Approches de sauvegarde et de restauration sur AWS

AWS Directives prescriptives

AWS Directives prescriptives: Approches de sauvegarde et de restauration sur AWS

Table of Contents

Approches de sauvegarde et de restauration surAWS

Khurram Nizami, Amazon Web Services (AWS)

avril 2023(historique du document)

Ce guide explique comment mettre en œuvre des approches de sauvegarde et de restauration à l'aide d'Amazon Web Services (AWS) services pour les architectures sur site, natives du cloud et hybrides. Ces approches permettent de réduire les coûts, d'améliorer l'évolutivité et d'accroître la durabilité afin de répondre aux objectifs de temps de restauration (RTO), de point de restauration (RPO) et aux exigences de conformité.

Ce guide s'adresse aux responsables techniques chargés de protéger les données dans les environnements informatiques et cloud de leur entreprise.

Ce guide couvre différentes architectures de sauvegarde (applications cloud natives, environnements hybrides et sur site). Il couvre également les services Amazon Web Services (AWS) associés qui peuvent être utilisés pour créer des solutions de protection des données évolutives et fiables pour les composants non immuables de votre architecture.

Une autre approche consiste à moderniser vos charges de travail pour utiliser des architectures immuables, réduisant ainsi le besoin de sauvegarde et de restauration des composants.AWSfournit un certain nombre de services permettant de mettre en œuvre des architectures immuables et de réduire les besoins en matière de sauvegarde et de restauration, notamment :

- Sans serveur avecAWS Lambda
- Des conteneurs avec Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) etAWS Fargate
- Amazon Machine Images (AMI) avec Amazon Elastic Compute Cloud (Amazon EC2)

À mesure que la croissance des données d'entreprise s'accélère, la tâche consistant à les protéger devient de plus en plus difficile. Les questions concernant la durabilité et l'évolutivité des approches de sauvegarde sont monnaie courante, notamment celle-ci : comment le cloud répond-il à mes besoins de sauvegarde et de restauration ?

Ce guide aborde les sujets suivants :

- Choix AWS des services de protection des données

- Conception d'une solution de sauvegarde et de restauration
- Backup et restauration à l'aide deAWS Backup
- Backup et restauration à l'aide d'Amazon S3 et Amazon S3 Glacier
- Backup et restauration pour Amazon EC2 avec des volumes EBS
- Sauvegarde et restauration depuis une infrastructure sur site versAWS
- Backup et restauration d'applications depuisAWSvers votre centre de données
- Backup et restauration deAWS services cloud natifs
- Backup et restauration pour architectures hybrides
- Reprise après sinistre avecAWS
- Nettoyage des sauvegardes

Pourquoi utiliserAWSen tant que plateforme de protection des données ?

AWS est une solution sécurisée, performante, flexible, économique eteasy-to-useplateforme de cloud computing.AWSprend en charge les tâches complexes nécessaires à la création, à la mise en œuvre et à la gestion de solutions de sauvegarde et de restauration évolutives.

L'utilisation deAWSdans le cadre de votre stratégie de protection des données :

- Durabilité: Amazon Simple Storage Service (Amazon S3), Amazon S3 Glacier et S3 Glacier Deep Archive sont conçus pour offrir une durabilité de 99,999999999 % (11 neuf). Les deux plateformes offrent une sauvegarde fiable des données, avec réplication d'objets sur au moins trois zones de disponibilité géographiquement dispersées. De nombreuxAWSles services utilisent Amazon S3 pour le stockage et les opérations d'exportation/importation. Par exemple, Amazon Elastic Block Store (Amazon EBS) utilise Amazon S3 pour le stockage d'instantanés.
- Sécurité:AWSfournit un certain nombre d'options pour le contrôle d'accès et le chiffrement des données en transit et au repos.
- Infrastructure mondiale:AWSles services sont disponibles dans le monde entier, ce qui vous permet de sauvegarder et de stocker des données dans la région qui répond à vos exigences de conformité et de charge de travail.
- Conformité:AWSl'infrastructure est certifiée conforme aux normes suivantes, ce qui vous permet d'adapter facilement la solution de sauvegarde à votre régime de conformité existant :
  - Contrôles de l'organisation des services (SOC)

  - Déclaration sur les normes relatives aux engagements d'attestation (SSAE) 16
  - Organisation internationale de normalisation (ISO) 27001
  - Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - SEC1
  - Federal Risk and Authorization Management Program (FedRAMP)
- Évolutivité: AvecAWS, vous n'avez pas à vous soucier de la capacité. À mesure que vos besoins évoluent, vous pouvez augmenter ou réduire votre consommation sans frais administratifs.
- Réduction du coût total de possession (TCO): L'échelle deAWSles opérations réduisent les coûts de service et contribuent à réduire le coût total de possession deAWSservices.AWSrépercute ces économies de coûts sur les clients par le biais de baisses de prix.
- Pay-as-you-gotarification: AchatAWSles services dont vous avez besoin et uniquement pendant la période pendant laquelle vous prévoyez de les utiliser.AWSla tarification ne comporte pas de frais initiaux, de pénalités de résiliation ou de contrats à long terme.

Résultats commerciaux ciblés

L'objectif de ce guide est de fournir une vue d'ensemble desAWSservices que vous pouvez utiliser pour prendre en charge les approches de sauvegarde et de restauration dans les domaines suivants :

- Architectures sur site
- Architectures natives pour le cloud
- Architectures hybrides
- Services natifs AWS
- Reprise après sinistre (DR)

Les meilleures pratiques et considérations sont abordées, ainsi qu'un aperçu des services. Ce guide explique également les compromis entre l'utilisation d'une approche plutôt qu'une autre pour la sauvegarde et la restauration.

Choix AWS des services de protection des données

AWS fournit un certain nombre de services de stockage et complémentaires qui peuvent être utilisés dans le cadre de votre approche de sauvegarde et de restauration. Ces services peuvent prendre en charge à la fois des architectures cloud natives et hybrides. Différents services sont plus efficaces pour différents cas d'utilisation.

