de outra VPC
- Criação ou atualização de uma AWS Global Acceleratorconfiguração que possa permitir acesso direto à Internet aos recursos da VPC

Pré-requisitos e limitações

Pré-requisitos

- Um ou vários Contas da AWS gerenciados como uma organização em AWS Organizations.
- Todos os recursos estão habilitados em AWS Organizations.
- SCPs estão habilitados na organização.
- Permissões para:
  - Acesse a conta de gerenciamento da organização.

- Crie SCPs. Para obter mais informações sobre as permissões mínimas, consulte Criando um SCP.
- Anexe o SCP às contas ou unidades organizacionais de destino (OUs). Para obter mais informações sobre as permissões mínimas, consulte Anexar e desanexar políticas de controle de serviço.

Limitações

- SCPs não afetam usuários ou funções na conta de gerenciamento. Elas afetam apenas as contas-membro de sua organização.
- SCPs afetam somente usuários e funções AWS Identity and Access Management (IAM) que são gerenciados por contas que fazem parte da organização. Para obter mais informações, consulte Efeitos do SCP sobre as permissões.

Ferramentas

Serviços da AWS

- AWS Organizationsé um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente. Nesse padrão, você usa políticas de controle de serviço (SCPs) em AWS Organizations.
- A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Práticas recomendadas

Depois de estabelecer esse SCP em sua organização, certifique-se de atualizá-lo com frequência para abordar quaisquer novos recursos Serviços da AWS ou recursos que possam afetar o acesso à Internet.

Épicos

Crie e anexe o SCP

Tarefa	Descrição	Habilidades necessárias
Crie o SCP.	1. Faça login no console do AWS Organizations. Você deve entrar na conta de gerenciamento da organização. 2. No painel esquerdo, escolha Políticas. 3. Na página de políticas , escolha Políticas de controle de serviço. 4. Na página Service control policies (Políticas de controle de serviço), escolha Create policy (Criar política). 5. Na página Criar nova política de controle de serviço, insira um nome da política e uma descrição opcional da política. 6. (Opcional) Adicione AWS tags à sua política. 7. No editor JSON, exclua a política de espaço reservado. 8. Cole a política a seguir no editor de JSON. `{`	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias

	<pre>{
	  "Version":
	 "2012-10-17",
	  "Statement": [
	  {
	  "Action": [
	  "ec2:Atta
	chInternetGateway",
	  "ec2:Crea
	teInternetGateway",
	
	  "ec2:Crea
	teVpcPeeringConnec
	tion",
	  "ec2:Acce
	ptVpcPeeringConnec
	tion",
	  "ec2:Crea
	teEgressOnlyIntern
	etGateway"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  },
	  {
	  "Action": [
	  "globalac
	celerator:Create*",
	  "globalac
	celerator:Update*"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  }
	  ]
	}</pre>
	9. Escolha Criar política.	

Tarefa	Descrição	Habilidades necessárias
Conecte o SCP.	1. Na página Políticas de controle de serviços, escolha a política que você criou. 2. Na guia Targets (Alvos), selecione Attach (Anexar). 3. Selecione a OU ou a conta à qual você deseja anexar a política. Talvez seja necessário expandir o OUs para encontrar a OU ou a conta que você deseja. 4. Escolha Anexar política.	Administrador da AWS

Recursos relacionados

- AWS Organizations documentação
- Políticas de controle de serviços (SCPs)
- Arquitetura de inspeção centralizada com AWS Gateway Load Balancer AWS Transit Gateway e AWS (postagem no blog)

Restrinja o acesso com base no endereço IP ou geolocalização usando AWS WAF

Criado por Louis Hourcade (AWS)

Resumo

AWS WAFé um firewall de aplicativos da Web que ajuda a proteger os aplicativos da Web APIs contra explorações e bots comuns da Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos. As listas de controle de acesso à Web (web ACLs) AWS WAF fornecem controle sobre como o tráfego chega aos seus aplicativos. Em uma ACL da web, você adiciona regras ou grupos de regras projetados para permitir tráfego legítimo, controlar o tráfego de bots e bloquear padrões de ataque comuns. Para obter mais informações, consulte Como AWS WAF funciona.

Você pode associar os seguintes tipos de regras à sua AWS WAF web ACLs:

- Grupos de regras AWS gerenciadas — equipes e AWS Marketplace vendedores de regras gerenciadas oferecem conjuntos de regras pré-configurados. Alguns grupos de regras gerenciados são projetados para ajudar a proteger tipos específicos de aplicativos da Web. Outros oferecem ampla proteção contra ameaças conhecidas ou vulnerabilidades comuns.
- Regras personalizadas e grupos de regras personalizados — Você também pode criar regras e grupos de regras que personalizam o acesso aos seus aplicativos web APIs e. Por exemplo, você pode restringir o tráfego com base em uma lista específica de endereços IP ou em uma lista de países.

Usando esse padrão e o repositório de código associado, você pode usar o AWS Cloud Development Kit (AWS CDK)para implantar a AWS WAF web ACLs com regras personalizadas. Essas regras restringem o acesso aos recursos do aplicativo web com base no endereço IP ou na geolocalização do usuário final. Opcionalmente, você também pode anexar vários grupos de regras gerenciados.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Permissões para implantar AWS WAF recursos

- AWS CDK, instalado e configurado em sua conta
- Git, instalado

Limitações

- Você pode usar esse padrão somente Regiões da AWS onde AWS WAF estiver disponível. Para ver a disponibilidade da região, consulte Serviços da AWS por região.

Ferramentas

Serviços da AWS

- AWS Cloud Development Kit (AWS CDK)é uma estrutura de desenvolvimento de software que ajuda você a definir e provisionar Nuvem AWS infraestrutura em código.
- AWS WAFé um firewall de aplicativo web que ajuda você a monitorar solicitações HTTP e HTTPS que são encaminhadas para seus recursos protegidos de aplicativos web.

Repositório de código

O código desse padrão está disponível na restrição de GitHub IP e geolocalização com AWS WAF repositório. O código implanta duas AWS WAF web ACLs. A primeira é uma ACL web regional destinada aos recursos do Amazon API Gateway. A segunda é a ACL global da web para CloudFront recursos da Amazon. Ambos os sites ACLs contêm as seguintes regras personalizadas:

- `IPMatch`bloqueia solicitações de endereços IP não permitidos.
- `GeoMatch`bloqueia solicitações de países não permitidos.

Durante a implantação, você pode, opcionalmente, anexar todos os seguintes grupos de regras gerenciadas à sua web ACLs:

- Conjunto de regras básicas (CRS) — Esse grupo de regras contém regras que geralmente são aplicáveis a aplicativos da Web. Ele ajuda a proteger contra a exploração de uma ampla variedade de vulnerabilidades, incluindo algumas das vulnerabilidades de alto risco e comuns descritas nas publicações do OWASP, como o OWASP Top 10.
- Proteção do administrador — Esse grupo de regras contém regras que ajudam a bloquear o acesso externo às páginas administrativas expostas.

- Entradas incorretas conhecidas — Esse grupo de regras ajuda a bloquear padrões de solicitação que são reconhecidamente inválidos e estão associados à exploração ou descoberta de vulnerabilidades.
- Lista de reputação de IP da Amazon — Esse grupo de regras contém regras baseadas na inteligência interna de ameaças da Amazon. Ele ajuda você a bloquear endereços IP normalmente associados a bots ou outras ameaças.
- Grupo de regras gerenciadas pelo sistema operacional Linux — Esse grupo de regras ajuda a bloquear padrões de solicitação associados à exploração de vulnerabilidades do Linux, incluindo ataques de inclusão local de arquivos (LFI) específicos do Linux.
- Grupo de regras gerenciadas do banco de dados SQL — Esse grupo de regras ajuda a bloquear padrões de solicitação associados à exploração de bancos de dados SQL, como ataques de injeção de SQL.

Épicos

Configurar a AWS WAF web ACLs

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Digite o comando a seguir para clonar a restrição de IP e geolocalização com o AWS WAF repositório na sua estação de trabalho local: `git clone https://github.com/aws-samples/ip-and-geolocation-restriction-with-waf-cdk.git`	Git
Configure as regras.	1. No repositório clonado, abra o arquivo app.py. 2. Modifique os valores das seguintes variáveis para personalizar as regras:	AWS geral, Python

Tarefa	Descrição	Habilidades necessárias

	<pre>aws_acccount = "AWS_ACCOUNT"
	region = "AWS_REGION"
	ip_list = ["CIDR_RANGE_1", "CIDR_RANGE_2"]
	geo_list = ["COUNTRY_CODE_1", "COUNTRY_CODE_2"]
	aws_managed_rules = True</pre>
	Em que:
	• `aws_account` é o ID do alvo Conta da AWS.
	• `region`oné o destino da Web ACL Região da AWS para recursos do API Gateway.
	Note
	A ACL da web para CloudFront recursos é global e será implantada na `us-east-1` região.
	• `ip_list`é a lista de intervalos de CIDR que têm acesso permitido.
	• `geo_list`é a lista de países que têm acesso	

Tarefa	Descrição	Habilidades necessárias
	permitido. Para valores válidos, consulte a AWS WAF documentação. • `aws_managed_rules` controla se os grupos de regras gerenciadas são adicionados à ACL da web. Se esse valor for`True`, eles serão adicionados. Se esse valor for`False`, eles serão excluídos. 3. Salve e feche o arquivo app.py.	

Inicialize e implante o código

Tarefa	Descrição	Habilidades necessárias
Inicialize seu AWS ambiente.	Se ainda não tiver feito isso, você precisará inicializar seu AWS ambiente antes de poder implantar o AWS CDK aplicativo. 1. Na AWS CDK CLI, digite o seguinte comando para inicializar a região: `us-east-1` `cdk bootstrap aws://<account-id>/us-east-1`	AWS geral

Tarefa	Descrição	Habilidades necessárias
	2. Se você estiver implantando a ACL da web para o API Gateway em uma região diferente de `us-east-1`, digite o seguinte comando para inicializar a região de destino: `cdk bootstrap aws://<account-id>/<region>`	
Implante o AWS CDK aplicativo.	1. Insira o comando a seguir para implantar o AWS CDK aplicativo: `cdk deploy --all` 2. Espere até que a implantação da AWS CloudFormation pilha seja concluída.	AWS geral

Valide a implantação

Tarefa	Descrição	Habilidades necessárias
Confirme se a web ACLs foi implantada com sucesso.	1. Faça login no e AWS Management Console, em seguida, abra o AWS WAF console. 2. No painel de navegação, escolha Web ACLs. 3. Na lista de Regiões da AWS, escolha Global (CloudFront).	AWS geral

Tarefa	Descrição	Habilidades necessárias
	4. Verifique se a nova ACL CloudFront da web foi implantada e confirme se ela tem o endereço IP e as regras de geolocalização que você definiu. O nome padrão dessa ACL da web é `WebACLCloudfront-<ID>` . 5. Na lista de Regiões da AWS, escolha a região na qual você implantou a pilha. 6. Verifique se uma nova ACL da web para recursos do API Gateway foi implantada. Confirme se ele tem o endereço IP e as regras de geolocalização que você definiu. O nome padrão dessa ACL da web é `WebACLApiGW-<ID>` .	

Tarefa	Descrição	Habilidades necessárias
(Opcional) Associe a web ACLs aos seus recursos.	Associe a AWS WAF web ACLs aos seus AWS recursos, como um Application Load Balancer, API Gateway ou CloudFront distribuição. Para obter instruções, consulte Associando ou desassociando uma ACL da web com um recurso.AWS Para obter um exemplo, consulte class CfnWeb ACLAssociation (construct) na AWS CDK documentação.	AWS geral

Limpar os recursos

Tarefa	Descrição	Habilidades necessárias
Exclua as pilhas.	1. Desassocie a ACL da web de qualquer AWS recurso. Para obter instruções, consulte a AWS WAF documentação. 2. Na AWS CDK CLI, digite o comando a seguir para excluir o AWS CDK aplicativo. `cdk destroy --all`	AWS geral

Recursos relacionados

- Referência da API (AWS CDK documentação)

- aws-cdk-libmódulo.aws_wafv2 (documentação)AWS CDK
- Trabalhando com a web ACLs (AWS WAF documentação)
- Gerenciando seus próprios grupos de regras (AWS WAF documentação)
- Regras (AWS WAF documentação)

Examine os repositórios Git em busca de informações confidenciais e problemas de segurança usando git-secrets

Criado por Saurabh Singh (AWS)

Resumo

Esse padrão descreve como usar a ferramenta de código aberto git-secrets do Labs AWS para escanear os repositórios de origem do Git e encontrar códigos que possam incluir informações confidenciais, como senhas de usuário ou chaves de AWS acesso, ou que tenham outros problemas de segurança.

`git-secrets` verifica confirmações, mensagens de confirmação e fusão para evitar que informações confidenciais, como segredos, sejam adicionadas aos seus repositórios Git. Por exemplo, se uma confirmação, mensagem de confirmação ou qualquer confirmação em um histórico de fusão corresponder a um de seus padrões de expressão regular proibidos e configurados, a confirmação será rejeitada.

Pré-requisitos e limitações

Pré-requisitos

- Um ativo Conta da AWS
- Um repositório Git que requer uma verificação de segurança
- Um cliente Git (versão 2.37.1 e superior) instalado

Arquitetura

Arquitetura de destino

- Git
- `git-secrets`

Ferramentas

- A git-secrets é uma ferramenta que impede que você envie informações confidenciais nos repositórios Git.
- O Git é um sistema de código aberto de controle de versão distribuído.

Práticas recomendadas

- Sempre verifique um repositório Git incluindo todas as revisões:

```
git secrets --scan-history
```

Épicos

Conecte-se a uma EC2 instância

Tarefa	Descrição	Habilidades necessárias
Conecte-se a uma EC2 instância usando SSH.	Conecte-se a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) usando SSH e um arquivo de par de chaves. Você pode ignorar esta etapa se estiver verificando um repositório em sua máquina local.	AWS geral

Instale o Git.

Tarefa	Descrição	Habilidades necessárias
Instale o Git.	Instale o Git usando o comando:	AWS geral

Tarefa	Descrição	Habilidades necessárias
	`yum install git -y` Se você estiver usando sua máquina local, poderá instalar um cliente Git para uma versão específica do sistema operacional. Para obter mais informações, acesse o site do Git.	

Clone o repositório de origem e instale git-secrets

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório de origem do Git.	Para clonar o repositório Git que você deseja verificar, escolha o comando clonar Git no seu diretório inicial.	AWS geral
Clone git-secrets.	Clone o repositório git `git-secrets` . `git clone https://github.com/awslabs/git-secrets.git` Coloque `git-secrets` em algum lugar no seu PATH para que o Git o pegue quando você executa `git-secrets` .	AWS geral
Instalar git-secrets.	Para Unix e variantes (Linux/ macOS):	AWS geral

Tarefa	Descrição	Habilidades necessárias

	Você pode usar o destino `install` do `Makefile` (fornecido no repositório `git-secrets`) para instalar a ferramenta. Você pode personalizar o caminho de instalação usando as variáveis `PREFIX` e `MANPREFIX` .
	`make install`
	Para Windows:
	Execute o PowerShel l `install.ps1` script fornecido no `git-secrets` repositório. Esse script copia os arquivos de instalação para um diretório de instalação (`%USERPROFILE%/.git-secrets` por padrão) e adiciona o diretório ao usuário atual `PATH`.
	`PS > ./install.ps1`
	Para Homebrew (usuários do macOS):
	Execute:
	`brew install git-secrets`	

Digitalizar o repositório de código git

Tarefa	Descrição	Habilidades necessárias
Acesse o repositório de origem.	Alterne para o diretório do repositório Git que você deseja verificar: `cd my-git-repository`	AWS geral
Registre o conjunto de regras da AWS (Git hooks).	Para configurar `git-secrets` para verificar seu repositório Git em cada commit, execute o comando: `git secrets --register-aws`	AWS geral
Verificar o repositório.	Execute o comando a seguir para iniciar a verificação do seu repositório: `git secrets --scan`	AWS geral

Analise o arquivo de saída.	A ferramenta gera um arquivo de saída se encontrar uma vulnerabilidade no seu repositório Git. Por exemplo:
	`example.sh:4:AWS_SECRET_ACCESS_KEY = *********`
	
	`[ERROR] Matched one or more prohibited patterns`
	
	`Possible mitigations:`
		AWS geral

Tarefa	Descrição	Habilidades necessárias
	- Mark false positives as allowed using: git config --add secrets.allowed ... - Mark false positives as allowed by adding regular expressions to .gitallowed at repository's root directory - List your configured patterns: git config --get-all secrets.patterns - List your configured allowed patterns: git config --get-all secrets.allowed - List your configured allowed patterns in .gitallowed at repository's root directory - Use --no-verify if this is a one-time false positive	

Recursos relacionados

- ferramenta git-secrets

Envie alertas do AWS Network Firewall para um canal do Slack

Criado por Venki Srivatsav (AWS) e Aromal Raj Jayarajan (AWS)

Resumo

Esse padrão descreve como implantar um firewall usando o Firewall de Rede da Amazon Web Services (AWS) com o modelo de implantação distribuída e como propagar os alertas gerados pelo AWS Network Firewall para um canal configurável do Slack.