- Amazon S3, Amazon S3 Glacier et S3 Glacier Deep Archive conviennent à la fois aux cas d'utilisation hybrides et cloud natifs. Ces services fournissent des solutions de stockage d'objets polyvalentes très durables, adaptées à la sauvegarde de fichiers individuels, de serveurs ou de l'ensemble d'un centre de données.
- AWS Storage Gatewayest idéal pour les cas d'utilisation hybrides. Storage Gateway utilise la puissance d'Amazon S3 pour répondre aux besoins courants en matière de sauvegarde et de stockage sur site. Vos applications se connectent au service via une machine virtuelle (VM) ou une passerelle matérielle en utilisant les protocoles de stockage standard suivants :
  - Système de fichiers réseau (NFS)
  - Bloc de messages du serveur (SMB)
  - Interface système Internet pour petits ordinateurs (iSCSI)

  La passerelle relie ces protocoles locaux courants à des services AWS de stockage tels que les suivants :
  - Amazon S3
  - Amazon S3 Glacier
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway permet de fournir plus facilement un stockage élastique et performant pour les fichiers, les volumes, les instantanés et les bandes virtuelles. AWS
- AWS Backupest un service de sauvegarde entièrement géré permettant de centraliser et d'automatiser la sauvegarde des données entre AWS les services. Vous pouvez ainsi configurer les politiques de sauvegarde de manière centralisée et surveiller les activités de sauvegarde AWS des ressources, telles que les suivantes : AWS Backup
  - Volumes EBS
  - Instances EC2 (y compris les applications Windows)

  - Bases de données Amazon RDS et Amazon Aurora
  - Tables DynamoDB
  - Bases de données Amazon Neptune
  - Bases de données Amazon DocumentDB (avec compatibilité MongoDB)
  - Système de fichiers Amazon EFS
  - Systèmes de fichiers Amazon FSx for Lustre et systèmes de fichiers Amazon FSx for Windows File Server
  - Charges de travail VMware sur site et dans VMware Cloud sur AWS
  - Volumes Storage Gateway

  Le coût d'AWS Backup est basé sur le stockage que vous consommez, restaurez et transférez en un mois. Pour plus d'informations, consultez les AWS Backup tarifs.
- AWS Elastic Disaster Recoveryréplique en continu vos machines dans une zone de transit à faible coût de votre AWS compte cible et de votre région préférée. Vous pouvez utiliser Elastic Disaster Recovery pour la reprise après premises-to-cloud sinistre sur site ou entre régions
- AWS Configfournit une vue détaillée de la configuration des AWS ressources de votre AWS compte. Cela inclut la manière dont les ressources sont liées les unes aux autres et la manière dont elles ont été configurées dans le passé. Dans cette vue, vous pouvez voir comment la configuration et les relations des ressources ont évolué au fil du temps.

  Lorsque vous activez l'enregistrement AWS Config de la configuration pour vos AWS ressources, vous conservez un historique de vos relations avec les ressources au fil du temps. Cela permet d'identifier et de suivre les relations entre les AWS ressources (y compris les ressources supprimées) pendant une période pouvant aller jusqu'à sept ans. Par exemple, AWS Config peut suivre la relation entre un volume de snapshots Amazon EBS et l'instance EC2 à laquelle le volume a été attaché.
- AWS Lambdapeut être utilisé pour définir et automatiser par programmation vos procédures de sauvegarde et de restauration pour vos charges de travail. Vous pouvez utiliser les AWS SDK pour interagir avec les AWS services et leurs données. Vous pouvez également utiliser Amazon CloudWatch Events pour exécuter vos fonctions Lambda de manière planifiée.

AWS les services fournissent des fonctionnalités spécifiques pour la sauvegarde et la restauration. Pour chaque AWS service que vous utilisez, consultez la AWS documentation afin de déterminer les fonctionnalités de sauvegarde, de restauration et de protection des données fournies par le service. Vous pouvez utiliser les AWS Command Line Interface (AWS CLI), les AWS SDK et les opérations

d'API pour automatiser les fonctionnalités AWS spécifiques au service pour la sauvegarde et la restauration des données.

Conception d'une solution de sauvegarde et de restauration

Lorsque vous développez une stratégie complète de sauvegarde et de restauration des données, vous devez d'abord identifier les situations de panne ou de sinistre possibles et leur impact potentiel sur l'entreprise. Dans certains secteurs, vous devez prendre en compte les exigences réglementaires en matière de sécurité des données, de confidentialité et de conservation des enregistrements.

Les processus de sauvegarde et de restauration doivent inclure le niveau de granularité approprié pour atteindre l'objectif de temps de restauration (RTO) et l'objectif de point de restauration (RPO) pour la charge de travail et ses processus métier connexes, notamment les suivants :

- Restauration au niveau des fichiers (par exemple, les fichiers de configuration d'une application)
- Restauration au niveau des données de l'application (par exemple, une base de données spécifique dans MySQL)
- Restauration au niveau de l'application (par exemple, une version spécifique d'une application de serveur Web)
- Restauration au niveau du volume Amazon EC2 (par exemple, un volume EBS)
- Restauration au niveau de l'instance EC2. (par exemple, une instance EC2)
- Restauration des services gérés (par exemple, une table DynamoDB)

Assurez-vous de prendre en compte toutes les exigences de restauration de votre solution et les dépendances des données entre les différents composants de votre architecture. Pour garantir la réussite du processus de restauration, coordonnez la sauvegarde et la restauration entre les différents composants de votre architecture.

Les rubriques suivantes décrivent les approches de sauvegarde et de restauration basées sur l'organisation de votre infrastructure. L'infrastructure informatique peut généralement être classée comme étant sur site, hybride ou native pour le cloud.

Backup et restauration à l'aide deAWS Backup

AWS Backupest un service de sauvegarde entièrement géré qui centralise et automatise la sauvegarde des données surAWSServices .AWS Backupfournit une couche d'orchestration qui intègre Amazon CloudWatch,AWS CloudTrail,AWS Identity and Access Management(IAM),AWS Organizationset d'autres services. Ce système centralisé,AWSLa solution native Cloud fournit des fonctionnalités de sauvegarde mondiales qui peuvent vous aider à atteindre vos exigences de reprise après sinistre et de conformité. A l'aide deAWS Backuppermet de configurer de manière centralisée les stratégies de sauvegarde et de surveiller l'activité de sauvegarde pourAWSAWS.

AWS Backupest une solution idéale pour mettre en œuvre des plans de sauvegarde standard pour votreAWSressources dans votreAWScomptes et régions. Etant donné queAWS Backupprend en charge plusieursAWSles types de ressources, il facilite la maintenance et la mise en œuvre d'une stratégie de sauvegarde pour les charges de travail utilisant plusieursAWSressources qui doivent être sauvegardées collectivement.AWS Backupvous permet également de surveiller collectivement une opération de sauvegarde et de restauration impliquant plusieursAWSAWS.

Si vous avez des exigences de conformité et d'audit, vous pouvez utiliser leAWS BackupAudit Managerpermettant de créer des cadres d'audit et des rapports pour prendre en charge vos exigences de conformité. LeAWS BackupVerrouillage de coffreprend également en charge les exigences de conformité en appliquant une configuration WORM (Write-Once, Lecture Many) pour toutes vos sauvegardes stockées dans un coffre-fort de sauvegarde dansAWS Backup.