Padrões de conformidade como o Payment Card Industry Data Security (PCI DSS) exigem que você instale e mantenha um firewall para proteger os dados do cliente. Na Nuvem AWS, uma nuvem privada virtual (VPC) é considerada o mesmo que uma rede física no contexto desses requisitos de conformidade. Você pode usar o Firewall de Rede para monitorar o tráfego de rede entre VPCs e proteger suas cargas de trabalho que são executadas VPCs regidas por um padrão de conformidade. O Network Firewall bloqueia o acesso ou gera alertas quando detecta o acesso não autorizado de outras pessoas VPCs na mesma conta. No entanto, o Network Firewall suporta um número limitado de destinos para a entrega dos alertas. Esses destinos incluem buckets do Amazon Simple Storage Service (Amazon S3), grupos de log da Amazon CloudWatch e fluxos de entrega do Amazon Data Firehose. Qualquer ação adicional sobre essas notificações requer análise off-line usando o Amazon Athena ou o Amazon Kinesis.

Esse padrão fornece um método para propagar alertas gerados pelo Firewall de Rede para um canal configurável do Slack para ações adicionais quase em tempo real. Você também pode estender a funcionalidade a outros mecanismos de alerta PagerDuty, como Jira e e-mail. (Essas personalizações estão fora do escopo desse padrão.)

Pré-requisitos e limitações

Pré-requisitos

- Canal do Slack (consulte Primeiros passos na Central de ajuda do Slack)
- Privilégios necessários para enviar uma mensagem ao canal
- O URL do endpoint do Slack com um token de API (selecione seu aplicativo e escolha um webhook de entrada para ver seu URL; para obter mais informações, consulte Criação de um webhook de entrada na documentação da API do Slack)
- Uma instância de teste do Amazon Elastic Compute Cloud (Amazon EC2) nas sub-redes de carga de trabalho

- Regras de teste no Network Firewall
- Tráfego real ou simulado para acionar as regras de teste
- Um bucket S3 para armazenar os arquivos de origem a serem implantados

Limitações

- Atualmente, essa solução suporta apenas um único intervalo de roteamento entre domínios sem classe (CIDR) como filtro para origem e destino. IPs

Arquitetura

Pilha de tecnologias de destino

- Uma VPC
- Quatro sub-redes (duas para o firewall e duas para cargas de trabalho)
- Gateway da Internet
- Quatro tabelas de rotas com regras
- Bucket S3 usado como destino de alerta, configurado com uma política de bucket e configurações de eventos para executar uma função do Lambda
- Função do Lambda com uma função de execução para enviar notificações do Slack
- Segredo do AWS Secrets Manager para armazenar a URL do Slack
- Firewall de rede com configuração de alertas
- Canal do Slack

Todos os componentes, exceto o canal Slack, são provisionados pelos CloudFormation modelos e pela função Lambda que são fornecidos com esse padrão (consulte a seção Código).

Arquitetura de destino

Esse padrão configura um firewall de rede descentralizado com integração com o Slack. Essa arquitetura consiste em uma VPC com duas zonas de disponibilidade. A VPC inclui duas sub-redes protegidas e duas sub-redes de firewall com endpoints de firewall de rede. Todo o tráfego que entra e sai das sub-redes protegidas pode ser monitorado por meio da criação de políticas e regras de firewall. O firewall de rede está configurado para colocar todos os alertas em um bucket do S3. Esse bucket do S3 está configurado para chamar uma função do Lambda ao receber um evento `put`. A

função Lambda busca a URL configurada do Slack no Secrets Manager e envia a mensagem de notificação para o espaço de trabalho do Slack.

Para obter mais informações sobre essa arquitetura, consulte a postagem do blog da AWS Modelos de implantação para o AWS Network Firewall.

Ferramentas

Serviços da AWS

- O Firewall de Rede da AWS é um firewall de rede gerenciado e monitorado, além de um serviço de detecção e prevenção de intrusões VPCs na Nuvem AWS. Você pode usar o Firewall para filtrar o tráfego no perímetro da VPC e proteger suas workloads na AWS.
- O AWS Secrets Manager é um serviço para armazenamento e recuperação de credenciais. O Secrets Manager permite a substituição de credenciais codificadas no seu código, incluindo senhas, por uma chamada de API para o Secrets Manager para recuperar o segredo de forma programática. Esse padrão usa o Secrets Manager para armazenar o URL do Slack.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objeto. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web. Esse padrão usa o Amazon S3 para armazenar os CloudFormation modelos e o script Python para a função Lambda. Ele também usa um bucket do S3 como destino de alerta de firewall de rede.
- CloudFormationA AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente. Esse padrão usa CloudFormation a AWS para implantar automaticamente uma arquitetura distribuída para o Firewall Manager.

Código

O código desse padrão está disponível em GitHub, no repositório Network Firewall Slack Integration. Na pasta `src` do repositório, você encontrará:

- Um conjunto de CloudFormation arquivos no formato YAML. Você usa esses modelos para provisionar os componentes desse padrão.

- Um arquivo de origem em Python (`slack-lambda.py`) para criar a função do Lambda.
- Um pacote de implantação com arquivo .zip (`slack-lambda.py.zip`) para carregar o código de função do Lambda.

Para usar esses arquivos, siga as instruções da próxima seção.

Épicos

Configurar o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Criar um bucket do S3.	1. Faça login no AWS Management Console e abra o console do Amazon S3 em. https://console.aws.amazon.com/s3/ 2. Escolha ou crie um bucket do S3 para hospedar o código. Um nome de bucket do S3 é globalmente exclusivo, e o namespace é compartilhado por todas as contas da AWS. O nome do bucket do S3 não pode incluir barras iniciais. Recomendamos que você use um prefixo para organizar o código desse padrão. Para obter mais informações, consulte Criar um bucket na documentação do Amazon S3.	Desenvolvedor do aplicativo, proprietário do aplicativo, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
Faça o upload dos CloudFormation modelos e do código Lambda.	1. Faça o download dos seguintes arquivos do GitHub repositório para esse padrão: • `base.yml` • `igw-ingress-route.yml` • `slack-lambda.py` • `slackLambda.yml` • `decentralized-deployment.yml` • `protected-subnet-route.yml` • `slack-lambda.py.zip` 2. Faça upload dos arquivos no bucket do S3 criado.	Desenvolvedor do aplicativo, proprietário do aplicativo, administrador da nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo.	Abra o CloudFormation console da AWS na mesma região da AWS do seu bucket do S3 e implante o modelo`base.yml`. Esse modelo cria os recursos da AWS e as funções do Lambda necessários para que os alertas sejam transmitidos ao canal do Slack.	Desenvolvedor do aplicativo, proprietário do aplicativo, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informaçõ es sobre a implantação CloudFormation de modelos, consulte Como criar uma pilha no CloudFormation console da AWS na CloudFormation documentação.	
Preencha os parâmetros no modelo.	Especifique valores de parâmetros e o nome da pilha. Para obter uma lista de parâmetros, suas descriçõe s e valores padrão, consulte CloudFormation parâmetro s na seção Informações adicionais.	Desenvolvedor do aplicativ o, proprietário do aplicativo, administrador da nuvem
Crie a pilha.	1. Revise os detalhes da pilha e atualize os valores com base nos requisitos do seu ambiente. 2. Selecione Criar pilha para implantar o modelo.	Desenvolvedor do aplicativ o, proprietário do aplicativo, administrador da nuvem

Verifique a solução

Tarefa	Descrição	Habilidades necessárias
Teste a implantação.	Use o CloudFormation console da AWS ou a AWS Command Line Interface (AWS CLI) para verificar se os recursos listados na seção da pilha de tecnologia do Target foram criados.	Desenvolvedor do aplicativ o, proprietário do aplicativo, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias
	Se o CloudFormation modelo não for implantado com êxito, verifique os valores fornecidos para os `pAvailabilityZone2` parâmetros `pAvailabilityZone1` e. Eles devem ser apropriados para a região da AWS na qual você está implantando a solução. Para obter uma lista de zonas de disponibilidade para cada região, consulte Regiões e zonas na EC2 documentação da Amazon.	

Tarefa	Descrição	Habilidades necessárias

Teste a funcionalidade.	1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
	
	2. Crie uma EC2 instância em uma das sub-redes protegidas. Escolha um Amazon Linux 2 AMI (HVM) para usar como servidor HTTPS. Para obter instruções, consulte Iniciar uma instância na EC2 documentação da Amazon.
	
	Note
	O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs.
	
	3. Use os seguintes dados do usuário para instalar um servidor web na EC2 instância:
	
	`#!/bin/bash`
	`yum install httpd -y`
	`systemctl start httpd`
	`systemctl stop firewalld`
	`cd /var/www/html`
		Desenvolvedor do aplicativo, proprietário do aplicativo, administrador da nuvem

Tarefa	Descrição	Habilidades necessárias

	`echo "Hello!! this is a NFW alert test page, 200 OK" > index.html`
	
	4. Crie as seguintes regras de firewall de rede:
	
	Regra sem estado:
	
	`Source: 0.0.0.0/0`
	`Destination 10.0.3.65 /32 (private IP of the EC2 instance)`
	`Action: Forward`
	
	Regra com estado:
	
	`Protocol: HTTP`
	`Source ip/port: Any / Any`
	`Destination ip/port: Any /Any`
	
	5. Obtenha o IP público do servidor Web criado na etapa 3.
	
	6. Acesse o IP público em um navegador. Você deve ver a seguinte mensagem no navegador:
	
	`Hello!! this is a NFW alert test page, 200 OK`
	
	Você também receberá uma notificação no canal do Slack.	

Tarefa	Descrição	Habilidades necessárias
	A notificação pode ser adiada, dependendo do tamanho da mensagem. Para fins de teste, considere fornecer um filtro CIDR que não seja muito estreito (por exemplo, um valor CIDR com /32 seria considerado muito estreito e /8 seria muito amplo). Para obter mais informações, consulte a seção Comportamento do filtro em Informações adicionais.	

Recursos relacionados

- Modelos de implantação para o AWS Network Firewall (publicação no blog da AWS)
- AWS Network Firewall (documentação da AWS)
- Integração com o Firewall de Rede com o Slack (GitHub repositório)
- Crie um espaço de trabalho do Slack (Central de ajuda do Slack)

Mais informações

CloudFormation parameters

Parâmetro	Descrição	Valor padrão ou de amostra
`pVpcName`	O nome do VPC a ser criado.	Inspeção
`pVpcCidr`	O intervalo CIDR para a VPC criar.	10.0.0.0/16
`pVpcInstanceTenancy`	Como EC2 as instâncias são distribuídas em todo o hardware físico. As opções	padrão

	são `default` (locação compartilhada) ou `dedicated` (locação única).	
`pAvailabilityZone1`	A primeira zona de disponibilidade para a infraestrutura.	us-east-2a
`pAvailabilityZone2`	A segunda zona de disponibilidade para a infraestrutura.	us-east-2b
`pNetworkFirewallSubnet1Cidr`	O intervalo CIDR para a primeira sub-rede do firewall (mínimo /28).	10.0.1.0/24
`pNetworkFirewallSubnet2Cidr`	O intervalo CIDR para a segunda sub-rede do firewall (mínimo /28).	10.0.2.0/24
`pProtectedSubnet1Cidr`	O intervalo CIDR para a primeira sub-rede protegida (workload).	10.0.3.0/24
`pProtectedSubnet2Cidr`	O intervalo CIDR para a segunda sub-rede protegida (workload).	10.0.4.0/24
`pS3BucketName`	O nome do bucket do S3 existente onde você carregou o código-fonte do Lambda.	nós-w2- yourname-lambda-functions
`pS3KeyPrefix`	O prefixo do bucket do S3 em que você fez o upload do código-fonte do Lambda.	aod-test
`pAWSSecretName4Slack`	O nome do segredo que contém a URL do Slack.	SlackEnpoint-Cfn
`pSlackChannelName`	O nome do canal do Slack criada.	somename-notifications

`pSlackUserName`	Nome de usuário do Slack.	Usuário do Slack
`pSecretKey`	Isso pode ser qualquer chave. Recomendamos que você use o padrão.	webhookUrl
`pWebHookUrl`	O valor do URL do Slack.	https://hooks.slack.com/services/T??? 9º?? /A031885 JRM7 /9D4Y??????
`pAlertS3Bucket`	O nome do bucket do S3 a ser usado como destino de alerta de firewall de rede. Esse bucket será criado para você.	nós-w2- yourname-security-aod-alerts
`pSecretTagName`	O nome da etiqueta do segredo.	AppName
`pSecretTagValue`	O valor da tag para o nome da tag especificada.	LambdaSlackIntegration
`pdestCidr`	O filtro para o intervalo CIDR de destino. Para obter mais informações, consulte a próxima sessão, Comportamento do filtro.	10.0.0.0/16
`pdestCondition`	O sinalizador para indicar se a correspondência de destino deve ser excluída ou incluída. Para obter mais informações, consulte a próxima seção. Os valores válidos são `include` e `exclude`.	include

`psrcCidr`	O filtro do intervalo CIDR de origem a ser alertado. Para obter mais informações, consulte a próxima seção.	118.2.0.0/16
`psrcCondition`	O sinalizador para excluir ou incluir a correspondência de origem. Para obter mais informações, consulte a próxima seção.	include

Comportamento do filtro

Se você não configurou nenhum filtro no AWS Lambda, todos os alertas gerados serão enviados para o seu canal do Slack. A origem e o destino IPs dos alertas gerados são comparados com os intervalos de CIDR que você configurou ao implantar o modelo. CloudFormation Se uma correspondência é encontrada, a condição é aplicada. Se a origem ou o destino estiverem dentro do intervalo CIDR configurado e pelo menos um deles estiver configurado com a condição `include`, um alerta será gerado. As tabelas a seguir fornecem exemplos de valores, condições e resultados do CIDR.

	CIDR configurado	IP de alerta	Configured	Alerta
Origem	10.0.0.0/16	10.0.0.25	include	Sim
Destination (Destino)	10.0.0.0/16	202.0.0.13	include	

	CIDR configurado	IP de alerta	Configured	Alerta
Origem	10.0.0.0/16	10.0.0.25	exclude	Não
Destination (Destino)	10.0.0.0/16	202.0.0.13	include	

	CIDR configurado	IP de alerta	Configured	Alerta
Origem	10.0.0.0/16	10.0.0.25	include	Sim
Destination (Destino)	10.0.0.0/16	100.0.0.13	include	

	CIDR configurado	IP de alerta	Configured	Alerta
Origem	10.0.0.0/16	90.0.0.25	include	Sim
Destination (Destino)	Null	202.0.0.13	include	

	CIDR configurado	IP de alerta	Configured	Alerta
Origem	10.0.0.0/16	90.0.0.25	include	Não
Destination (Destino)	10.0.0.0/16	202.0.0.13	include	

Simplificar o gerenciamento de certificados privados usando a CA privada da AWS e o AWS RAM

Criado por Everett Hinckley (AWS) e Vivek Goyal (AWS)

Resumo

Usar a AWS Private Certificate Authority (CA privada da AWS) para emitir certificados privados para autenticar recursos internos e assinar código de computador. Esse padrão fornece um CloudFormation modelo da AWS para a rápida implantação de uma hierarquia de CA de vários níveis e uma experiência de provisionamento consistente. Opcionalmente, você pode usar o AWS Resource Access Manager (AWS RAM) para compartilhar com segurança a CA dentro de suas organizações ou unidades organizacionais (OUs) no AWS Organizations e centralizar a CA enquanto usa a AWS RAM para gerenciar permissões. Não há necessidade de uma CA privada em todas as contas, então essa abordagem economiza seu dinheiro. Além disso, é possível usar o Amazon Simple Storage Service (Amazon S3) para armazenar a lista de revogação de certificados (CRL) e os logs de acesso.