Un facteur de différenciation clé pourAWS Backupest un support pour les Organizations. Grâce à cette prise en charge, vous pouvez définir et gérer des stratégies de sauvegarde au niveau de l'organisation ou de l'unité organisationnelle et mettre automatiquement en œuvre ces stratégies pour chaque stratégie associée.AWScompte et région. Comme vous embarquez dans le nouveauAWScomptes et régions, vous n'avez pas besoin de définir et de gérer des plans de sauvegarde séparément.

AWS Backuppeut faciliter la mise en œuvre d'une stratégie de sauvegarde à l'échelle de l'organisation à l'aide de balises. Vous pouvez créer des plans de sauvegarde distincts qui possèdent chacun des paramètres de fréquence et de rétention uniques, puis créer des balises de paires clé-valeur uniques qui sélectionnent les ressources à inclure pour la sauvegarde.

Par exemple, vous pouvez créer un plan de sauvegarde quotidien qui démarre une sauvegarde à 5 h 00 UTC quotidiennement et qui dispose d'une stratégie de rétention de 35 jours. Ce plan de sauvegarde peut inclure unaffectation des ressources de sauvegardequi spécifie que toute prise

en chargeAWSressource avec la clé de balisesauvegardeet valeur de balisetous les joursseront sauvegardés conformément à ce plan. En outre, vous pouvez créer un plan de sauvegarde mensuel qui commence à 5 h 00 UTC le premier jour de chaque mois et qui dispose d'une stratégie de rétention de 366 jours. Ce plan de sauvegarde peut inclure une affectation de ressources de sauvegarde qui spécifie que toutes les données prises en chargeAWSressource avec la clé de balisesauvegardeet valeur de balisemensuelseront sauvegardés conformément à ce plan.

Vous pouvez ensuite utiliser les stratégies de balises et lerequired-tags AWS Configrègle pour s'assurer que tous vosAWSles ressources prises en charge possèdent cette clé de balise et l'une de ces valeurs de balise. Cette approche peut vous aider à mettre en œuvre et à maintenir systématiquement une approche de sauvegarde standard dansAWSpour prise en chargeAWS BackupAWS. Vous pouvez étendre cette approche pour normaliser les sauvegardes de vos applications et des couches architecturales qui ont des exigences différentes en matière d'objectif de point de récupération (RPO).

Nous vous recommandons de prendre des mesures pour sécuriser votre coffre-fort de sauvegarde. Par exemple, vous pouvez implémenter une stratégie SCP (Organizations Service Control Policy) qui empêche la suppression de votre coffre-fort de sauvegarde ou le partage avec des éléments non intentionnelsAWScomptes. Pour plus de détails et d'autres considérations importantes en matière de sécurité, consultez leMeilleures pratiques de sécurité pour sécuriser les sauvegardes dansAWSbillet de blog.

AWS Backuppeut simplifier la mise en œuvre de votre plan de reprise après sinistre (DR) pourAWScar il prend en charge plusieursAWSressources qui peuvent être traitées collectivement. Par exemple, vous pouvez implémenterentre Régionsetentre comptessauvegarde pour la plupart desAWStypes de ressource pris en charge parAWS Backup. La sauvegarde entre comptes améliore la sécurité des sauvegardes car une copie est disponible dans un compte distinct. La sauvegarde entre régions améliore la disponibilité car les sauvegardes sont disponibles dans plusieurs régions. Pour plus de détails sur le supportAWStypes de ressources, consultez leDisponibilité des fonctions par ressourcetable.

Vous pouvez utiliser l'exempleBackup et restauration avecAWS Backupsolution open sourcepour implémenter une approche d'infrastructure en tant que code (iAC) et d'intégration continue et de diffusion continue (CI/CD) pour gérer les sauvegardes de votreAWS Organizationsorganisation. Cette solution inclut des fonctionnalités personnalisées, telles que la réapplication automatiqueAWSétiquettes sur restauréAWSainsi que l'établissement d'un coffre-fort de sauvegarde secondaire dans un compte séparé et une région à des fins de reprise après sinistre.

Backup et restauration à l'aide d'Amazon S3 et Amazon S3 Glacier

Amazon S3 et Amazon S3 Glacier sont des services de stockage idéaux pour une utilisation dans les architectures sur site, hybrides et cloud natives. Ces services fournissent des plateformes de stockage durables et peu coûteuses qui offrent une capacité évolutive et ne nécessitent aucune gestion des volumes ou des supports à mesure que vos ensembles de données de sauvegarde augmentent. Le modèle pay-for-what-you d'utilisation et le faible coût par Go/mois font de ces services une solution adaptée à un large éventail de cas d'utilisation liés à la protection des données.

> **Note**
>
> Certaines classes de stockage sont soumises à des frais de durée minimale. Pour plus de détails, consultez la tarification d'Amazon S3 et utilisez la fonction de recherche sur la page Web pour trouver`duration`.

Rubriques

Amazon S3

Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quel volume de données, à tout moment. Vous pouvez utiliser Amazon S3 comme magasin durable pour les données de vos applications et les processus de sauvegarde et de restauration au niveau des fichiers. Par exemple, vous pouvez copier vos sauvegardes de base de données depuis une instance de base de données vers Amazon S3 à l'aide d'un script de sauvegarde à l' AWS CLI aide des kits de développement logiciel (SDK).

AWS les services utilisent Amazon S3 pour un stockage extrêmement durable et fiable, comme dans les exemples suivants :

- Amazon EC2 utilise Amazon S3 pour stocker des instantanés Amazon EBS pour les volumes EBS et pour les magasins d'instances EC2.

- Storage Gateway s'intègre à Amazon S3 pour fournir aux environnements sur site des partages de fichiers, des volumes et des bibliothèques de bandes basés sur Amazon S3.
- Amazon RDS utilise Amazon S3 pour les instantanés de base de données.

De nombreuses solutions de sauvegarde tierces utilisent également Amazon S3. Par exemple, Arcserve Unified Data Protection prend en charge Amazon S3 pour une sauvegarde durable des serveurs sur site et cloud natifs.

Vous pouvez utiliser les fonctionnalités intégrées à Amazon S3 de ces services pour simplifier votre approche de sauvegarde et de restauration. Dans le même temps, vous pouvez bénéficier de la durabilité et de la disponibilité élevées offertes par Amazon S3.

Amazon S3 stocke les données sous forme d'objets au sein de ressources appelées buckets. Vous pouvez stocker autant d'objets que vous le souhaitez dans un compartiment. Vous pouvez écrire, lire et supprimer des objets dans votre compartiment grâce à un contrôle d'accès précis. La taille des objets individuels peut atteindre 5 To.

Amazon S3 propose une gamme de classes de stockage conçues pour différents cas d'utilisation, notamment les classes suivantes :

- S3 Standard pour le stockage à usage général des données fréquemment consultées (par exemple, les fichiers de configuration, les sauvegardes imprévues, les sauvegardes quotidiennes).
- S3 Standard-IA pour les données de longue durée mais moins fréquemment consultées (par exemple, les sauvegardes mensuelles). IA est l'abréviation de « accès peu fréquent ».

Amazon S3 propose des politiques de cycle de vie que vous pouvez configurer pour gérer vos données tout au long de leur cycle de vie. Une fois qu'une politique est définie, vos données sont migrées vers la classe de stockage appropriée sans aucune modification de votre application. Pour plus d'informations, consultez la documentation sur la gestion du cycle de vie des objets Amazon S3.

Pour réduire vos coûts de sauvegarde, utilisez une approche de classe de stockage hiérarchisée basée sur vos objectifs de temps de restauration (RTO) et de point de restauration (RPO), comme dans l'exemple suivant :

- Sauvegardes quotidiennes des 2 dernières semaines à l'aide de S3 Standard
- Sauvegardes hebdomadaires des 3 derniers mois à l'aide de S3 Standard-IA
- Sauvegardes trimestrielles de l'année écoulée sur S3 Glacier Flexible Retrieval

- Sauvegardes annuelles des 5 dernières années sur S3 Glacier Deep Archive
- Sauvegardes supprimées de S3 Glacier Deep Archive après 5 ans

Vous pouvez automatiser la transition de vos sauvegardes en utilisant la gestion du cycle de vie des objets.

> **Note**
>
> Certaines classes de stockage sont soumises à des frais de durée minimale. Pour plus de détails, consultez la tarification d'Amazon S3 et utilisez la fonction de recherche sur la page Web pour trouver`duration`.

Création de compartiments S3 standard pour la sauvegarde et l'archivage

Vous pouvez créer un compartiment S3 standard pour la sauvegarde et l'archivage avec la politique de sauvegarde et de rétention de votre entreprise mise en œuvre par le biais des politiques de cycle de vie S3. Le balisage de la répartition des coûts et les rapports pour la AWS facturation sont basés sur les balises attribuées au niveau du compartiment. Si la répartition des coûts est importante, créez des compartiments S3 de sauvegarde et d'archivage distincts pour chaque projet ou unité commerciale afin de pouvoir répartir les coûts en conséquence.

Vos scripts et applications de sauvegarde peuvent utiliser le compartiment S3 de sauvegarde et d'archivage que vous créez pour stocker des point-in-time instantanés des données d'application et de charge de travail. Vous pouvez créer un préfixe s3 standard pour vous aider à organiser vos instantanés de point-in-time données. Par exemple, si vous créez des sauvegardes horaires, pensez à utiliser un préfixe de sauvegarde tel queYYYY/MM/DD/HH/<WorkloadName>/<files...>. Ce faisant, vous pouvez récupérer rapidement vos point-in-time sauvegardes manuellement ou par programmation.

Utilisation de la gestion des versions d'Amazon S3 pour conserver automatiquement l'historique des annulations

Vous pouvez activer le contrôle de version des objets S3 pour conserver un historique des modifications apportées aux objets, y compris la possibilité de revenir à une version précédente. Cela est utile pour les fichiers de configuration et autres objets susceptibles de changer plus fréquemment

que votre planning de point-in-time sauvegarde. C'est également utile pour les fichiers qui doivent être restaurés individuellement.

Utilisation d'Amazon S3 pour sauvegarder et récupérer des fichiers de configuration personnalisés pour les AMI

Amazon S3 avec gestion des versions d'objets peut devenir votre système d'enregistrement pour la configuration de votre charge de travail et vos fichiers d'options. Par exemple, vous pouvez utiliser une image AWS Marketplace Amazon EC2 standard gérée par un éditeur de logiciels indépendants. Cette image peut contenir un logiciel dont la configuration est conservée dans un certain nombre de fichiers de configuration. Vous pouvez gérer vos fichiers de configuration personnalisés dans Amazon S3. Lorsque votre instance est lancée, vous pouvez copier ces fichiers de configuration dans le cadre des données utilisateur de l'instance. Lorsque vous appliquez cette approche, vous n'avez pas besoin de personnaliser et de recréer une AMI pour utiliser une version mise à jour.

Utilisation d'Amazon S3 dans votre processus de sauvegarde et de restauration personnalisé

Amazon S3 fournit un magasin de sauvegarde polyvalent que vous pouvez intégrer rapidement à vos processus de sauvegarde personnalisés existants. Vous pouvez utiliser les AWS CLI AWS SDK et les opérations d'API pour intégrer vos scripts et processus de sauvegarde et de restauration qui utilisent Amazon S3. Par exemple, vous pouvez avoir un script de sauvegarde de base de données qui effectue des exportations de base de données tous les soirs. Vous pouvez personnaliser ce script pour copier vos sauvegardes nocturnes sur Amazon S3 pour un stockage hors site. Consultez le didacticiel sur le téléchargement par lots de fichiers dans le cloud pour obtenir un aperçu de la procédure à suivre.

Vous pouvez adopter une approche similaire pour exporter et sauvegarder les données de différentes applications en fonction de leur RPO individuel. En outre, vous pouvez utiliser AWS Systems Manager pour exécuter vos scripts de sauvegarde sur vos instances gérées. Systems Manager assure l'automatisation, le contrôle d'accès, la planification, la journalisation et les notifications pour vos processus de sauvegarde individuels.

Amazon S3 Glacier

Amazon S3 Glacier est un service de stockage d'archives dans le cloud à faible coût qui fournit un stockage sécurisé et durable pour l'archivage des données et la sauvegarde en ligne. Pour réduire les coûts, S3 Glacier propose trois classes de stockage allant de quelques millisecondes à

quelques heures. S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive proposent des options supplémentaires en fonction de la rapidité avec laquelle vous devez restaurer les données. Avec S3 Glacier, vous pouvez stocker de manière fiable de grandes ou de petites quantités de données en réalisant des économies considérables par rapport aux solutions sur site. S3 Glacier convient parfaitement au stockage de données de sauvegarde soumises à des exigences de conservation longues ou indéfinies et à l'archivage des données à long terme. S3 Glacier fournit les classes de stockage suivantes :

- S3 Glacier Instant Retrieval pour archiver les données qui peuvent être nécessaires une fois par trimestre et qui doivent être restaurées rapidement (en millisecondes)
- S3 Glacier Flexible Retrieval pour archiver les données qui peuvent avoir rarement besoin d'être restaurées, une ou deux fois par an, en quelques heures
- S3 Glacier Deep Archive pour archiver les données du cycle de sauvegarde à long terme qui peuvent rarement avoir besoin d'être restaurées dans les 12 heures

Le tableau suivant récapitule les options de récupération d'archive.