Essa implementação fornece estes atributos e benefícios:

- Centraliza e simplifica o gerenciamento da hierarquia da CA privada usando a CA privada da AWS.
- Exporta certificados e chaves para dispositivos gerenciados pelo cliente na AWS e on-premises.
- Usa um CloudFormation modelo da AWS para uma implantação rápida e uma experiência de provisionamento consistente.
- Cria uma CA raiz privada junto com uma hierarquia de CA subordinada de 1, 2, 3 ou 4.
- Opcionalmente, usa o AWS RAM para compartilhar a CA subordinada da entidade final com outras contas no nível da organização ou da OU.
- Economiza dinheiro ao eliminar a necessidade de uma CA privada em todas as contas usando o AWS RAM.
- Cria um bucket do S3 opcional para a CRL.
- Cria um bucket do S3 opcional para logs de acesso da CRL.

Pré-requisitos e limitações

Pré-requisitos

Se você quiser compartilhar a CA dentro de uma estrutura do AWS Organizations, identifique ou configure o seguinte:

- Uma conta de segurança para criar a hierarquia e o compartilhamento da CA.
- Uma OU ou conta separada para teste.
- Compartilhamento habilitado na conta de gerenciamento do AWS Organizations. Para obter mais informações, consulte Habilitar compartilhamento de recursos com o AWS Organizations na documentação do RAM.

Limitações

- CAs são recursos regionais. Todos CAs residem em uma única conta da AWS e em uma única região da AWS.
- Não há suporte para certificados e chaves gerados pelo usuário. Para este caso de uso, recomendamos que você personalize essa solução para usar uma CA raiz externa.
- O bucket público de CRL é incompatível. Recomendamos que você mantenha a CRL privada. Se o acesso à Internet à CRL for necessário, consulte a seção sobre como usar a Amazon CloudFront para servir CRLs em Habilitando o recurso S3 Block Public Access (BPA) na documentação da CA privada da AWS.
- Esse padrão implementa uma abordagem de região única. Se você precisar de uma autoridade de certificação multirregional, poderá implementar subordinados em uma segunda região da AWS ou on-premises. Essa complexidade está fora do escopo deste padrão, porque a implementação depende do seu caso de uso específico, do volume da workload, das dependências e dos requisitos.

Arquitetura

Pilha de tecnologias de destino

- CA privada da AWS
- AWS RAM
- Amazon S3
- AWS Organizations
- AWS CloudFormation

Arquitetura de destino

Esse padrão fornece duas opções de compartilhamento com o AWS Organizations:

Opção 1: criar o compartilhamento em nível da organização. Todas as contas na organização podem emitir os certificados privados usando a CA compartilhada, conforme mostrado no diagrama a seguir.

Opção 2: criar o compartilhamento em nível de unidade da organização (OU). Somente as contas na OU especificada podem emitir os certificados privados usando a CA compartilhada. Por exemplo, no diagrama a seguir, se o compartilhamento for criado no nível de OU Sandbox, tanto o Desenvolvedor 1 quanto o Desenvolvedor 2 poderão emitir certificados privados usando a CA compartilhada.

Ferramentas

Serviços da AWS

- CA privada da AWS: a Autoridade de certificação privada da AWS (CA privada da AWS) é um serviço de CA privada hospedado para emitir e revogar certificados digitais privados. Ele ajuda você a criar hierarquias de CA privadas, incluindo raiz e subordinada CAs, sem os custos de investimento e manutenção da operação de uma CA local.
- AWS RAM — O AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar com segurança seus recursos entre contas da AWS e dentro de sua organização ou OUs em organizações da AWS. Para reduzir a sobrecarga operacional em um ambiente com várias contas, você pode criar um recurso e usar o AWS RAM para compartilhar esse recurso entre contas.
- AWS Organizations: o AWS Organizations é um serviço de gerenciamento de contas que ajuda você a consolidar várias contas da AWS em uma organização que você cria e gerencia de maneira centralizada.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web. Esse padrão usa o Amazon S3 para armazenar a lista de revogação de certificados (CRL) e os logs de acesso.
- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente.

Esse padrão usa CloudFormation a AWS para implantar automaticamente uma hierarquia de CA de vários níveis.

Código

O código-fonte desse padrão está disponível no GitHub repositório hierárquico de CA privada da AWS. O repositório inclui:

- O CloudFormation modelo da AWS`ACMPCA-RootCASubCA.yaml`. Você pode usar esse modelo para implantar a hierarquia da CA para essa implementação.
- Arquivos de teste para casos de uso, como solicitação, exportação, descrição e exclusão de um certificado.

Para usar esses arquivos, siga as instruções na seção Épicos.

Épicos

Arquitetar a hierarquia da CA

Tarefa	Descrição	Habilidades necessárias
Coletar informações sobre o sujeito do certificado.	Colete informações do sujeito do certificado sobre o proprietário do certifica do: nome da organização, unidade organizacional, país, estado, localidade e nome comum.	Arquiteto de nuvem, arquiteto de segurança, engenheiro de PKI
Coletar informações opcionais sobre o AWS Organizations.	Se a CA fizer parte de uma estrutura do AWS Organizat ions e você quiser compartil har a hierarquia da CA dentro dessa estrutura, colete o número da conta de gerenciamento, o ID da organização e, opcionalm	Arquiteto de nuvem, arquiteto de segurança, engenheiro de PKI

Tarefa	Descrição	Habilidades necessárias
	ente, o ID da OU (se você quiser compartilhar a hierarquia da CA somente com uma OU específica). Além disso, determine as contas do AWS Organizations ou OUs, se houver, com as quais você deseja compartilhar a CA.	
Criar a hierarquia da CA.	Determine qual conta abrigará a raiz e a subordinada. CAs Determine quantos níveis subordinados a hierarquia exige entre os certificados raiz e da entidade final. Para obter mais informações, consulte Criar uma hierarquia de CA na documentação da CA privada da AWS.	Arquiteto de nuvem, arquiteto de segurança, engenheiro de PKI
Determinar as convenções de nomenclatura e marcação para a hierarquia da CA.	Determine os nomes dos recursos da AWS: a CA raiz e cada CA subordinada. Determine quais tags devem ser atribuídas a cada CA.	Arquiteto de nuvem, arquiteto de segurança, engenheiro de PKI

Tarefa	Descrição	Habilidades necessárias
Determine os algoritmos de criptografia e assinatura necessários.	Determine o seguinte: • Os requisitos do algoritmo de criptografia da sua organização para as chaves públicas que sua CA usa ao emitir um certificado. O padrão é RSA_2048. • O algoritmo chave que sua CA usa para assinatura de certificados. O padrão é SHA256 WITHRSA.	Arquiteto de nuvem, arquiteto de segurança, engenheiro de PKI
Determinar os requisitos de revogação de certificados para a hierarquia da CA.	Se forem necessários recursos de revogação de certificados, estabeleça uma convenção de nomenclatura para o bucket do S3 que contém a lista de revogação de certificados (CRL).	Arquiteto de nuvem, arquiteto de segurança, engenheiro de PKI
Determinar os requisitos de registro em log para a hierarquia da CA.	Se forem necessários recursos de registro em log de acesso, estabeleça uma convenção de nomenclatura para o bucket do S3 que contém os logs de acesso.	Arquiteto de nuvem, arquiteto de segurança, engenheiro de PKI

Tarefa	Descrição	Habilidades necessárias
Determinar os períodos de expiração do certificado.	Determine a data de expiração do certificado raiz (o padrão é 10 anos), dos certificados da entidade final (o padrão é 13 meses) e dos certificados de CA subordinados (o padrão é 3 anos). Os certificados de CA subordinados devem expirar antes dos certifica dos de CA em níveis mais altos na hierarquia. Para obter mais informações, consulte Gerenciar o ciclo de vida da CA privada na documentação da CA privada da AWS.	Arquiteto de nuvem, arquiteto de segurança, engenheiro de PKI

Implantar a hierarquia da CA

Tarefa	Descrição	Habilidades necessárias
Concluir os pré-requisitos.	Conclua as etapas na seção Pré-requisitos deste padrão.	Administrador de nuvem, engenheiros de segurança, engenheiros de PKI
Criar funções de CA para várias pessoas.	1. Determine os tipos de funções ou usuários do AWS Identity and Access Management (IAM) no AWS IAM Identity Center (sucessor do AWS Single Sign-On) necessários para administrar os vários níveis da hierarquia da CA, como CAAdmin Root, Subordina	Administrador de nuvem, engenheiros de segurança, engenheiros de PKI

Tarefa	Descrição	Habilidades necessárias
	te e. CAAdmin Certificate Consumer 2. Determine a granularidade das políticas necessárias para separar as tarefas. 3. Crie os perfis ou usuários do IAM necessários no IAM Identity Center na conta em que a hierarquia da CA reside.	
Implante a CloudFormation pilha.	1. No GitHub repositório desse padrão, baixe o modelo AWSPCA-RootCASubCA .yaml. 2. Implante o modelo a partir do CloudFormation console da AWS ou da AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Como trabalhar com pilhas na CloudFormation documentação. 3. Preencha os parâmetros no modelo, incluindo o nome da organização, o nome da OU, o algoritmo de chave, o algoritmo de assinatura e outras opções.	Administrador de nuvem, engenheiros de segurança, engenheiros de PKI

Tarefa	Descrição	Habilidades necessárias
Arquitetar uma solução para atualizar certificados usados por recursos gerenciados pelo usuário.	Recursos de serviços integrados da AWS, como o Elastic Load Balancing , atualizam os certificados automaticamente antes da expiração. No entanto, recursos gerenciados pelo usuário, como servidores web que estão sendo executados em instâncias do Amazon Elastic Compute Cloud EC2 (Amazon), exigem outro mecanismo. 1. Determine quais recursos gerenciados pelo usuário exigem certificados de entidade final da CA privada. 2. Planeje um processo para ser notificado sobre a expiração dos recursos e certificados gerenciados pelo usuário. Para obter exemplos, consulte o seguinte: • Usar uma regra gerenciada do AWS Config • Usando a Amazon CloudWatch e a Amazon EventBridge 3. Crie scripts personalizados para atualizar certificados	Administrador de nuvem, engenheiros de segurança, engenheiros de PKI

Tarefa	Descrição	Habilidades necessárias
	em recursos gerenciados pelo usuário e integre-os aos serviços da AWS para automatizar as atualizaç ões. Para obter mais informações sobre os serviços integrados da AWS, consulte Serviços integrados ao AWS Certificate Manager na documentação do ACM.	

Validar e documentar a hierarquia da CA

Tarefa	Descrição	Habilidades necessárias
Validar o compartilhamento opcional de RAM da AWS.	Se a hierarquia da CA for compartilhada com outras contas no AWS Organizat ions, faça login em uma dessas contas no Console de Gerenciamento da AWS, navegue até o Console da CA privada da AWS e confirme se a CA recém-criada está compartilhada com essa conta. Somente a CA de nível mais baixo na hierarqui a estará visível, porque é a CA que gera os certificados da entidade final. Repita o procedimento para obter uma amostra das contas com as quais a CA é compartilhada.	Administrador de nuvem, engenheiros de segurança, engenheiros de PKI

Tarefa	Descrição	Habilidades necessárias
Validar a hierarquia da CA com testes de ciclo de vida do certificado.	No GitHub repositório desse padrão, localize os testes do ciclo de vida. Execute os testes na AWS CLI para solicitar um certificado, exportar um certificado, descrever um certificado e excluir um certificado.	Administrador de nuvem, engenheiros de segurança, engenheiros de PKI
Importar a cadeia de certificados para lojas confiáveis.	Para que navegadores e outros aplicativos confiem em um certificado, o emissor do certificado deve ser incluído no repositório confiável do navegador, que é uma lista de confiáveis CAs. Adicione a cadeia de certificados da nova hierarquia de CA ao armazenamento confiável do seu navegador e do aplicativo. Confirme se os certificados da entidade final são confiáveis.	Administrador de nuvem, engenheiros de segurança, engenheiros de PKI

Tarefa	Descrição	Habilidades necessárias
Criar um runbook para documentar a hierarquia da CA.	Crie um documento do runbook para descrever a arquitetura da hierarquia da CA, a estrutura da conta que pode solicitar certificados de entidade final, o processo de criação e as tarefas básicas de gerenciamento, como emissão de certificados de entidade final (a menos que você queira permitir o autoatendimento por contas secundárias), uso e rastreamento.	Administrador de nuvem, engenheiros de segurança, engenheiros de PKI

Recursos relacionados

- Criar uma hierarquia de CA (documentação da CA privada da AWS)
- Criar uma CA privada (documentação da CA privada da AWS)
- Como usar o AWS RAM para compartilhar sua conta cruzada de CA privada da AWS (publicação no blog da AWS)
- Práticas recomendadas de CA privada da AWS (publicação no blog da AWS)
- Habilitar compartilhamento de recursos com o AWS Organizations (documentação do AWS RAM)
- Gerenciar do ciclo de vida da CA privada (documentação da CA privada da AWS)
- acm-certificate-expiration-check para o AWS Config (documentação do AWS Config)
- O AWS Certificate Manager agora fornece monitoramento de expiração de certificados por meio da Amazon CloudWatch (anúncio da AWS)
- Serviços integrados ao AWS Certificate Manager (ACM) (documentação do ACM)

Mais informações

Ao exportar certificados, use uma frase secreta que seja criptograficamente forte e alinhada à estratégia de prevenção de perda de dados da sua organização.

Desative os controles padrão de segurança em todas as contas de membros do Security Hub em um ambiente com várias contas

Criado por Michael Fuellbier (AWS) e Ahmed Bakry (AWS)

Resumo

> **Important**
>
> AWS Security Hub agora oferece suporte à configuração central para padrões e controles de segurança em todas as contas. Esse novo recurso aborda muitos dos cenários abordados pela solução nesse padrão de orientação AWS prescritiva. Antes de implantar a solução nesse padrão, consulte Configuração central no Security Hub.

Na nuvem Amazon Web Services (AWS), controles AWS Security Hub padrão, como CIS AWS Foundations Benchmark ou AWS Foundational Security Best Practices, só podem ser desativados (desativados) manualmente a partir de um único. Conta da AWS Em um ambiente com várias contas, você não pode desativar os controles em várias contas de membros do Security Hub com "um clique" (ou seja, uma chamada de API). Esse padrão demonstra como usar um clique para desativar os controles padrão do Security Hub em todas as contas de membros do Security Hub gerenciadas pela sua conta de administrador do Security Hub.

Pré-requisitos e limitações

Pré-requisitos

- Um ambiente de várias contas que consiste em uma conta de administrador do Security Hub que gerencia várias contas de membros
- AWS Command Line Interface (AWS CLI) versão 2, instalada
- AWS Serverless Application Model Interface de linha de comando (AWS SAM CLI), instalada

Limitações

- Esse padrão funciona somente em um ambiente de várias contas em que uma única conta de administrador do Security Hub gerencia várias contas de membros.

- O início do evento causa várias invocações paralelas se você alterar muitos controles em um período de tempo muito curto. Isso pode levar ao controle de utilização da API e fazer com que as invocações falhem. Por exemplo, esse cenário pode acontecer se você alterar programaticamente muitos controles usando a CLI do Security Hub Controls.

Arquitetura

O diagrama a seguir mostra um exemplo de um AWS Step Functions fluxo de trabalho que desativa os controles padrão do Security Hub em várias contas de membros do Security Hub (conforme visualizado na conta de administrador do Security Hub).