Classe de stockage	Accéléré	Standard	Volume
S3 Glacier Instant Retrieval	Ne s’applique pas	Ne s’applique pas	Ne s’applique pas
S3 Glacier Flexible Retr	1 à 5 minutes	3 à 5 heures	5 à 12 heures
S3 Glacier Deep Archive	Non disponible	Dans les 12 heures	Dans les 48 heures

À l'aide d'Amazon S3, vous pouvez définir la classe de stockage pour chaque objet de votre compartiment S3 lorsque vous le créez. Une fois l'objet créé, vous pouvez modifier la classe de stockage en copiant l'objet vers un nouvel objet avec une autre classe de stockage. Vous pouvez également activer une configuration du cycle de vie qui modifiera automatiquement la classe de stockage des objets en fonction des règles que vous spécifiez.

Pour automatiser vos processus de sauvegarde et de restauration, vous pouvez accéder à Amazon S3 Glacier et S3 Glacier Deep Archive via les AWS Management Console kits de AWS développement logiciel (SDK) et (SDK). AWS CLI Pour plus d'informations, consultez Amazon S3 Glacier.

> **Note**
>
> Les classes de stockage S3 Glacier sont soumises à des frais de durée minimale. Pour plus de détails, consultez la tarification d'Amazon S3 et utilisez la fonction de recherche sur la page Web pour trouver`duration`.

Utilisation de la transition d'objets Amazon S3 Lifecycle vers Amazon S3 Glacier par rapport à la gestion des archives Amazon S3 Glacier

Amazon S3 permet une transition pratique des objets S3 vers les classes de stockage Amazon S3 Glacier, afin que vous puissiez gérer le cycle de vie et les coûts de vos sauvegardes. Toutefois, en fonction de la taille des objets et de la nécessité ou non de restaurer une collection d'objets pour différents composants de votre architecture, vous souhaiterez peut-être gérer ce processus vous-même.

Si vous avez un grand nombre de petits objets qui doivent être restaurés collectivement, considérez les implications financières des options suivantes :

- Utilisation d'une politique de cycle de vie pour transférer automatiquement les objets individuellement vers Amazon S3 Glacier
- Compresser des objets dans un seul fichier et les stocker dans Amazon S3 Glacier

Amazon S3 Glacier impose des frais de capacité minimaux pour chaque objet en fonction de la classe de stockage que vous utilisez. Par exemple, S3 Glacier Instant Retrieval a une charge de capacité minimale de 128 Ko pour chaque objet. Consultez le tableau des performances pour obtenir le plus up-to-date d'informations.

Pour chaque objet que vous archivez dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, Amazon S3 utilise 8 Ko de stockage pour le nom de l'objet et les autres métadonnées. Amazon S3 stocke ces métadonnées pour que vous puissiez obtenir une liste en temps réel de vos objets archivés à l'aide de l'API Amazon S3. Le tarif S3 Standard vous est facturé pour ce stockage supplémentaire.

Amazon S3 ajoute également 32 Ko de stockage pour l'index et les métadonnées associées pour chaque objet archivé dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Ces données supplémentaires sont nécessaires pour identifier et restaurer l'objet. Les tarifs Amazon S3 Glacier ou S3 Glacier Deep Archive vous sont facturés pour ce stockage supplémentaire.

En compressant vos objets dans un seul fichier, vous pouvez réduire le stockage supplémentaire utilisé par Amazon S3 Glacier et éviter des frais de capacité minimaux pour de nombreux petits objets.

Une autre considération importante est que les politiques de cycle de vie sont appliquées aux objets individuellement. Cela peut avoir un impact sur l'intégrité de votre sauvegarde si un ensemble d'objets doit être restauré collectivement à partir d'un moment précis. Rien ne garantit que tous les objets seront transférés en même temps, même si les délais d'expiration et de transition du cycle de vie sont les mêmes pour tous les objets. Il peut y avoir un délai entre le moment où la règle du cycle de vie est satisfaite et le moment où l'action correspondant à la règle est terminée. Pour plus d'informations, consultez le centre de connaissances AWS.

Enfin, considérez l'effort de restauration entre l'utilisation des archives issues des politiques de cycle de vie et la gestion d'une archive distincte que vous créez. Vous devez lancer une restauration pour chaque objet à partir d'Amazon S3 Glacier séparément. Cela nécessite que vous écriviez un script ou que vous utilisiez un outil afin de lancer une restauration collective pour de nombreux objets. Vous pouvez utiliser S3 Batch Operations pour réduire le nombre de demandes individuelles, ou vous pouvez utiliser la console Amazon S3.

Sécurisation des données de sauvegarde dans Amazon S3 et Amazon S3 Glacier

La sécurité des données est une préoccupation universelle qui AWS prend la sécurité très au sérieux. La sécurité est la base de tout AWS service. Les services de stockage tels qu'Amazon S3 fournissent de puissantes fonctionnalités de contrôle d'accès et de chiffrement au repos et en transit. Tous les points de terminaison d'API Amazon S3 et Amazon S3 Glacier prennent en charge le protocole Secure Sockets Layer/Transport Layer Security (SSL/TLS) pour chiffrer les données en transit. Amazon S3 Glacier chiffre toutes les données au repos par défaut. Avec Amazon S3, vous pouvez choisir le chiffrement côté serveur pour les objets au repos en procédant comme suit :

- Utilisation du chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3
- Utilisation du chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) stockées dans AWS KMS

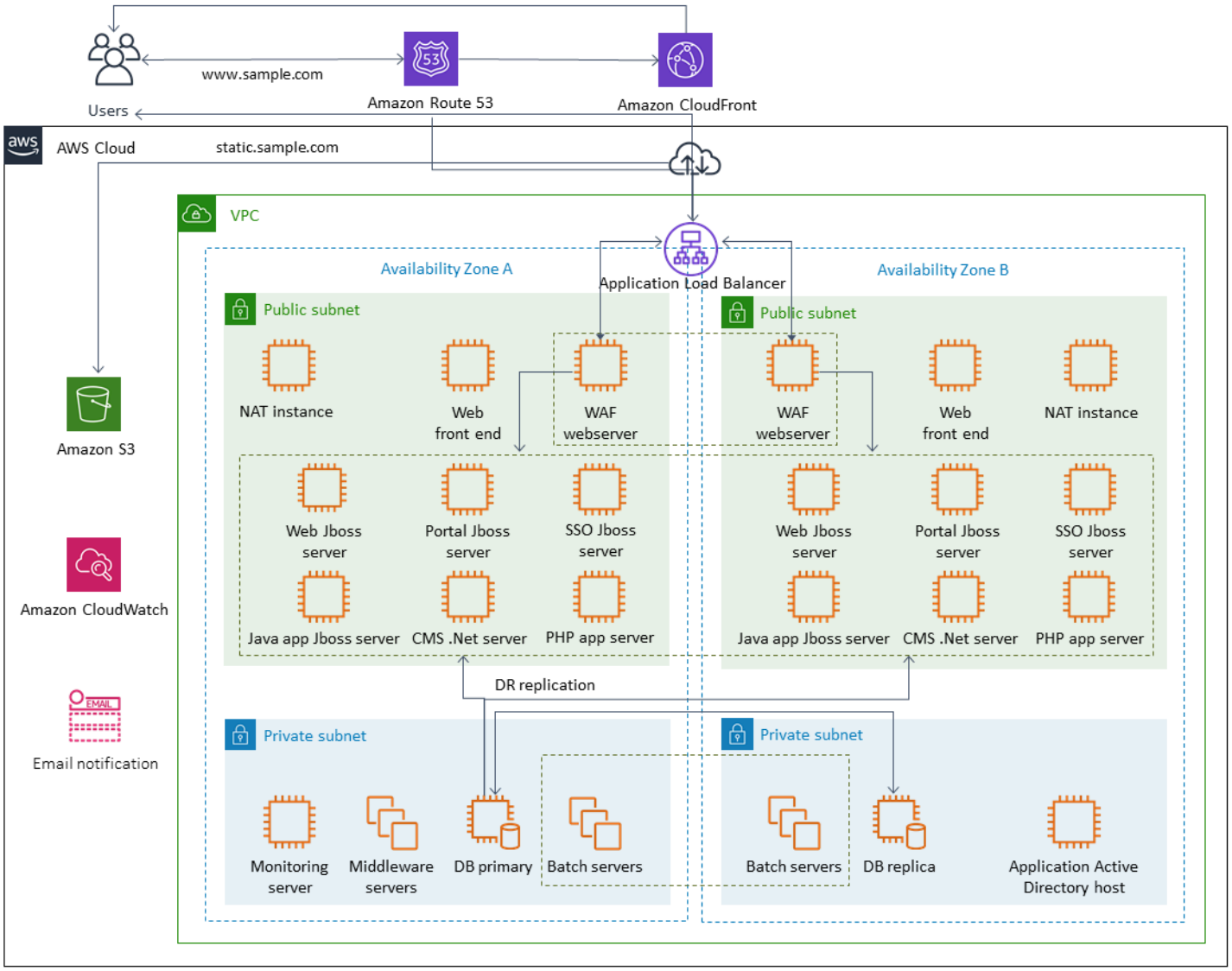
Vous pouvez également chiffrer vos données avant de les télécharger sur. AWS Pour plus d'informations, consultez la documentation sur le chiffrement côté client.

Vous pouvez utiliser AWS Identity and Access Management (IAM) pour contrôler l'accès aux objets S3. IAM permet de contrôler les autorisations pour des objets individuels et des chemins de préfixes spécifiques au sein d'un compartiment S3. Vous pouvez auditer l'accès aux objets S3 en utilisant la journalisation au niveau de l'objet avec AWS CloudTrail.

Backup et restauration pour Amazon EC2 avec des volumes EBS

AWS propose plusieurs méthodes pour sauvegarder vos instances Amazon EC2. Cette section couvre différents aspects de la sauvegarde des volumes Amazon Elastic Block Store (Amazon EBS) ou des volumes de stockage d'instance à des fins de stockage. AWS Backup Considérez-le comme votre premier choix pour gérer les sauvegardes AWS s'il répond à vos exigences. N'oubliez pas que les sauvegardes ne sont valables que si elles peuvent être restaurées à la fonction pour laquelle elles étaient destinées. La fonction de restauration et de restauration doit être régulièrement testée pour le confirmer.

L'architecture de la solution présentée dans le schéma suivant décrit un environnement de charge de travail qui repose entièrement sur AWS la majeure partie de l'architecture basée sur Amazon EC2. Comme le montre la figure suivante, le scénario inclut les serveurs Web, les serveurs d'applications, les serveurs de surveillance, les bases de données et Active Directory.



AWS fournit de nombreux services complets à de nombreux serveurs Amazon EC2 représentés dans cette architecture afin d'effectuer le travail indifférencié de création, de provisionnement, de sauvegarde, de restauration et d'optimisation des instances et du stockage. Déterminez si ces services ont du sens dans votre architecture afin de réduire la complexité et la gestion. AWS fournit également des services pour améliorer la disponibilité de vos architectures basées sur Amazon EC2. Pensez notamment à Amazon EC2 Auto Scaling et Elastic Load Balancing pour compléter vos charges de travail sur Amazon EC2. L'utilisation de ces services peut améliorer la disponibilité et la tolérance aux pannes de votre architecture et vous aider à restaurer les instances défectueuses avec un impact minimal sur les utilisateurs.

Les instances EC2 utilisent principalement les volumes Amazon EBS pour le stockage persistant. Amazon EBS fournit un certain nombre de fonctionnalités de sauvegarde et de restauration qui sont abordées en détail dans cette section.

Rubriques

Sauvegarde et restauration Amazon EC2 avec snapshots et AMI

Déterminez si vous devez créer une sauvegarde complète d'une instance EC2 avec une Amazon Machine Image (AMI) ou prendre un instantané d'un volume individuel.

Utilisation d'AMI ou de snapshots Amazon EBS pour les sauvegardes

Une AMI comprend les éléments suivants :

- Un ou plusieurs instantanés. Les nstance-store-backed AMI I incluent un modèle pour le volume racine de l'instance (par exemple, un système d'exploitation, un serveur d'applications et des applications).
- Autorisations de lancement qui contrôlent AWS les comptes autorisés à utiliser l'AMI pour lancer des instances.
- Un mappage de périphériques en mode bloc qui spécifie les volumes à associer à l'instance lors de son lancement.

Vous pouvez utiliser les AMI pour lancer de nouvelles instances avec des logiciels et des données préconfigurés. Vous pouvez créer des AMI lorsque vous souhaitez établir une base de référence, qui est une configuration réutilisable pour lancer davantage d'instances. Lorsque vous créez une AMI d'une instance EC2 existante, un instantané est pris pour tous les volumes attachés à l'instance. L'instantané inclut les mappages des appareils.

Vous ne pouvez pas utiliser de snapshots pour lancer une nouvelle instance, mais vous pouvez les utiliser pour remplacer des volumes sur une instance existante. En cas de corruption de données ou de panne de volume, vous pouvez créer un volume à partir d'un instantané que vous avez pris et remplacer l'ancien volume. Vous pouvez également utiliser des instantanés pour approvisionner de nouveaux volumes et les associer lors du lancement d'une nouvelle instance.