O diagrama inclui o seguinte fluxo de trabalho:

1. Uma EventBridge regra da Amazon é iniciada diariamente e invoca a máquina de estado. Você pode modificar o tempo da regra atualizando o `Schedule` parâmetro em seu AWS CloudFormation modelo.
2. Uma EventBridge regra é iniciada sempre que um controle é ativado ou desativado na conta de administrador do Security Hub.
3. Uma máquina de estado do Step Functions propaga o status dos controles padrão de segurança (ou seja, controles que estão ativados ou desativados) da conta do administrador do Security Hub para as contas dos membros.
4. Uma função entre contas AWS Identity and Access Management (IAM) é implantada em cada conta membro e assumida pela máquina de estado. A máquina de estado ativa ou desativa os controles na conta de cada membro.
5. Uma tabela do Amazon DynamoDB contém exceções e informações sobre quais controles ativar ou desativar em uma conta específica. Essas informações substituem as configurações obtidas da conta de administrador do Security Hub para a conta de membro especificada.

> **Note**
>
> O objetivo da EventBridge regra agendada é garantir que as contas de membros recém-adicionadas do Security Hub tenham o mesmo status de controle das contas existentes.

Ferramentas

Serviços da AWS

- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que ajuda você a conectar seus aplicativos com dados em tempo real de várias fontes. Por exemplo, AWS Lambda funções, endpoints de invocação HTTP usando destinos de API ou barramentos de eventos em outros. Contas da AWS
- AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que ajuda você a interagir Serviços da AWS por meio de comandos em seu shell de linha de comando.
- O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.
- AWS Serverless Application Model (AWS SAM) é uma estrutura de código aberto que ajuda você a criar aplicativos sem servidor no. Nuvem AWS
- AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS. Também ajuda você a verificar seu AWS ambiente de acordo com os padrões e as melhores práticas do setor de segurança.
- AWS Step Functionsé um serviço de orquestração sem servidor que ajuda você a combinar AWS Lambda funções e outras Serviços da AWS para criar aplicativos essenciais para os negócios.

Repositório de código

O código desse padrão está disponível no repositório GitHub AWS Security Hub Cross-Account Controls Disabler. O repositório de código contém os seguintes arquivos e pastas:

- UpdateMembers/template.yaml — Esse arquivo contém componentes implantados na conta de administrador do Security Hub, incluindo a máquina de estado do Step Functions e as regras. EventBridge
- member-iam-role/template.yaml — Esse arquivo contém o código para implantar a função do IAM entre contas em uma conta membro.
- StateMachine.json — Esse arquivo define o fluxo de trabalho da máquina de estado.

- GetMembers/index.py — Esse arquivo contém o código da máquina de GetMembersestado. Um script recupera o status dos controles padrão de segurança em todas as contas existentes dos membros do Security Hub.
- UpdateMember/index.py — Esse arquivo contém um script que atualiza o status de controle em cada conta de membro.
- CheckResult/index.py — Esse arquivo contém um script que verifica o status da invocação do fluxo de trabalho (aceita ou falhada).

Épicos

Implemente um perfil do IAM entre contas nas contas dos membros do Security Hub

Tarefa	Descrição	Habilidades necessárias
Identifique o ID da conta de administrador do Security Hub.	Configure uma conta de administrador do Security Hub e, em seguida, anote o ID da conta do administrador.	Arquiteto de nuvem
Implante o CloudFormation modelo que inclui a função do IAM entre contas nas contas dos membros.	Para implantar o modelo member-iam-role/template.yaml em todas as contas de membros gerenciadas pela conta de administrador do Security Hub, execute o seguinte comando: `aws cloudformation deploy \ --template-file member-iam-role/template.yaml \ --capabilities CAPABILITY_NAMED_IAM \ --stack-name <your-stack-name> \`	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	`--parameter-overrides SecurityHubAdminAccountId=<account-ID>` O parâmetro `SecurityHubAdminAccountId` deve corresponder ao ID da conta do administrador do Security Hub que você anotou anteriormente.	

Implantar uma máquina de estado na conta de administrador do Security Hub

Tarefa	Descrição	Habilidades necessárias

Package o CloudFormation modelo que inclui a máquina de estado com AWS SAM.	Para empacotar o UpdateMembersmodelo /template.yaml na conta de administrador do Security Hub, execute o seguinte comando:
	
	`sam package \`
	`  --template-file UpdateMembers/template.yaml \`
	`  --output-template-file UpdateMembers/template-out.yaml \`
	`  --s3-bucket <amzn-s3-demo-bucket>`
	
	Note
	Seu bucket do Amazon Simple Storage Service
		AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	(Amazon S3) deve estar no Região da AWS mesmo local em que você implanta o modelo. CloudFormation	

Tarefa	Descrição	Habilidades necessárias
Implante o CloudFormation modelo empacotado na conta de administrador do Security Hub.	Para implantar o CloudFormation modelo na conta de administrador do Security Hub, execute o seguinte comando: `aws cloudformation deploy \ --template-file UpdateMembers/template-out.yaml \ --capabilities CAPABILITY_IAM \ --stack-name <stack-name>` No modelo member-iam-role/template.yaml, o `MemberIAMRolePath` parâmetro deve corresponder ao parâmetro e deve corresponder. `IAMRolePath MemberIAMRoleName IAMRoleName` **Note** Como o Security Hub é um serviço regional, você deve implantar o modelo individualmente em cada um Região da AWS. Certifique-se primeiro de empacotar a solução em um	AWS DevOps

Tarefa	Descrição	Habilidades necessárias
	bucket do Amazon S3 em cada região.	

Recursos relacionados

- Designação de uma conta de administrador do Security Hub (documentação do Security Hub)
- Tratamento de erros, novas tentativas e adição de alertas às execuções de máquinas de AWS Step Functions estado (AWS publicação do blog)

Atualize as credenciais da AWS CLI do AWS IAM Identity Center usando PowerShell

Criado por Chad Miles (AWS) e Andy Bowen (AWS)

Resumo

Se você quiser usar as credenciais do AWS IAM Identity Center (sucessor do AWS Single Sign-On) com a AWS Command Line Interface (AWS CLI), a AWS SDKs ou o AWS Cloud Development Kit (AWS CDK), você normalmente precisa copiar e colar as credenciais do console do IAM Identity Center na interface da linha de comando. Esse processo pode levar um tempo considerável e deve ser repetido para cada conta que requer acesso.

Uma solução comum é usar o comando `aws sso configure` da AWS CLI. Esse comando adiciona um perfil compatível com o IAM Identity Center para a AWS CLI ou AWS SDK. No entanto, a desvantagem dessa solução é que você deve executar o comando `aws sso login` para cada perfil ou conta ds AWS CLI que você configurou dessa forma.

Como uma solução alternativa, esse padrão descreve como usar perfis nomeados da AWS CLI e ferramentas da AWS para PowerShell armazenar e atualizar credenciais para várias contas de uma única instância do IAM Identity Center simultaneamente. O script também armazena os dados da sessão do IAM Identity Center na memória para atualizar as credenciais sem fazer login novamente no IAM Identity Center.

Pré-requisitos e limitações

Pré-requisitos

- PowerShell, instalado e configurado. Para obter mais informações, consulte Instalando PowerShell (documentação da Microsoft).
- AWS Tools para PowerShell, instaladas e configuradas. Por motivos de desempenho, é altamente recomendável que você instale a versão modularizada do AWS Tools for PowerShell, chamada. `AWS.Tools` Cada serviço da AWS é compatível com seu próprio módulo individual pequeno. No PowerShell prompt, insira os seguintes comandos para instalar os módulos necessários para esse padrão: `AWS.Tools.InstallerSSO`,, `SSOIDC` e.

```
Install-Module AWS.Tools.Installer
Install-AWSToolsModule SSO, SSOOIDC
```

Para obter mais informações, consulte Instalar o AWS.Tools no Windows ou Instalar o AWS.Tools no Linux ou no macOS.

- A AWS CLI ou o AWS SDK devem ser previamente configurados com credenciais de trabalho, fazendo o seguinte:
  - Use o comando `aws configure` da AWS CLI. Para obter mais informações, consulte Configuração rápida (documentação da AWS CLI).
  - Configure a AWS CLI ou o AWS CDK para obter acesso temporário por meio de um perfil do IAM. Para obter mais informações, consulte Obter credenciais de perfil do IAM para acesso à CLI (documentação do Centro de Identidade IAM).

Limitações

- Esse script não pode ser usado em um pipeline ou em uma solução totalmente automatizada. Ao implantar esse script, você deve autorizar manualmente o acesso do IAM Identity Center. Em seguida, o script continua automaticamente.

Versões do produto

- Para todos os sistemas operacionais, é recomendável usar a PowerShell versão 7.0 ou posterior.

Arquitetura

Você pode usar o script nesse padrão para atualizar simultaneamente várias credenciais do IAM Identity Center e criar um arquivo de credencial para uso com a AWS CLI, a AWS ou o AWS CDK. SDKs

Ferramentas

Serviços da AWS

- A AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite que você interaja com serviços da AWS usando comandos no shell da linha de comando.
- O Centro de Identidade do AWS IAM ajuda você a gerenciar centralmente o acesso à autenticação única (SSO) a todas as suas contas e aplicativos na nuvem da AWS.

- As ferramentas da AWS para PowerShell são um conjunto de PowerShell módulos que ajudam você a criar scripts de operações em seus recursos da AWS a partir da linha de PowerShell comando.

Outras ferramentas

- PowerShellé um programa de gerenciamento de automação e configuração da Microsoft executado em Windows, Linux e macOS.

Práticas recomendadas

Mantenha uma cópia desse script para cada instância do IAM Identity Center. Não há suporte para o uso de um script para várias instâncias.

Épicos

Executar o script de SSO

Tarefa	Descrição	Habilidades necessárias
Personalize o script de SSO.	1. Copie o script de SSO na seção Informações adicionais. 2. Na seção `Param`, no seu ambiente da AWS, defina os valores para as seguintes variáveis: • `DefaultRoleName` : o perfil do IAM ou o conjunto de permissões a ser usado por padrão. • `Region`: a região da AWS na qual o Centro de Identidade IAM está implantado. Para obter uma lista completa de	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	regiões e seus códigos, consulte Endpoints regionais. • `StartUrl`: o URL usado para acessar sua página de login do IAM Identity Center. Use o mesmo formato do valor de exemplo no script. • `EnvironmentName` : um nome curto para fazer referência a essa cópia do script, a ser usado quando você estiver executando várias cópias de script na mesma sessão. 3. Na linha 10, que diz # `Add your Account Information` , edite os seguintes valores nas tabelas de hash para refletir seu ambiente: • `Profile`: o nome do perfil da AWS CLI no qual armazenar as credenciais temporárias. • `AccountId` : o ID da conta da AWS para a qual você está recuperan do as credenciais. • `RoleName`: o nome da função ou do conjunto	

Tarefa	Descrição	Habilidades necessárias
	de permissões do IAM Identity Center que você deseja usar. Você pode deixar isso como `$DefaultRoleName` se quiser usar a mesma função que definiu na seção `Param`. Cada linha na tabela de hash deve terminar com uma vírgula, exceto a última.	

Executar o script de SSO.	É recomendável que você execute seu script personalizado no PowerShell shell com o comando a seguir.
	
	`./Set-AwsCliSsoCredentials.ps1`
	
	Como alternativa, você pode executar o script de outro shell digitando o comando a seguir.
	
	`pwsh Set-AwsCliSsoCredentials.ps1`
		Administrador de nuvem

Solução de problemas

Problema	Solução
Erro `No Access`	O perfil do IAM que você está usando não tem permissões para acessar a função ou

Problema	Solução
	o conjunto de permissões que você definiu em um parâmetro `RoleName`. Atualize as permissões da função que você está usando ou defina uma função ou conjunto de permissões diferente no script.

Recursos relacionados

- Onde as definições de configuração ficam armazenadas? (Documentação da AWS CLI)
- Configurar a AWS CLI para usar o Centro de Identidade do AWS IAM (documentação da AWS CLI)
- Usar perfis nomeados (documentação da AWS CLI)

Mais informações

Script de SSO

No script a seguir, substitua os espaços reservados entre colchetes angulares (**<>**) por suas próprias informações e remova os colchetes angulares.

```
Set-AwsCliSsoCredentials.ps1
Param(
    $DefaultRoleName = '<AWSAdministratorAccess>',
    $Region          = '<us-west-2>',
    $StartUrl        = "<https://d-12345abcde.awsapps.com/start/>",
    $EnvironmentName = "<CompanyName>"
)
Try {$SsoAwsAccounts = (Get-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Scope
 Global -ErrorAction 'SilentlyContinue').Value.Clone()}
Catch {$SsoAwsAccounts = $False}
if (-not $SsoAwsAccounts) { $SsoAwsAccounts = @(
# Add your account information in the list of hash tables below, expand as necessary,
 and do not forget the commas
    @{Profile = "<Account1>"      ; AccountId = "<012345678901 >"; RoleName =
 $DefaultRoleName },
    @{Profile = "<Account2>"      ; AccountId = "<123456789012>"; RoleName =
 "<AWSReadOnlyAccess>" }
```

```
)}
$ErrorActionPreference = "Stop"
if (-not (Test-Path ~\.aws))      { New-Item ~\.aws -type Directory }
if (-not (Test-Path ~\.aws\credentials)) { New-Item ~\.aws\credentials -type File }
$CredentialFile = Resolve-Path ~\.aws\credentials
$PsuedoCreds    = @{AccessKey =
 'AKAEXAMPLE123ACCESS';SecretKey='PsuedoS3cret4cceSSKey123PsuedoS3cretKey'} # Pseudo
 Creds, do not edit.
Try {$SSOTokenExpire = (Get-Variable -Scope Global -Name
 "$($EnvironmentName)SSOTokenExpire" -ErrorAction 'SilentlyContinue').Value} Catch
 {$SSOTokenExpire = $False}
Try {$SSOToken       = (Get-Variable -Scope Global -Name "$($EnvironmentName)SSOToken"
 -ErrorAction 'SilentlyContinue').Value }      Catch {$SSOToken       = $False}
if ( $SSOTokenExpire -lt (Get-Date) ) {
    $SSOToken = $Null
    $Client   = Register-SSOOIDCClient -ClientName cli-sso-client -ClientType public -
Region $Region @PsuedoCreds
    $Device   = $Client | Start-SSOOIDCDeviceAuthorization -StartUrl $StartUrl -Region
 $Region @PsuedoCreds
    Write-Host "A Browser window should open. Please login there and click ALLOW." -
NoNewline
    Start-Process $Device.VerificationUriComplete
    While (-Not $SSOToken){
        Try {$SSOToken = $Client | New-SSOOIDCToken -DeviceCode $Device.DeviceCode -
GrantType "urn:ietf:params:oauth:grant-type:device_code" -Region $Region @PsuedoCreds}
        Catch {If ($_.Exception.Message -notlike "*AuthorizationPendingException*")
{Write-Error $_.Exception} ; Start-Sleep 1}
    }
    $SSOTokenExpire = (Get-Date).AddSeconds($SSOToken.ExpiresIn)
    Set-Variable -Name "$($EnvironmentName)SSOToken" -Value $SSOToken -Scope Global
    Set-Variable -Name "$($EnvironmentName)SSOTokenExpire" -Value $SSOTokenExpire -
Scope Global
}
$CredsTime     = $SSOTokenExpire - (Get-Date)
$CredsTimeText = ('{0:D2}:{1:D2}:{2:D2} left on SSO Token' -f $CredsTime.Hours,
 $CredsTime.Minutes, $CredsTime.Seconds).TrimStart("0 :")
for ($i = 0; $i -lt $SsoAwsAccounts.Count; $i++) {
    if (([DateTimeOffset]::FromUnixTimeSeconds($SsoAwsAccounts[$i].CredsExpiration /
 1000)).DateTime -lt (Get-Date).ToUniversalTime()) {
        Write-host "`r
    `rRegistering Profile $($SsoAwsAccounts[$i].Profile)" -NoNewline
        $TempCreds = $SSOToken | Get-SSORoleCredential -AccountId
 $SsoAwsAccounts[$i].AccountId -RoleName $SsoAwsAccounts[$i].RoleName -Region $Region
 @PsuedoCreds
```

```
        [PSCustomObject]@{AccessKey = $TempCreds.AccessKeyId; SecretKey =
 $TempCreds.SecretAccessKey; SessionToken = $TempCreds.SessionToken
        } | Set-AWSCredential -StoreAs $SsoAwsAccounts[$i].Profile -ProfileLocation
 $CredentialFile
        $SsoAwsAccounts[$i].CredsExpiration = $TempCreds.Expiration
    }
}
Set-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Value $SsoAwsAccounts.Clone() -
Scope Global
Write-Host "`r$($SsoAwsAccounts.Profile) Profiles registered, $CredsTimeText"
```

Use o AWS Config para monitorar as configurações de segurança do Amazon Redshift

Criado por Lucas Kauffman (AWS) e Abhishek Sengar (AWS)

Resumo

Usando o AWS Config, você pode avaliar as configurações de segurança dos seus recursos da AWS. O AWS Config pode monitorar os recursos e, se as configurações violarem suas regras definidas, o AWS Config sinaliza o recurso como não compatível.

É possível usar o AWS Config para avaliar e monitorar seus clusters e bancos de dados do Amazon Redshift. Para obter mais informações sobre recomendações e atributos de segurança, consulte Segurança no Amazon Redshift. Esse padrão inclui regras personalizadas do AWS Lambda para o AWS Config. Você pode implantar essas regras em sua conta para monitorar as configurações de segurança dos seus clusters e bancos de dados do Amazon Redshift. As regras desse padrão ajudam você a usar o AWS Config para confirmar que:

- O log de auditoria está habilitado para os bancos de dados no cluster do Amazon Redshift
- O SSL é necessário para se conectar ao cluster do Amazon Redshift
- As cifras do Federal Information Processing Standards (FIPS) estão em uso
- Os bancos de dados no cluster Amazon Redshift são criptografados
- O monitoramento da atividade do usuário está ativado

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- O AWS Config deve estar habilitado em sua conta da AWS. Para obter mais informações, consulte Configurar o AWS Config com o console ou Configurar o AWS Config com a AWS CLI.
- A versão 3.9 ou superior do Python deve ser usada para o manipulador do AWS Lambda. Para obter mais informações, consulte Trabalhar com o Python (Documentação do AWS Lambda).

Versões do produto

- Python, versão 3.9 ou superior

Arquitetura

Pilha de tecnologias de destino

- AWS Config

Arquitetura de destino

1. O AWS Config executa periodicamente a regra personalizada.
2. A regra personalizada invoca a função do Lambda.
3. A função do Lambda verifica se há configurações não compatíveis nos clusters do Amazon Redshift.
4. A função do Lambda relata o estado de conformidade de cada cluster do Amazon Redshift para o AWS Config.

Automação e escala

As regras personalizadas do AWS Config escalam para avaliar todos os clusters do Amazon Redshift em sua conta. Nenhuma ação adicional é necessária para escalar essa solução.

Ferramentas

Serviços da AWS

- O AWS Config oferece uma visualização de detalhes dos recursos na sua conta da AWS e como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Lambda é um serviço de computação que ajuda você a executar código sem exigir provisionamento ou gerenciamento de servidores. Ele executa o código somente quando necessário e dimensiona automaticamente, assim, você paga apenas pelo tempo de computação usado.

- O Amazon Redshift é um serviço de data warehouse em escala de petabytes gerenciado na Nuvem AWS.

Repositório de código

O código desse padrão está disponível no GitHub aws-config-rulesrepositório. As regras personalizadas nesse repositório são regras Lambda na linguagem de programação Python. Esse repositório contém muitas regras personalizadas para o AWS Config. Somente as seguintes regras são usadas nesse padrão:

- `REDSHIFT_AUDIT_ENABLED`: confirme se o log de auditoria está habilitado no cluster do Amazon Redshift. Se você também quiser confirmar se o monitoramento de atividades do usuário está ativado, implante a regra `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`, em vez disso.
- `REDSHIFT_SSL_REQUIRED`: confirme se o SSL é necessário para se conectar ao cluster do Amazon Redshift. Se você também quiser confirmar se as cifras do Federal Information Processing Standards (FIPS) estão em uso, implante a regra `REDSHIFT_FIPS_REQUIRED`, em vez disso.
- `REDSHIFT_FIPS_REQUIRED`: confirme se o SSL é necessário e se as cifras FIPS estão em uso.
- `REDSHIFT_DB_ENCRYPTED`: confirme se os bancos de dados no cluster do Amazon Redshift estão criptografados.
- `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`: confirme se o log de auditoria e o monitoramento de atividades do usuário estão ativados.

Épicos

Prepare-se para implantar as regras

Tarefa	Descrição	Habilidades necessárias
Configurar políticas do IAM.	1. Crie uma política personalizada baseada em identidade do IAM que permita que a função de execução do Lambda leia as configurações de cluster do Amazon Redshift. Para obter mais informações, consulte	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	Gerenciamento do acesso aos recursos (Document ação do Amazon Redshift) e Criação de políticas do IAM (Documentação do IAM). `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["redshift:DescribeClusterParameterGroups", "redshift:DescribeClusterParameters", "redshift:DescribeClusters", "redshift:DescribeClusterSecurityGroups", "redshift:DescribeClusterSnapshots", "redshift:DescribeClusterSubnetGroups", "redshift:DescribeEventSubscriptions", "redshift:DescribeLoggingStatus"],`	

Tarefa	Descrição	Habilidades necessárias
	<pre>"Resource": "*" }] }</pre> 2. Atribua as políticas AWSLambdaExecute e AWSConfigRulesExecutionRolegerenciadas como uma política de permissões para a função de execução do Lambda. Para obter instruções, consulte Adicionar permissões de identidade do IAM (Documentação do IAM).	
Clonar o repositório.	Em um shell bash, execute o comando a seguir. Isso clona o aws-config-rulesrepositório de. GitHub <pre>git clone https://github.com/awslabs/aws-config-rules.git</pre>	AWS geral

Implante as regras no AWS Config

Tarefa	Descrição	Habilidades necessárias
Implante as regras no AWS Config.	Seguindo as instruções em Criação de regras personalizadas do Lambda (Documentação do AWS Config), implante uma ou mais das	Administrador da AWS

Tarefa	Descrição	Habilidades necessárias
	seguintes regras em sua conta: • `REDSHIFT_AUDIT_ENABLED` • `REDSHIFT_SSL_REQUIRED` • `REDSHIFT_FIPS_REQUIRED` • `REDSHIFT_DB_ENCRYPTED` • `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`	
Verifique se as regras estão funcionando.	Depois de implantar as regras, siga as instruções em Avaliação de seus recursos (Documentação do AWS Config) para confirmar se o AWS Config está avaliando corretamente seus recursos do Amazon Redshift.	AWS geral

Recursos relacionados

Documentação do serviço AWS

- Segurança no Amazon Redshift (Documentação do Amazon Redshift)
- Gerenciando a segurança do banco de dados (Documentação do Amazon Redshift)
- Regras personalizadas do AWS Config (Documentação do AWS Config)

Recomendações da AWS

- Verificar se os novos clusters do Amazon Redshift têm os endpoints SSL necessários
- Garanta que um cluster do Amazon Redshift seja criptografado na criação

Mais informações

Você pode usar as seguintes regras gerenciadas da AWS no AWS Config para confirmar as seguintes configurações de segurança para o Amazon Redshift:

- redshift-cluster-configuration-check— Use essa regra para confirmar se o registro de auditoria está habilitado para os bancos de dados no cluster do Amazon Redshift e confirmar se os bancos de dados estão criptografados.
- redshift-require-tls-ssl— Use essa regra para confirmar que o SSL é necessário para se conectar ao cluster do Amazon Redshift.

Use o Network Firewall para capturar os nomes de domínio DNS da Indicação de Nome do Servidor para tráfego de saída

Criado por Kirankumar Chandrashekar (AWS)

Resumo

Esse padrão mostra como usar o Firewall de Rede da AWS para coletar os nomes de domínio DNS fornecidos pela Indicação de Nome do Servidor (SNI) no cabeçalho HTTPS do seu tráfego de rede de saída. O Network Firewall é um serviço gerenciado que facilita a implantação de proteções de rede críticas para a Amazon Virtual Private Cloud (Amazon VPC), incluindo a capacidade de proteger o tráfego de saída com um firewall que bloqueia pacotes que não atendem a determinados requisitos de segurança. Proteger o tráfego de saída para nomes de domínio DNS específicos é chamado de filtragem de saída, que é a prática de monitorar e potencialmente restringir o fluxo de informações de saída de uma rede para outra.

Depois de capturar os dados do SNI que passam pelo Network Firewall, você pode usar o Amazon CloudWatch Logs e o AWS Lambda para publicar os dados em um tópico do Amazon Simple Notification Service (Amazon SNS) que gera notificações por e-mail. As notificações por e-mail incluem o nome do servidor e outras informações relevantes da SNI. Além disso, você pode usar a saída desse padrão para permitir ou restringir o tráfego de saída por nome de domínio na SNI usando regras de firewall. Para obter mais informações, consulte Trabalhar com grupos de regras com estado no AWS Network Firewall na documentação do Network Firewall.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- AWS Command Line Interface (AWS CLI) versão 2, instalada e configurada em Linux, macOS ou Windows.
- Firewall de rede, instalado e configurado na Amazon VPC e em uso para inspecionar o tráfego de saída. Você pode configurar o Network Firewall para usar qualquer uma das seguintes configurações de VPC:
  - Arquitetura simples de zona única com um gateway da Internet
  - Arquitetura de várias zonas com um gateway da Internet

- Arquitetura com um gateway da Internet e um gateway NAT

Arquitetura

O diagrama a seguir mostra como usar o Firewall de Rede para coletar dados SNI do tráfego de rede de saída e, em seguida, publicar esses dados em um tópico do SNS usando Logs CloudWatch e Lambda.

O diagrama mostra o seguinte fluxo de trabalho:

1. O Network Firewall coleta nomes de domínio dos dados da SNI no cabeçalho HTTPS do tráfego de saída da rede.
2. CloudWatch O Logs monitora os dados do SNI e invoca uma função Lambda sempre que o tráfego de saída da rede passa pelo Network Firewall.
3. A função Lambda lê os dados SNI capturados pelo CloudWatch Logs e depois publica esses dados em um tópico do SNS.
4. O tópico SNS envia uma notificação por e-mail que inclui os dados da SNI.

Automação e escala

- Você pode usar CloudFormation a AWS para criar esse padrão usando a infraestrutura como código.

Pilha de tecnologia

- CloudWatch Registros da Amazon
- Amazon SNS
- Amazon VPC
- AWS Lambda
- AWS Network Firewall

Ferramentas

Serviços da AWS

- Amazon CloudWatch Logs — Você pode usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar seus arquivos de log a partir de instâncias do Amazon Elastic Compute Cloud (Amazon EC2), AWS CloudTrail, Amazon Route 53 e outras fontes.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) é um serviço gerenciado que fornece entrega de mensagens de publicadores para assinantes (também conhecido como produtores e consumidores).
- Amazon VPC: a Amazon Virtual Private Cloud (Amazon VPC) provisiona uma seção logicamente isolada da Nuvem AWS, em que é possível executar recursos da AWS em uma rede virtual que você definiu. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu datacenter, com os benefícios de usar a infraestrutura dimensionável da AWS.
- AWS Lambda: o AWS Lambda é um serviço de computação com tecnologia que pode ser usado para executar código sem provisionamento ou gerenciamento de servidores.
- Firewall de Rede da AWS — O Firewall de Rede da AWS é um serviço gerenciado que facilita a implantação de proteções de rede essenciais para toda a Amazon VPCs.

Épicos

Crie um grupo de CloudWatch registros para o Network Firewall

Tarefa	Descrição	Habilidades necessárias
Crie um grupo de CloudWatch registros.	1. Faça login no Console de Gerenciamento da AWS e abra o console do CloudWatch . 2. No painel de navegação, escolha Grupos de logs. 3. Selecione Actions (Ações) e selecione Create log group (Criar grupo de logs). 4. Digite um nome para o grupo de logs e escolha Create log group (Criar grupo de logs).	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	Para obter mais informações, consulte Trabalhando com grupos e fluxos de registros na CloudWatch documentação.	

Crie um tópico do SNS e inscrição

Tarefa	Descrição	Habilidades necessárias
Criar um tópico do SNS.	Para criar um tópico do SNS, siga as instruções na documentação do Amazon SNS.	Administrador de nuvem
Inscreva um endpoint em um tópico do SNS.	Para inscrever um endereço de e-mail como endpoint para o tópico do SNS que você criou, siga as instruções na documentação do Amazon SNS. Em Protocolo, escolha E-mail/e-mail-JSON. **Note** Você também pode escolher um endpoint diferente com base em seus requisitos.	Administrador de nuvem

Configurar o login no Network Firewall

Tarefa	Descrição	Habilidades necessárias
Habilitar o registro em log de firewall.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. 2. No painel de navegação, em NETWORK FIREWALL, escolha Firewalls. 3. Na seção Firewalls, escolha o firewall em que você deseja capturar o nome do servidor do SNI para tráfego de saída. 4. Escolha a guia Detalhes do firewall e, em seguida, escolha Editar na seção Registro em log. 5. Em Tipo de registro, selecione Alerta. Em Destino do registro para alertas, selecione o grupo de CloudWatch registros. 6. Em grupo de CloudWatch registros, pesquise e escolha o grupo de registros que você criou anteriormente e, em seguida, escolha Salvar. Para obter mais informações sobre o uso de CloudWatch Logs como destino de log para	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	o Network Firewall, consulte Amazon CloudWatch Logs na documentação do Network Firewall.	

Configurar uma regra de estado no Network Firewall

Tarefa	Descrição	Habilidades necessárias
Crie uma regra com estado.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. 2. No painel de navegação, em NETWORK FIREWALL, escolha Grupos de regras do Network Firewall. 3. Escolha Criar grupo de regras do Network Firewall. 4. Na página Criar grupo de regras do Network Firewall, para o Tipo de grupo de regra, escolha Grupo de regras com estado. Observação: para obter mais informações, consulte Trabalhar com grupos de regras com estado no AWS Network Firewall. 5. Na seção Grupos de regras com estado, insira um nome e uma descrição	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	para o grupo de regras com estado. 6. Em Capacidade, defina a capacidade máxima que você deseja permitir para o grupo de regras com estado (até o máximo de 30.000). Observação: Não será possível alterar essa configuração após a criação do grupo de regras. Para obter informações sobre como calcular a capacidade, consulte Como definir a capacidade do grupo de regras no AWS Network Firewall. Para obter informações sobre a configuração máxima, consulte as cotas do AWS Network Firewall. 7. Em Opções de grupos de regras com estado, selecione 5 tuplas. 8. Na seção Ordem das regras com estado, escolha Padrão. 9. Na seção Variáveis da regra, mantenha os valores padrão. 10. Na seção Adicionar regra, escolha TLS para Protocolo. Em Fonte, escolha Qualquer. Em Porta de	

Tarefa	Descrição	Habilidades necessárias
	origem, escolha Qualquer porta. Em Destino, escolha Qualquer. Em Porta de destino, escolha Qualquer porta. Em Direção do tráfego, escolha Forward. Em Ação, escolha Alertar. Escolha Adicionar regra. 11. Escolha Criar grupo de regras com estado.	