Si vous utilisez des AMI de plateforme et d'application gérées et publiées par AWS ou depuis le AWS Marketplace, envisagez de conserver des volumes distincts pour vos données. Vous pouvez sauvegarder vos volumes de données sous forme de snapshots distincts des volumes du système d'exploitation et des applications. Utilisez ensuite les instantanés du volume de données avec les AMI récemment mises à jour publiées par AWS ou depuis le AWS Marketplace. Cette approche nécessite des tests et une planification minutieux pour sauvegarder et restaurer toutes les données personnalisées, y compris les informations de configuration, sur les AMI récemment publiées.

Le processus de restauration dépend de votre choix entre les sauvegardes AMI ou les sauvegardes instantanées. Si vous créez des AMI pour servir de sauvegarde d'instance, vous devez lancer une instance EC2 à partir de l'AMI dans le cadre de votre processus de restauration. Il se peut également que vous deviez arrêter l'instance existante pour éviter d'éventuelles collisions. Les identificateurs de sécurité (SID) pour les instances Windows jointes à un domaine constituent un exemple de collision potentielle. Le processus de restauration des instantanés peut vous obliger à détacher le volume existant et à joindre le volume récemment restauré. Il se peut également que vous deviez modifier la configuration pour faire pointer vos applications vers le volume que vous venez d'attacher.

AWS Backup prend en charge à la fois les sauvegardes au niveau de l'instance sous forme d'AMI et les sauvegardes au niveau du volume sous forme de snapshots distincts :

- Pour une sauvegarde complète de tous les volumes EBS de l'instance, créez une AMI de l'instance EC2 exécutée sous Linux ou Windows. Lorsque vous souhaitez revenir en arrière, utilisez l'assistant de lancement d'instance pour créer une instance. Dans l'assistant de lancement d'instance, sélectionnez Mes AMI.
- Pour sauvegarder un volume individuel, créez un instantané. Pour restaurer le cliché, voir Création d'un volume à partir d'un instantané. Vous pouvez utiliser le AWS Management Console ou le AWS Command Line Interface (AWS CLI).

Le coût d'une AMI d'instance correspond au stockage de tous les volumes de l'instance, mais pas aux métadonnées. Le coût d'un instantané EBS correspond au stockage du volume individuel. Pour plus d'informations sur les coûts de stockage en volume, consultez la page de tarification d'Amazon EBS.

Volumes du serveur

Les volumes EBS constituent la principale option de stockage persistant pour Amazon EC2. Vous pouvez utiliser ce stockage par blocs pour les données structurées, telles que les bases de données, ou les données non structurées, telles que les fichiers d'un système de fichiers sur un volume.

Les volumes EBS sont placés dans une zone de disponibilité spécifique. Les volumes sont répliqués sur plusieurs serveurs afin d'éviter la perte de données due à la défaillance d'un seul composant. Une panne fait référence à une perte totale ou partielle du volume, selon la taille et les performances du volume.

Les volumes EBS sont conçus pour un taux de défaillance annuel (AFR) de 0,1 à 0,2 %. Cela rend les volumes EBS 20 fois plus fiables que les disques classiques, qui tombent en panne avec un AFR d'environ 4 %. Par exemple, si vous avez 1 000 volumes EBS en cours d'exécution pendant un an, vous devez vous attendre à ce qu'un ou deux volumes soient défaillants.

Amazon EBS prend également en charge une fonctionnalité de capture instantanée pour point-in-time effectuer des sauvegardes de vos données. Tous les types de volumes EBS offrent des fonctionnalités de capture instantanée durables et sont conçus pour une disponibilité de 99,999 %. Pour plus d'informations, consultez l'accord de niveau de service Amazon Compute.

Amazon EBS permet de créer des instantanés (sauvegardes) de n'importe quel volume EBS. Un instantané est une fonctionnalité de base pour créer des sauvegardes de vos volumes EBS. Un instantané prend une copie du volume EBS et le place dans Amazon S3, où il est stocké de manière redondante dans plusieurs zones de disponibilité. L'instantané initial est une copie complète du volume ; les instantanés en cours stockent uniquement les modifications incrémentielles au niveau des blocs. Consultez la documentation Amazon EC2 pour savoir comment créer des instantanés Amazon EBS.

Vous pouvez effectuer une opération de restauration, supprimer un instantané ou mettre à jour les métadonnées du cliché, telles que les balises, associées à l'instantané depuis la console Amazon EC2 dans la même région que celle dans laquelle vous avez pris le cliché.

La restauration d'un instantané crée un nouveau volume Amazon EBS contenant l'intégralité des données du volume. Si vous n'avez besoin que d'une restauration partielle, vous pouvez associer le volume à l'instance en cours d'exécution sous un autre nom de périphérique. Montez-le ensuite et utilisez les commandes de copie du système d'exploitation pour copier les données du volume de sauvegarde vers le volume de production.

Les instantanés Amazon EBS peuvent également être copiés entre les AWS régions à l'aide de la fonctionnalité de copie d'instantanés Amazon EBS, comme décrit dans la documentation Amazon EC2. Vous pouvez utiliser cette fonctionnalité pour stocker votre sauvegarde dans une autre région sans avoir à gérer la technologie de réplication sous-jacente.

Création de volumes de serveurs distincts

Vous utilisez peut-être déjà un ensemble standard de volumes distincts pour le système d'exploitation, les journaux, les applications et les données. En établissant des volumes de serveur distincts, vous pouvez réduire l'impact des défaillances d'applications ou de plateformes dues à l'épuisement de l'espace disque. Ce risque est généralement plus élevé avec les disques durs physiques, car vous ne disposez pas de la flexibilité nécessaire pour augmenter rapidement les volumes. Dans le cas des disques physiques, vous devez acheter les nouveaux disques, sauvegarder les données, puis restaurer les données sur les nouveaux disques. Ce risque est ainsi considérablement réduit AWS, car vous pouvez utiliser Amazon EBS pour étendre vos volumes provisionnés. Pour en savoir plus, consultez la documentation AWS.

Gérez des volumes distincts pour les données d'application, les données utilisateur, les journaux et les fichiers d'échange afin de pouvoir utiliser des politiques de sauvegarde et de restauration distinctes pour ces ressources. En séparant les volumes de vos données, vous pouvez également utiliser différents types de volumes en fonction des exigences de performance et de stockage des données. Vous pouvez ensuite optimiser et ajuster vos coûts en fonction des différentes charges de travail.

Considérations relatives aux volumes de stockage, par exemple

Un stockage d’instances fournit un stockage temporaire de niveau bloc pour votre instance. Le stockage réside sur les disques physiquement attachés à l’ordinateur hôte. Les magasins d'instances sont idéaux pour le stockage temporaire d'informations fréquemment modifiées, telles que les tampons, les caches, les données temporaires et autres contenus temporaires. Ils sont également préférables pour les données répliquées sur un parc d'instances, tel qu'un pool de serveurs Web à charge équilibrée.