Tarefa	Descrição	Habilidades necessárias
Associe a regra de estado ao Network Firewall.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon VPC. 2. No painel de navegação, em NETWORK FIREWALL, escolha Firewalls. 3. Escolha o firewall em que você deseja capturar o nome do servidor do SNI para tráfego de saída. 4. Na seção Grupos de regras com estado, escolha Ações e, em seguida, escolha Adicionar grupos de regras com estado não gerenciados. 5. Na página Adicionar grupos de regras com estado não gerenciado, selecione o grupo de regras com estado que você criou anteriormente e escolha Adicionar grupo de regras com estado.	Administrador de nuvem

Criar uma função do Lambda para ler os logs

Tarefa	Descrição	Habilidades necessárias
Crie o código da função do Lambda.	Em um ambiente de desenvolvimento integrado (IDE) que pode ler o evento	Desenvolvedor de aplicativos

Tarefa	Descrição	Habilidades necessárias

	CloudWatch Logs do Network Firewall para tráfego de saída, cole o seguinte código do Python 3 e <SNS-topic-ARN> substitua pelo seu valor:
	
	`import json`
	`import gzip`
	`import base64`
	`import boto3`
	`sns_client = boto3.client('sns')`
	`def lambda_handler(event, context):`
	`  decoded_event = json.loads(gzip.decompress(base64.b64decode(event['awslogs']['data'])))`
	`  body = '''`
	`  {filtermatch}`
	`  '''.format(`
	`  loggroup=decoded_event['logGroup'],`
	`  logstream=decoded_event['logStream'],`
	`  filtermatch=decoded_event['logEvents'][0]['message'],`
	`  )`
	`  print(body)`
	`  filterMatch = json.loads(body)`
	`  data = []`
	`  if 'http' in filterMatch['event']:`
	`  data.append(filterMatch['ev`	

Tarefa	Descrição	Habilidades necessárias
	ent']['http']['hos tname']) elif 'tls' in filterMatch['event']: data.appe nd(filterMatch['ev ent']['tls']['sni']) result = 'Domain accessed ' + 1*' ' + (data[0]) + 1*' ' 'via AWS Network Firewall ' + 1*' ' + (filterMa tch['firewall_name']) print(result) message = {'ServerN ame': result} send_to_sns = sns_client.publish(TargetArn=<SNS-topic-ARN>, #Replace with the SNS topic ARN Message=j son.dumps({'default': json.dumps(message), 'sms': json.dump s(message), 'email': json.dump s(message)}), Subject='Server Name passed through the Network Firewall', MessageSt ructure='json') Esse exemplo de código analisa o conteúdo dos CloudWatch registros e	

Tarefa	Descrição	Habilidades necessárias
	captura o nome do servidor fornecido pelo SNI no cabeçalho HTTPS.	
Criar a função do Lambda.	Para criar a função do Lambda, siga as instruções na documentação do Lambda e escolha Python 3.9 para Runtime.	Administrador de nuvem
Adicionar o código à função do Lambda.	Para adicionar seu código Python à função do Lambda que você criou anteriorm ente, siga as instruções na documentação do Lambda.	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
Adicione CloudWatch registros como um gatilho à função Lambda.	1. Faça login no Console de Gerenciamento da AWS e abra o console do Lambda. 2. No painel de navegação, escolha Funções e escolha a função que você criou anteriormente. 3. Na seção Visão geral da função, selecione Adicionar gatilho. 4. Na página Adicionar gatilho, na seção Configuração do acionador, escolha CloudWatch Registros e, em seguida, escolha Adicionar. 5. Em Grupo de registros, escolha o grupo de CloudWatch registros que você criou anteriormente. 6. Em Nome do filtro, insira um nome para o seu filtro. 7. Escolha Adicionar. 8. Na guia Configuração da página da sua função, na seção Gatilhos, selecione o gatilho que você acabou de adicionar e escolha Ativar. Para obter mais informações, consulte Como usar o Lambda	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias
	com CloudWatch registros na documentação do Lambda.	

Tarefa	Descrição	Habilidades necessárias
Adicione permissões de publicação do SNS.	Adicione a permissão sns:Publish à função de execução do Lambda, para que o Lambda possa fazer chamadas de API para publicar mensagens no SNS. 1. Encontre a função de execução da função do Lambda criada anteriormente. 2. Adicione a seguinte política ao seu perfil do IAM (Identity and Access Management) da AWS: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "AllowSNSPublish", "Effect": "Allow", "Action": [ "sns:GetTopicAttributes", "sns:Subscribe", "sns:Unsubscribe", "sns:Publish" ],`	Administrador de nuvem

Tarefa	Descrição	Habilidades necessárias

	<pre>"Resource": "*"
	}
	]
	}</pre>	

Teste a funcionalidade da sua notificação do SNS

Tarefa	Descrição	Habilidades necessárias

Envie tráfego por meio do Network Firewall.	1. Envie ou aguarde até que o tráfego HTTPS passe pelo Network Firewall.
	2. Verifique o e-mail de notificação do SNS que você recebe da AWS quando o tráfego passa pelo Network Firewall. O e-mail inclui os detalhes do SNI para o tráfego de saída. Por exemplo, o e-mail gerado a partir do código Lambda acima terá o seguinte conteúdo se o nome de domínio acessado for https://aws.amazon.come o protocolo de assinatura for EMAIL-JSON:
	<pre>{
	"Type": "Notification",</pre>
		Engenheiro de testes

Tarefa	Descrição	Habilidades necessárias
	"MessageId": "<messageID>", "TopicArn": "arn:aws:sns:us-west-2:123456789:testSNSTopic", "Subject": "Server Name passed through the Network Firewall", "Message": "{\"ServerName\": \"Domain 'aws.amazon.com' accessed via AWS Network Firewall 'AWS-Network-Firewall-Multi-AZ-firewall\"}", "Timestamp": "2022-03-22T04:10:04.217Z", "SignatureVersion": "1", "Signature": "<Signature>", "SigningCertURL": "<SigningCertUrl>", "UnsubscribeURL": "<UnsubscribeURL>" } Em seguida, verifique o registro de alertas do Firewall de Rede na Amazon CloudWatch seguindo as instruções na CloudWatch documentação da Amazon. O log de alerta mostra a seguinte saída: {	

Tarefa	Descrição	Habilidades necessárias
	"firewall_name": "AWS-Network-Firewall-Multi-AZ-firewall", "availability_zone": "us-east-2b", "event_timestamp": "<event timestamp>", "event": { "timestamp": "2021-03-22T04:10:04.214222+0000", "flow_id": <flow ID>, "event_type": "alert", "src_ip": "10.1.3.76", "src_port": 22761, "dest_ip": "99.86.59.73", "dest_port": 443, "proto": "TCP", "alert": { "action": "allowed", "signature_id": 2, "rev": 0, "signature": "", "category": "", "severity": 3 }, "tls": { "subject": "CN=aws.amazon.com",	

Tarefa	Descrição	Habilidades necessárias
	"issuerdn ": "C=US, O=Amazon, OU=Server CA 1B, CN=Amazon", "serial": "<serial number>", "fingerpr int": "<fingerprint ID>", "sni": "aws.amazon.com", "version": "TLS 1.2", "notbefor e": "2020-09-30T00:00: 00", "notafter ": "2021-09-23T12:00: 00", "ja3": {}, "ja3s": {} }, "app_proto": "tls" } }	

Use o Terraform para habilitar automaticamente a Amazon GuardDuty para uma organização

Criado por Aarthi Kannan (AWS)

Resumo

A Amazon monitora GuardDuty continuamente suas contas da Amazon Web Services (AWS) e usa inteligência de ameaças para identificar atividades inesperadas e potencialmente maliciosas em seu ambiente da AWS. GuardDuty Habilitar manualmente várias contas ou organizações, em várias regiões da AWS ou por meio do AWS Management Console pode ser complicado. Você pode automatizar o processo usando uma ferramenta de infraestrutura como código (IaC), como o Terraform, que pode provisionar e gerenciar serviços e recursos de várias contas e várias regiões na nuvem.

A AWS recomenda usar o AWS Organizations para configurar e gerenciar várias contas em GuardDuty. Este padrão segue essa recomendação. Um benefício dessa abordagem é que, quando novas contas são criadas ou adicionadas à organização, elas são ativadas GuardDuty automaticamente nessas contas para todas as regiões suportadas, sem a necessidade de intervenção manual.

Esse padrão demonstra como usar o HashiCorp Terraform para habilitar a Amazon GuardDuty para três ou mais contas da Amazon Web Services (AWS) em uma organização. O código de amostra fornecido com esse padrão faz o seguinte:

- GuardDuty Habilita todas as contas da AWS que são membros atuais da organização-alvo no AWS Organizations
- Ativa o recurso de ativação automática em GuardDuty, que ativa automaticamente todas GuardDuty as contas que serão adicionadas à organização de destino no futuro
- Permite selecionar as regiões onde você deseja habilitar GuardDuty
- Usa a conta de segurança da organização como administrador GuardDuty delegado
- Cria um bucket do Amazon Simple Storage Service (Amazon S3) na conta de registro e GuardDuty configura para publicar as descobertas agregadas de todas as contas nesse bucket
- Atribui uma política de ciclo de vida que faz a transição das descobertas do bucket S3 para o Amazon S3 Glacier Flexible Retrieval Glacier após 365 dias, por padrão

É possível executar manualmente esse código de amostra ou integrá-lo ao pipeline de integração contínua e implantação contínua (CI/CD).

Público-alvo

Esse padrão é recomendado para usuários com experiência com Terraform, Python e AWS GuardDuty Organizations.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma organização está configurada no AWS Organizations e contém pelo menos as três contas a seguir:
  - Uma conta de gerenciamento: essa é a conta a partir da qual você implanta o código do Terraform, seja de forma independente ou como parte do pipeline de CI/CD. O estado do Terraform também é armazenado nessa conta.
  - Uma conta de segurança — Essa conta é usada como administrador GuardDuty delegado. Para obter mais informações, consulte Considerações importantes para administradores GuardDuty delegados (GuardDuty documentação).
  - Uma conta de registro — Essa conta contém o bucket do S3, onde GuardDuty publica as descobertas agregadas de todas as contas membros.

  Para obter mais informações sobre como configurar a organização com a configuração necessária, consulte Criar uma estrutura de conta (AWS Well-Architected Labs).
- Um bucket do Amazon S3 e uma tabela do Amazon DynamoDB que servem como backend remoto para armazenar o estado do Terraform na conta de gerenciamento. Para obter mais informações sobre o uso de backends remotos para o estado do Terraform, consulte Backends do S3 (documentação do Terraform). Para obter uma amostra de código que configura o gerenciamento remoto do estado com um back-end S3, consulte remote-state-s3-back-end (Terraform Registry). Observe os seguintes requisitos:
  - As tabelas do DynamoDB e do bucket do S3 devem estar na mesma região.
  - Ao criar a tabela do DynamoDB, a chave de partição deve ser `LockID` (com distinção entre maiúsculas e minúsculas) e o tipo de chave de partição deve ser String. Todas as outras configurações devem estar em seus valores predefinidos. Para obter mais informações, consulte Sobre chaves primárias e Criar uma tabela (documentação do DynamoDB).

- Um bucket do S3 que será usado para armazenar registros de acesso do bucket do S3 no qual GuardDuty publicará as descobertas. Para obter mais informações, consulte Habilitar o registro em log de acesso ao servidor Amazon S3 (documentação do Amazon S3). Se você estiver implantando em uma zona de pouso do AWS Control Tower, poderá reutilizar o bucket do S3 na conta de arquivamento de log para essa finalidade.
- A versão 0.14.6 ou superior do Terraform está instalada e configurada. Para obter mais informações, consulte Conceitos básicos – AWS (documentação do Terraform).
- A versão 3.9.6 ou superior está instalada e configurada. Para obter mais informações, consulte Versões de origem (site da Python).
- O AWS SDK para Python (Boto3) está instalado. Para obter mais informações, consulte Instalação (documentação do Boto3).
- O jq está instalado e configurado. Para obter mais informações, consulte Baixar o jq (documentação do jq).

Limitações

- Esse padrão é compatível com os sistemas operacionais macOS e Amazon Linux 2. Esse padrão não foi testado para uso em sistemas operacionais Windows.

> **Note**
>
> O Amazon Linux 2 está chegando ao fim do suporte. Para obter mais informações, consulte o Amazon Linux 2 FAQs.

- GuardDuty ainda não deve estar habilitado em nenhuma das contas, em nenhuma das regiões de destino.
- A solução IaC nesse padrão não implanta os pré-requisitos.
- Esse padrão foi projetado para uma Zona de Pouso da AWS que segue as seguintes práticas recomendadas:
  - A zona de pouso foi criada usando o AWS Control Tower.
  - Contas separadas da AWS são usadas para segurança e registro em log.

Versões do produto

- Versão 0.14.6 ou superior do Terraform. O código de amostra foi testado para a versão 1.2.8.

- Python, versão 3.9.6 ou superior.

Arquitetura

Esta seção fornece uma visão geral de alto nível dessa solução e da arquitetura estabelecida pelo código de amostra. O diagrama a seguir mostra os recursos implantados nas várias contas da organização, dentro de uma única região da AWS.

1. O Terraform cria a função GuardDutyTerraformOrgRoleAWS Identity and Access Management (IAM) na conta de segurança e na conta de registro.
2. O Terraform cria um bucket do S3 na região padrão da AWS na conta de registro em log. Esse bucket é usado como destino de publicação para agregar todas as GuardDuty descobertas em todas as regiões e de todas as contas da organização. O Terraform também cria uma chave do AWS Key Management Service (AWS KMS) na conta de segurança que é usada para criptografar as descobertas no bucket do S3 e configura o arquivamento automático das descobertas do bucket do S3 no armazenamento S3 Glacier Flexible Retrieval.
3. Na conta de gerenciamento, o Terraform designa a conta de segurança como administradora delegada da. GuardDuty Isso significa que a conta de segurança agora gerencia o GuardDuty serviço para todas as contas dos membros, incluindo a conta de gerenciamento. As contas de membros individuais não podem ser suspensas ou GuardDuty desativadas sozinhas.
4. O Terraform cria o GuardDuty detector na conta de segurança, para o administrador GuardDuty delegado.
5. Se ainda não estiver habilitado, o Terraform habilita a proteção S3. GuardDuty Para obter mais informações, consulte Proteção do Amazon S3 na Amazon GuardDuty (GuardDuty documentação).
6. O Terraform inscreve todas as contas de membros atuais e ativas na organização como GuardDuty membros.
7. O Terraform configura o administrador GuardDuty delegado para publicar as descobertas agregadas de todas as contas membros no bucket do S3 na conta de registro.
8. O Terraform repete as etapas 3 a 7 para cada região da AWS que você escolher.

Automação e escala

O código de amostra fornecido é modularizado para que você possa integrá-lo ao seu pipeline de CI/CD para implantação automatizada.

Ferramentas

Serviços da AWS

- O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável.
- GuardDutyA Amazon é um serviço contínuo de monitoramento de segurança que analisa e processa registros para identificar atividades inesperadas e potencialmente não autorizadas em seu ambiente da AWS.
- O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança o acesso aos seus recursos da AWS, controlando quem está autenticado e autorizado a usá-los.
- O AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para proteger seus dados.
- O AWS Organizations é um serviço de gerenciamento de contas que ajuda você a consolidar várias contas AWS em uma organização que você cria e gerencia de maneira centralizada.
- O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.
- O AWS SDK para Python (Boto3) é um kit de desenvolvimento de software que ajuda você a integrar seu aplicativo, biblioteca ou script Python aos serviços da AWS.

Outras ferramentas e serviços

- HashiCorp O Terraform é um aplicativo de interface de linha de comando que ajuda você a usar o código para provisionar e gerenciar a infraestrutura e os recursos da nuvem.
- Python é uma linguagem de programação de uso geral.
- O jq é um processador de linha de comando que ajuda você a trabalhar com arquivos JSON.

Repositório de código

O código desse padrão está disponível no GitHub organizations-with-terraform repositório amazon-guardduty-for-aws-.

Épicos

Habilitar GuardDuty na organização

Tarefa	Descrição	Habilidades necessárias
Clonar o repositório.	Em um shell bash, execute o comando a seguir. Em Clonar o repositório na seção Informações adicionais, você pode copiar o comando completo contendo a URL do GitHub repositório. Isso clona o organizations-with-terraform repositório amazon-guardduty-for-aws- de. GitHub `git clone <github-repository-url>`	DevOps engenheiro
Edite o arquivo de configuração do Terraform.	1. Na pasta `root` do repositório clonado, replique o arquivo configuration.json .sample executando o comando a seguir. `cp configuration.json .sample configuration.json` 2. Edite o novo arquivo configuration.json e defina os valores para cada uma das seguintes variáveis: • `management_acc_id` : ID da conta de gerenciamento.	DevOps engenheiro, AWS geral, Terraform, Python

Tarefa	Descrição	Habilidades necessárias
	• `delegated_admin_acc_id` : ID da conta de segurança. • `logging_acc_id` : ID da conta de registro em log. • `target_regions` — Lista separada por vírgula das regiões da AWS nas quais você deseja habilitar. GuardDuty • `organization_id` — ID da AWS Organizations da organização na qual você está habilitando GuardDuty. • `default_region` : a região em que seu estado do Terraform está armazenado na conta de gerenciamento. Essa é a mesma região em que você implantou o bucket do S3 e a tabela do DynamoDB para o backend do Terraform. • `role_to_assume_for_role_creation` : nome que você deseja atribuir a um novo perfil do IAM nas contas de segurança e registro em	

Tarefa	Descrição	Habilidades necessárias
	log. Você cria esse novo perfil na próxima história. O Terraform assume esse perfil para criar o perfil do IAM `GuardDutyTerraformOrgRole` nas contas de segurança e registro em log. • `finding_publishing_frequency` — Frequência na qual GuardDuty publica as descobertas no bucket do S3. • `guardduty_findings_bucket_region` : região preferencial na qual você deseja criar o bucket do S3 para descobertas publicadas. • `logging_acc_s3_bucket_name` : nome preferido do bucket do S3 para descobertas publicadas. • `security_acc_kms_key_alias` — Alias do AWS KMS para a chave usada para criptografar descobertas. GuardDuty • `s3_access_log_bucket_name` — Nome de um bucket S3 preexistente em que você deseja	

Tarefa	Descrição	Habilidades necessárias
	coletar registros de acesso para o bucket S3 usado para descobertas. GuardDuty Esse bucket deve estar na mesma região da AWS que o bucket de GuardDuty descobertas. • `tfm_state_backend_s3_bucket` : nome do bucket S3 preexistente para armazenar o estado do backend remoto do Terraform. • `tfm_state_backend_dynamodb_table` : nome da tabela preexistente do DynamoDB para bloquear o estado do Terraform. 3. Salve e feche o arquivo de configuração.	

Tarefa	Descrição	Habilidades necessárias
Gere CloudFormation modelos para novas funções do IAM.	Esse padrão inclui uma solução IaC para criar dois CloudFormation modelos. Esses modelos criam dois perfis do IAM que o Terraform usa durante o processo de configuração. Esses modelos seguem as práticas recomendadas de segurança de permissões com privilégios mínimos. 1. Em um shell do Bash, na pasta `root` do repositór io, navegue até `cfn-templates/` . Essa pasta contém arquivos CloudFormation de modelos com stubs. 2. Execute o seguinte comando: Isso substitui os stubs pelos valores fornecidos no arquivo configuration.json. `bash scripts/r eplace_config_stub s.sh` 3. Confirme se os seguintes CloudFormation modelos foram criados na `cfn-templates/` pasta: • management-account-role.yaml — Esse arquivo	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
	contém a definição da função e as permissões associadas à função do IAM na conta de gerenciamento, que tem as permissões mínimas necessárias para concluir esse padrão. • role-to-assume-for-role-creation.yaml — Esse arquivo contém a definição da função e as permissões associadas à função do IAM nas contas de segurança e registro. O Terraform assume essa função para criar a GuardDuty TerraformOrgRolefunção nessas contas.	

Tarefa	Descrição	Habilidades necessárias
Criar o perfil do IAM.	Seguindo as instruções em Criação de uma pilha (CloudFormation documentação), faça o seguinte: 1. Implante a pilha role-to-assume-for-role-creation.yaml nas contas de segurança e de registro. 2. Implante a pilha management-account-role.yaml na conta de gerenciamento. Quando você criar a pilha com sucesso e ver o status da `CREATE_COMPLETE` pilha, na saída, anote o nome do recurso da Amazon (ARN) desse novo perfil.	DevOps engenheiro, General AWS
Provisione o perfil do IAM na conta de gerenciamento.	Como prática recomendada de segurança, recomendamos que você assuma a nova função management-account-roledo IAM antes de continuar. Na AWS Command Line Interface (AWS CLI), insira o comando em Assumir o perfil do IAM da conta de gerenciamento na seção deInformações adicionais.	DevOps engenheiro, General AWS

Tarefa	Descrição	Habilidades necessárias
Execute o script de configuração.	Na pasta `root` do repositório, execute o comando a seguir para iniciar o script de configuração. `bash scripts/full-setup.sh` O script full-setup.sh executa as seguintes ações: • Exporta todos os valores de configuração como variáveis de ambiente • Gera os arquivos de código backend.tf e terraform .tfvars para cada módulo do Terraform • Permite acesso confiável para GuardDuty a organização por meio da AWS CLI. • Importa o estado da organização para o estado do Terraform • Cria o bucket do S3 para publicar descobertas na conta de registro em log • Cria a chave do AWS KMS para criptografar descobertas na conta de segurança • Ativa GuardDuty em toda a organização, em todas as regiões selecionadas,	DevOps engenheiro, Python

Tarefa	Descrição	Habilidades necessárias
	conforme descrito na seção Arquitetura	

(Opcional) Desativar GuardDuty na organização

Tarefa	Descrição	Habilidades necessárias
Executar o script de limpeza.	Se você usou esse padrão para habilitar GuardDuty para a organização e quiser desabilitá-lo GuardDuty, na `root` pasta do repositório, execute o comando a seguir para iniciar o script cleanup-gd.sh. `bash scripts/cleanup-gd.sh` Esse script é desativado GuardDuty na organização de destino, remove todos os recursos implantados e restaura a organização ao estado anterior antes de usar o Terraform para habilitar. GuardDuty **Note** Esse script não remove os arquivos de estado do Terraform nem bloqueia os arquivos dos back-	DevOps engenheiro, AWS geral, Terraform, Python

Tarefa	Descrição	Habilidades necessárias
	ends locais e remotos. Se você precisar fazer isso, deverá executar essas ações manualmente. Além disso, esse script não exclui a organizaç ão importada nem as contas gerenciad as por ela. O acesso confiável para GuardDuty não está desativado como parte do script de limpeza.	
Remover os perfis do IAM.	Exclua as pilhas que foram criadas com os modelos role-to-assume-for-role-creation.yaml e .yaml. management-account-role CloudFormation Para obter mais informações, consulte Excluindo uma pilha (CloudFormation documentação).	DevOps engenheiro, General AWS

Recursos relacionados

Documentação da AWS

- Gerenciando várias contas (GuardDuty documentação)
- Conceder o privilégio mínimo (documentação do IAM)

Marketing da AWS

- Amazon GuardDuty
- AWS Organizations

Outros recursos

- Terraforma
- Documentação da CLI do Terraform

Mais informações

Clonar o repositório

Execute o comando a seguir para clonar o GitHub repositório.

```
git clone https://github.com/aws-samples/amazon-guardduty-for-aws-organizations-with-terraform
```

Assumir o perfil do IAM na conta de gerenciamento

Para assumir um perfil do IAM na conta de gerenciamento, execute o comando a seguir. Substitua `<IAM role ARN>` pelo ARN do seu perfil do IAM .

```
export ROLE_CREDENTIALS=$(aws sts assume-role --role-arn <IAM role ARN> --role-session-name AWSCLI-Session --output json)
export AWS_ACCESS_KEY_ID=$(echo $ROLE_CREDENTIALS | jq .Credentials.AccessKeyId | sed 's/"//g')
export AWS_SECRET_ACCESS_KEY=$(echo $ROLE_CREDENTIALS | jq .Credentials.SecretAccessKey | sed 's/"//g')
export AWS_SESSION_TOKEN=$(echo $ROLE_CREDENTIALS | jq .Credentials.SessionToken | sed 's/"//g')
```

Verifique as melhores práticas operacionais para o PCI DSS 4.0 usando AWS Config

Criado por Tala Qraitem (AWS) e Alex Goff (AWS)

Resumo

O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) descreve protocolos técnicos e operacionais essenciais para ajudar a proteger os dados de pagamento. O PCI DSS foi desenvolvido para incentivar e aprimorar a segurança dos dados das contas de cartões de pagamento. Também facilita a adoção global de medidas de segurança consistentes. Embora tenha sido projetado especificamente para ambientes com dados de contas de cartões de pagamento, você pode usar o PCI DSS para ajudar a se proteger contra ameaças e proteger outros elementos no ecossistema de pagamento.

A versão 4.0 do PCI DSS foi lançada para atender aos requisitos em evolução, fornecer esclarecimentos ou orientações adicionais e melhorar a estrutura e o formato do padrão. Para obter mais informações sobre as alterações, consulte Resumo das alterações do PCI DSS versão 3.2.1 para 4.0.

Um pacote de AWS Config conformidade é um conjunto de AWS Config regras e ações de remediação que ajudam você a criar verificações de governança de segurança, operacionais ou de otimização de custos. Você pode implantar um pacote de conformidade como uma única entidade em um Conta da AWS e Região da AWS, ou você pode implantar em uma organização em. AWS Organizations

Os pacotes de conformidade para a versão 4.0 do PCI DSS aumentam e se baseiam no pacote de conformidade da versão 3.2.1. As regras no pacote de conformidade são mapeadas com as regras do padrão. Para obter mais informações, consulte o mapeamento fornecido na seção Anexos. Você pode escolher entre duas versões desse pacote de conformidade: uma que inclui tipos de recursos globais e outra que os exclui.

> **Important**
>
> Os pacotes de conformidade não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por fazer sua própria avaliação sobre se o uso atende aos requisitos legais e regulamentares aplicáveis.

Pré-requisitos e limitações

Pré-requisitos

- Tenha um ativo Conta da AWS.
- Configurar AWS Config.
- Atenda aos pré-requisitos dos pacotes de conformidade.
- Implante o pacote de conformidade do PCI DSS versão 3.2.1.
- Tenha permissões para acessar AWS Config e gerenciar pacotes de conformidade. Para ver um exemplo de política, consulte a seção Informações adicionais desse padrão.

Limitações

- Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada um. AWS service (Serviço da AWS) A menos que especificado de outra forma, cada cota é específica da região. Você pode solicitar aumentos para algumas cotas, mas nem todas as cotas podem ser aumentadas. Certifique-se de estar familiarizado com os limites do AWS Config serviço, incluindo os limites para pacotes de conformidade de conta única e pacotes de conformidade organizacional.
- A versão desse pacote de conformidade que inclui tipos de recursos globais é destinada à implantação somente na `us-east-1` região.
- A versão desse pacote de conformidade que exclui os tipos de recursos globais é destinada à implantação somente nas seguintes regiões:
  - `ap-east-1`
  - `ap-south-1`
  - `ap-northeast-2`
  - `ap-southeast-1`
  - `ap-southeast-2`
  - `ap-northeast-1`
  - `ca-central-1`
  - `eu-central-1`
  - `eu-west-1`
  - `eu-west-2`

- `eu-west-3`
- `eu-north-1`
- `sa-east-1`
- `us-east-2`
- `us-west-1`
- `us-west-2`

Ferramentas

Serviços da AWS

- AWS Configfornece uma visão detalhada dos recursos em seu computador Conta da AWS e de como eles estão configurados. Ajuda a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo.
- O AWS Systems Manager ajuda você a gerenciar suas aplicações e infraestrutura em execução na Nuvem AWS. Ele simplifica o gerenciamento de aplicativos e recursos, reduz o tempo para detectar e resolver problemas operacionais e ajuda você a gerenciar seus AWS recursos com segurança em grande escala.

Repositório de código

Os pacotes de conformidade estão localizados no repositório de pacotes de AWS Config conformidade. GitHub Esse repositório contém os seguintes modelos relacionados à versão 4.0 do PCI DSS:

- Melhores práticas operacionais para PCI-DSS-V4.0- .yaml including-global-resourcetypes
- Melhores práticas operacionais para PCI-DSS-V4.0- .yaml excluding-global-resourcetypes

Épicos

Implemente e gerencie o pacote de conformidade

Tarefa	Descrição	Habilidades necessárias
Baixe o pacote de conformidade.	Se você estiver implantando o pacote de conformidade na `us-east-1` região, baixe o modelo Operational-Best-Practices-for-PCI-DSS-v4.0 - .yaml. including-global-resourcetypes Se você estiver implantando o pacote de conformidade em uma região diferente, baixe o modelo Operational-Best-Practices-for-PCI-DSS-v4.0 - .yaml. excluding-global-resourcetypes	DevOps engenheiro
(Opcional) Modifique o pacote de conformidade.	Você pode modificar o modelo do pacote de conformidade de acordo com as necessidades exclusivas da sua organização. Por exemplo, você pode criar ações de remediação personalizadas. Para obter mais informações sobre como criar e modificar modelos, consulte Criação de modelos para pacotes de conformidade personalizados na documentação. AWS Config	AWS geral
Implante o pacote de conformidade.	Se você estiver implantando em um destino Conta da	AWS geral

Tarefa	Descrição	Habilidades necessárias
	AWS ou Região da AWS, siga as instruções em Implantação de pacotes de conformidade na documentação. AWS Config Você pode usar o AWS Management Console ou o AWS Command Line Interface (AWS CLI). Se você estiver implantando o pacote de conformidade em uma organização em AWS Organizations, siga as instruções em Implantar o pacote de AWS Config conformidade usando a Configuração rápida na documentação. AWS Systems Manager	
(Opcional) Edite o pacote de conformidade.	Se você quiser editar o pacote de conformidade, siga as instruções em Edição de pacotes de conformidade na documentação. AWS Config Você pode usar o AWS Management Console ou AWS CLI o.	AWS geral

Tarefa	Descrição	Habilidades necessárias
(Opcional) Exclua o pacote de conformidade.	Se você quiser excluir o pacote de conformidade, siga as instruções em Excluindo pacotes de conformidade na documentação. AWS Config Você pode usar o AWS Management Console ou AWS CLI o.	AWS geral

Recursos relacionados

AWS recursos

- Pacotes de conformidade para AWS Config(documentação)AWS Config
- Implemente o pacote de AWS Config conformidade usando o Quick Setup (documentação do Systems Manager)
- Conformidade com PCI DSS em AWS(site)AWS
- PCI DSS versão 4.0 ativado AWS(guia de conformidade)

Recursos do PCI DSS

- Hub de recursos PCI DSS versão 4.0
- Biblioteca de documentos do PCI Security Standards Council
- Resumo das alterações da versão 3.2.1 para 4.0 do PCI DSS

Mais informações

Veja a seguir um exemplo de política AWS Identity and Access Management (IAM) que permite ao usuário acessar AWS Config e gerenciar pacotes de conformidade:

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

```
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:PutConformancePack",
                "config:DeleteConfigRule",
                "config:DeleteRemediationConfiguration",
                "config:DeleteConformancePack",
                "config:PutRemediationConfigurations",
                "config:BatchGetAggregateResourceConfig",
                "config:BatchGetResourceConfig",
                "config:Get*",
                "config:Describe*",
                "config:Deliver*",
                "config:List*",
                "config:Select*"
            ],
            "Resource": "*"
        }
    ]
}
```

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Verificar se os novos clusters do Amazon Redshift têm os endpoints SSL necessários

Criado por Priyanka Chaudhary (AWS)

Resumo

Esse padrão fornece um CloudFormation modelo da Amazon Web Services (AWS) que notifica você automaticamente quando um novo cluster do Amazon Redshift é lançado sem endpoints Secure Sockets Layer (SSL).

O Amazon Redshift é um serviço de data warehouse em escala de petabytes totalmente gerenciado baseado na nuvem. Ele foi projetado para armazenamento e análise de conjuntos de dados em grande escala. Ele também é usado para realizar migrações de banco de dados em grande escala. Por motivos de segurança, o Amazon Redshift oferece suporte a SSL para criptografar a conexão entre o aplicativo cliente do SQL Server do usuário e o cluster do Amazon Redshift. Para configurar seu cluster para solicitar uma conexão SSL, configure o parâmetro `require_SSL` como `true` no grupo de parâmetros que está associado ao cluster durante a inicialização.

O controle de segurança fornecido com esse padrão monitora as chamadas de API do Amazon Redshift nos CloudTrail logs da AWS e inicia um evento Amazon CloudWatch Events para o CreateCluster,, ModifyClusterRestoreFromClusterSnapshot, e. CreateClusterParameterGroupModifyClusterParameterGroup APIs Quando o evento detecta um deles APIs, ele chama o AWS Lambda, que executa um script Python. A função Python analisa o CloudWatch evento para os eventos listados. CloudTrail Quando um cluster do Amazon Redshift é criado, modificado ou restaurado a partir de um snapshot existente, um novo grupo de parâmetros é criado para o cluster ou um grupo de parâmetros existente é modificado, a função verifica o parâmetro `require_SSL` do cluster. Se o valor do parâmetro for `false`, a função enviará uma notificação do Amazon Simple Notification Service (Amazon SNS) ao usuário com as informações relevantes: nome do cluster do Amazon Redshift, região da AWS, conta da AWS e nome do recurso da Amazon (ARN) for Lambda de onde essa notificação é proveniente.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa

- Uma nuvem privada virtual (VPC) com um grupo de sub-redes de cluster e um grupo de segurança associado.

Limitações

- Esse controle de segurança é regional. Você deve implantá-lo em cada região da AWS que você deseja monitorar.

Arquitetura

Arquitetura de destino

Automação e escala

- Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

Serviços da AWS

- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores
- Amazon Redshift: o Amazon Redshift é um serviço de data warehouse em escala de petabytes totalmente gerenciado na nuvem.
- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web.

- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail. Os assinantes recebem todas as mensagens publicadas nos tópicos para os quais eles se inscrevem, e todos os assinantes em um tópico recebem as mesmas mensagens.

Código

Esse padrão inclui os seguintes anexos:

- `RedshiftSSLEndpointsRequired.zip`: o código Lambda para o controle de segurança.
- `RedshiftSSLEndpointsRequired.yml`— O CloudFormation modelo que configura o evento e a função Lambda.

Épicos

Configurar o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	No console do Amazon S3, escolha ou crie um bucket do S3 para hospedar o arquivo .zip do código do Lambda. Esse bucket do S3 deve estar na mesma região da AWS que o cluster do Amazon Redshift que você deseja monitorar. Um nome de bucket do S3 é globalmente exclusivo, e o namespace é compartilhado por todas as contas da AWS. O nome do bucket do S3 não pode incluir barras iniciais.	Arquiteto de nuvem
Fazer o upload do código do Lambda.	Faça upload do arquivo .zip do código do Lambda fornecido	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	na seção Anexos no bucket do S3.	

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo da AWS.	Abra o CloudFormation console da AWS na mesma região da AWS do seu bucket do S3 e implante o modelo `RedshiftSSLEndpointsRequired.yml` anexado. Para obter mais informações sobre a implantação de CloudFormation modelos da AWS, consulte Como criar uma pilha no CloudFormation console da AWS na CloudFormation documentação.	Arquiteto de nuvem
Preencher os parâmetros no modelo.	Ao iniciar o modelo, você será solicitado a fornecer as seguintes informações: • Bucket S3: especifique o bucket que você criou ou selecionou no primeiro épico. É onde que você fez o upload do código do Lambda anexado (arquivo .zip). • Chave do S3: especifique a localização do arquivo .zip	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	do Lambda em seu bucket do S3 (por exemplo, nome do arquivo.zip ou controles /nome do arquivo.zip). Não inclua barras iniciais. • E-mail de notificação: forneça um endereço de e-mail ativo para receber notificações do Amazon SNS. • Nível de registro em log do Lamba: especifique o nível de registro e a frequência da função do Lambda. Use Informações para registrar em log mensagens informativas detalhadas sobre o progresso, Erro para eventos de erro que ainda permitiriam a continuidade da implantação e Aviso sobre situações potencialmente prejudiciais.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o CloudFormation modelo é implantado com sucesso, ele envia um e-mail de assinatura para o endereço de e-mail que você forneceu. Você deve confirmar essa	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	assinatura de e-mail para começar a receber notificaç ões de violação.	

Recursos relacionados

- Criar um bucket do S3 (documentação do Amazon S3)
- Upload de arquivos para um bucket do S3 (documentação do Amazon S3)
- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS (documentação CloudTrail da AWS CloudTrail)
- Criar um cluster do Amazon Redshift (documentação do Amazon Redshift)
- Configurando opções de segurança para conexões (documentação do Amazon Redshift)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Verificar se os novos clusters do Amazon Redshift são executados em uma VPC

Criado por Priyanka Chaudhary (AWS)

Resumo

Esse padrão fornece um CloudFormation modelo da Amazon Web Services (AWS) que notifica você automaticamente quando um cluster do Amazon Redshift é lançado fora de uma nuvem privada virtual (VPC).

O Amazon Redshift é um produto de data warehouse em escala de petabytes totalmente gerenciado baseado na nuvem. Ele foi projetado para armazenamento e análise de conjuntos de dados em grande escala. Ele também é usado para realizar migrações de banco de dados em grande escala. A Amazon Virtual Private Cloud (Amazon VPC) permite provisionar uma seção logicamente isolada da Nuvem AWS , em que é possível executar recursos da AWS, como clusters do Amazon Redshift, em uma rede virtual que você mesmo define.

O controle de segurança fornecido com esse padrão monitora as chamadas de API do Amazon Redshift nos CloudTrail logs da AWS e inicia um evento Amazon CloudWatch Events para e. CreateClusterRestoreFromClusterSnapshot APIs Quando o evento detecta um deles APIs, ele chama o AWS Lambda, que executa um script Python. A função Python analisa o evento. CloudWatch Se um cluster do Amazon Redshift for criado ou restaurado a partir de um snapshot e aparecer fora da rede Amazon VPC, a função enviará uma notificação do Amazon Simple Notification Service (Amazon SNS) ao usuário com as informações relevantes: nome do cluster do Amazon Redshift, região da AWS, conta da AWS e nome do recurso da Amazon (ARN) for Lambda de onde essa notificação é proveniente.

Pré-requisitos e limitações

Pré-requisitos

- Uma conta AWS ativa
- Uma VPC com um grupo de sub-redes de cluster e um grupo de segurança associado.

Limitações

- O CloudFormation modelo da AWS oferece suporte somente RestoreFromClusterSnapshotàs ações CreateClustere (novos clusters). Ele não detecta clusters existentes do Amazon Redshift que foram criados fora de uma VPC.
- Esse controle de segurança é regional. Você deve implantá-lo em cada região da AWS que você deseja monitorar.

Arquitetura

Arquitetura de destino

Automação e escala

Se você estiver usando o AWS Organizations, poderá usar o AWS Cloudformation StackSets para implantar esse modelo em várias contas que você deseja monitorar.

Ferramentas

Serviços da AWS

- AWS CloudFormation — CloudFormation A AWS ajuda você a modelar e configurar seus recursos da AWS, provisioná-los de forma rápida e consistente e gerenciá-los durante todo o ciclo de vida. Você pode usar um modelo para descrever seus recursos e as dependências deles, além de inicializá-los e configurá-los juntos como uma pilha, em vez de gerenciar recursos individualmente.
- AWS CloudTrail — CloudTrail A AWS ajuda você a implementar governança, conformidade e auditoria operacional e de risco da sua conta da AWS. As ações realizadas por um usuário, função ou serviço da AWS são registradas como eventos em CloudTrail.
- Amazon CloudWatch Events — O Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos recursos da AWS.
- AWS Lambda: o AWS Lambda é um serviço de computação que permite a execução do código sem provisionar ou gerenciar servidores O AWS Lambda executa o código somente quando necessário e dimensiona automaticamente, desde algumas solicitações por dia a milhares por segundo.
- Amazon Redshift: o Amazon Redshift é um serviço de data warehouse em escala de petabytes totalmente gerenciado na nuvem. O Amazon Redshift é integrado ao seu data lake, o que permite que você use seus dados para adquirir novos insights para seus negócios e clientes.

- Amazon S3: o Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos altamente escalável que você pode usar para uma ampla variedade de soluções de armazenamento, incluindo sites, aplicativos móveis, backups e data lakes.
- Amazon SNS: o Amazon Simple Notification Service (Amazon SNS) coordena e gerencia a entrega ou o envio de mensagens entre publicadores e clientes, incluindo servidores da Web e endereços de e-mail.

Código

Esse padrão inclui os seguintes anexos:

- `RedshiftMustBeInVPC.zip`: o código Lambda para o controle de segurança.
- `RedshiftMustBeInVPC.yml`— O CloudFormation modelo que configura o evento e a função Lambda.

Para usar esses arquivos, siga as instruções da próxima seção.

Épicos

Configurar o bucket do S3

Tarefa	Descrição	Habilidades necessárias
Definir o bucket do S3.	No console do Amazon S3, escolha ou crie um bucket do S3 para hospedar o arquivo .zip do código do Lambda. Esse bucket do S3 deve estar na mesma região da AWS que o cluster do Amazon Redshift que você deseja monitorar. Um nome de bucket do S3 é globalmente exclusivo, e o namespace é compartilhado por todas as contas da AWS. O nome do	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	bucket do S3 não pode incluir barras iniciais.	
Fazer o upload do código do Lambda.	Faça upload do arquivo .zip do código do Lambda (arquivo `RedshiftMustBeInVPC.zip`) fornecido na seção Anexos para o bucket do S3.	Arquiteto de nuvem

Implante o CloudFormation modelo

Tarefa	Descrição	Habilidades necessárias
Inicie o CloudFormation modelo.	Abra o CloudFormation console da AWS na mesma região da AWS do seu bucket do S3 e implante o modelo anexado (`RedshiftMustBeInVPC.yml`). Para obter mais informações sobre a implantação de CloudFormation modelos da AWS, consulte Como criar uma pilha no CloudFormation console da AWS na CloudFormation documentação.	Arquiteto de nuvem
Preencher os parâmetros no modelo.	Ao iniciar o modelo, você será solicitado a fornecer as seguintes informações: • Bucket S3: especifique o bucket que você criou ou selecionou no primeiro épico. É onde que você	Arquiteto de nuvem

Tarefa	Descrição	Habilidades necessárias
	fez o upload do código do Lambda anexado (arquivo .zip). • Chave do S3: especifique a localização do arquivo .zip do Lambda em seu bucket do S3 (por exemplo, nome do arquivo.zip ou controles /nome do arquivo.zip). Não inclua barras iniciais. • E-mail de notificação: forneça um endereço de e-mail ativo para receber notificações do Amazon SNS. • Nível de registro em log do Lamba: especifique o nível de registro e a frequência da função do Lambda. Use Informações para registrar em log mensagens informativas detalhadas sobre o progresso, Erro para eventos de erro que ainda permitiriam a continuidade da implantação e Aviso sobre situações potencialmente prejudiciais.	

Confirmar a assinatura

Tarefa	Descrição	Habilidades necessárias
Confirmar a assinatura.	Quando o CloudFormation modelo é implantado com sucesso, ele envia um e-mail de assinatura para o endereço de e-mail que você forneceu. Você deve confirmar essa assinatura de e-mail para começar a receber notificaç ões de violação.	Arquiteto de nuvem

Recursos relacionados

- Criar um bucket do S3 (documentação do Amazon S3)
- Upload de arquivos para um bucket do S3 (documentação do Amazon S3)
- Criação de uma pilha no CloudFormation console da AWS (CloudFormation documentação da AWS)
- Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando a AWS (documentação CloudTrail da AWS CloudTrail)
- Criar um cluster do Amazon Redshift (documentação do Amazon Redshift)

Anexos

Para acessar o conteúdo adicional associado a este documento, descompacte o seguinte arquivo: attachment.zip

Mais padrões

- Acesse um bastion host usando o Session Manager e o Amazon EC2 Instance Connect
- Acesse aplicativos de contêineres de forma privada no Amazon ECS usando o AWS Fargate, a PrivateLink AWS e um Network Load Balancer
- Acesse aplicativos de contêineres de forma privada no Amazon ECS usando a AWS PrivateLink e um Network Load Balancer
- Acesse aplicativos de contêineres de forma privada no Amazon EKS usando a AWS PrivateLink e um Network Load Balancer
- Permitir que EC2 as instâncias gravem acesso aos buckets do S3 nas contas do AMS
- Associe um AWS CodeCommit repositório em um Conta da AWS com o Amazon SageMaker AI Studio Classic em outra conta
- Autentique os usuários existentes do aplicativo React usando o Amazon Cognito e a interface do usuário do AWS Amplify
- Automatizar a adição ou atualização de entradas de registro do Windows usando o AWS Systems Manager
- Automatize a aplicação da criptografia no AWS Glue usando um modelo da AWS CloudFormation
- Anexe automaticamente uma política gerenciada da AWS para Systems Manager aos perfis de EC2 instância usando o Cloud Custodian e o AWS CDK
- Criptografe automaticamente volumes novos e existentes do Amazon EBS
- Bloqueie o acesso público ao Amazon RDS usando o Cloud Custodian
- Centralize a resolução de DNS usando o Microsoft AWS Managed Microsoft AD Active Directory local
- Implemente o escaneamento Checkov personalizado e centralizado para aplicar a política antes de implantar a infraestrutura AWS
- Verifique os aplicativos ou CloudFormation modelos do AWS CDK para obter as melhores práticas usando pacotes de regras cdk-nag
- Verifique as EC2 instâncias para ver as tags obrigatórias no lançamento
- Configurar o acesso entre contas ao Amazon DynamoDB
- Configure a criptografia HTTPS para o Oracle JD Edwards EnterpriseOne no Oracle WebLogic usando um Application Load Balancer
- Configure o registro e o monitoramento de eventos de segurança em seu AWS IoT ambiente
- Configurar a autenticação de TLS mútuo para aplicativos em execução no Amazon EKS

- Conecte-se usando um túnel SSH no pgAdmin
- Crie um aplicativo React usando o AWS Amplify e adicione autenticação com o Amazon Cognito
- Crie um relatório das descobertas do Network Access Analyzer para acesso de entrada à Internet em vários Contas da AWS
- Personalize os CloudWatch alertas da Amazon para AWS Network Firewall
- Implante um firewall usando o AWS Network Firewall e o AWS Transit Gateway
- Implemente uma ChatOps solução para gerenciar os resultados do escaneamento SAST usando o Amazon Q Developer em aplicativos de bate-papo, ações personalizadas e AWS CloudFormation
- Documente seu projeto de landing zone na AWS
- Habilite conexões criptografadas para instâncias de banco de dados PostgreSQL no Amazon RDS
- Criptografe uma instância de banco de dados Amazon RDS para PostgreSQL existente
- Aplique a marcação automática dos bancos de dados do Amazon RDS no lançamento
- Imponha a marcação dos clusters do Amazon EMR no lançamento
- Garanta que o registro do Amazon EMR no Amazon S3 esteja habilitado no lançamento
- Gere um CloudFormation modelo da AWS contendo regras gerenciadas do AWS Config usando o Troposphere
- Receber notificações do Amazon SNS quando o estado de chave de uma chave do AWS KMS mudar
- Ajude a aplicar a marcação no DynamoDB
- Identifique e alerte quando os recursos do Amazon Data Firehose não estiverem criptografados com uma chave AWS KMS
- Implemente SHA1 o hashing para dados de PII ao migrar do SQL Server para o PostgreSQL
- Melhore o desempenho operacional habilitando o Amazon DevOps Guru em várias regiões e contas da AWS e OUs com o AWS CDK
- Ingira e migre instâncias EC2 do Windows para uma conta do AWS Managed Services
- Migre o Amazon RDS para Oracle para o Amazon RDS para PostgreSQL no modo SSL usando o AWS DMS
- Migre um pilha ELK para a Nuvem Elastic na AWS
- Migre uma workload do F5 BIG-IP para o F5 BIG-IP VE na Nuvem AWS
- Monitore o Amazon Aurora em busca de instâncias sem criptografia
- Provisione funções do IAM com privilégios mínimos implantando uma solução de máquina de venda automática de funções

- Alternar as credenciais do banco de dados sem reiniciar os contêineres
- Proteja e simplifique o acesso de usuários em um banco de dados de federação Db2 na AWS usando contextos confiáveis
- Envie AWS WAF registros para o Splunk usando o AWS Firewall Manager Amazon Data Firehose
- Ofereça conteúdo estático em um bucket do Amazon S3 por meio de uma VPC usando a Amazon CloudFront
- Configure a end-to-end criptografia para aplicativos no Amazon EKS usando cert-manager e Let's Encrypt
- Use o usuário IDs nas políticas do IAM para controle de acesso e automação
- Verifique se os balanceadores de carga ELB exigem terminação TLS
- Visualize registros e métricas do AWS Network Firewall usando o Splunk
- Visualize relatórios de credenciais do IAM para todas as contas da AWS usando a Amazon QuickSight

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.