Les données d'un stockage d'instances ne persistent que pendant la durée de vie de son instance associée. Si une instance redémarre (intentionnellement ou accidentellement), les données du stockage d'instances persistent. Toutefois, les données du magasin d'instances sont perdues dans l'une des circonstances suivantes.

- Le lecteur sous-jacent tombe en panne.
- L'instance s'arrête.
- L'instance est résiliée.

Par conséquent, ne vous fiez pas à un magasin d'instances pour obtenir des données précieuses à long terme. Utilisez plutôt un stockage de données plus durable comme Amazon S3, Amazon EBS ou Amazon EFS.

Une stratégie courante pour les volumes de stockage d'instance consiste à conserver régulièrement les données nécessaires sur Amazon S3 selon les besoins, en fonction de l'objectif de point de restauration (RPO) et de l'objectif de temps de restauration (RTO). Vous pouvez ensuite télécharger les données depuis Amazon S3 vers votre magasin d'instances lorsqu'une nouvelle instance est lancée. Vous pouvez également télécharger les données sur Amazon S3 avant qu'une instance ne soit arrêtée. Pour des raisons de persistance, créez un volume EBS, attachez-le à votre instance et copiez régulièrement les données du volume de stockage d'instance vers le volume EBS. Pour plus d'informations, consultez le centre de connaissances AWS.

Marquage et application des normes pour les instantanés EBS et les AMI

Le balisage de toutes vos AWS ressources est une pratique importante pour la répartition des coûts, l'audit, le dépannage et les notifications. Le balisage est important pour les volumes EBS afin que les informations pertinentes nécessaires à la gestion et à la restauration des volumes soient présentes. Les balises ne sont pas automatiquement copiées des instances EC2 vers les AMI ou des volumes source vers les instantanés. Assurez-vous que votre processus de sauvegarde inclut les balises pertinentes provenant de ces sources. Cela vous permet de définir les métadonnées des instantanés, telles que les politiques d'accès, les informations relatives aux pièces jointes et la répartition des coûts, afin d'utiliser ces sauvegardes à l'avenir. Pour plus d'informations sur le balisage de vos AWS ressources, consultez le paper technique sur les meilleures pratiques en matière de balisage.

Outre les balises que vous utilisez pour toutes les AWS ressources, utilisez les balises spécifiques à la sauvegarde suivantes :

- ID de l'instance source
- ID du volume source (pour les instantanés)
- Description du point de récupération

Vous pouvez appliquer des politiques de balisage à l'aide de AWS Config règles et d'autorisations IAM. IAM prend en charge l'utilisation forcée des balises. Vous pouvez donc rédiger des politiques IAM qui imposent l'utilisation de balises spécifiques lorsque vous agissez sur des instantanés Amazon EBS. Si une `CreateSnapshot` opération est tentée sans que les balises définies dans la politique d'autorisation IAM n'accordent des droits, la création du snapshot échoue et l'accès est

refusé. Pour plus d'informations, consultez le billet de blog sur le balisage des instantanés Amazon EBS lors de la création et de la mise en œuvre de politiques de sécurité plus strictes.

Vous pouvez utiliser AWS Config des règles pour évaluer automatiquement les paramètres de configuration de vos AWS ressources. Pour vous aider à démarrer, AWS Config fournit des règles prédéfinies personnalisables appelées règles gérées. Vous pouvez également créer vos propres règles personnalisées. Tout AWS Config en suivant en permanence les modifications de configuration de vos ressources, il vérifie si ces modifications enfreignent l'une des conditions de vos règles. Si une ressource enfreint une règle, AWS Config marque la ressource et la règle comme non conformes. Notez que la règle de gestion des balises requises ne prend actuellement pas en charge les instantanés et les AMI.

Création de sauvegardes de volumes EBS avec des AMI et des instantanés EBS

AWS fournit une multitude d'options pour créer et gérer des AMI et des instantanés. Vous pouvez utiliser l'approche qui répond à vos besoins. Un problème courant auquel de nombreux clients sont confrontés est la gestion du cycle de vie des instantanés et l'alignement clair des instantanés par objectif, politique de conservation, etc. Sans balisage approprié, les instantanés risquent d'être supprimés accidentellement ou dans le cadre d'un processus de nettoyage automatique. Vous pourriez également finir par payer pour des instantanés obsolètes qui sont conservés parce qu'il n'est pas clair s'ils sont toujours nécessaires.

Préparation d'un volume EBS avant de créer un instantané ou une AMI

Avant de prendre un instantané ou de créer une AMI, effectuez les préparatifs nécessaires pour votre volume EBS. La création d'une AMI génère un nouvel instantané pour chaque volume EBS attaché à l'instance. Ces préparations s'appliquent donc également aux AMI.

Vous pouvez prendre un instantané d'un volume EBS attaché qui est utilisé par une instance EC2 sous tension. Toutefois, les instantanés capturent uniquement les données qui ont été écrites sur votre volume EBS au moment où la commande de capture instantanée est émise. Cela peut exclure toutes les données mises en cache par les applications ou le système d'exploitation. La meilleure pratique consiste à placer le système dans un état où il n'effectue aucune E/S. Idéalement, la machine n'accepte pas le trafic et est à l'arrêt, mais cela est rare car les opérations informatiques 24 heures sur 24, 7 jours sur 7 deviennent la norme. Si vous pouvez transférer des données de la mémoire système sur le disque utilisé par vos applications et suspendre toute écriture de fichier sur le volume suffisamment longtemps pour prendre un instantané, celui-ci devrait être complet.

Pour effectuer une sauvegarde saine, vous devez suspendre la base de données ou le système de fichiers. La manière de procéder dépend de votre base de données ou de votre système de fichiers.

Le processus d'une base de données est le suivant :

1. Si possible, mettez la base de données en mode de sauvegarde à chaud.
2. Exécutez les commandes de capture instantanée Amazon EBS.
3. Sortez la base de données du mode de sauvegarde à chaud ou, si vous utilisez une réplique en lecture, mettez fin à l'instance de réplique en lecture.

Le processus d'un système de fichiers est similaire, mais il dépend des capacités du système d'exploitation ou du système de fichiers. Par exemple, XFS est un système de fichiers capable de vider ses données pour une sauvegarde cohérente. Pour plus d'informations, consultez xfs_freeze. Vous pouvez également faciliter ce processus en utilisant un gestionnaire de volumes logiques qui prend en charge le gel des E/S.

Toutefois, si vous ne parvenez pas à vider ou à suspendre toutes les écritures de fichiers sur le volume, procédez comme suit :

1. Démontez le volume du système d'exploitation.
2. Émettez la commande snapshot.
3. Remontez le volume pour obtenir un instantané cohérent et complet. Vous pouvez remonter et utiliser votre volume tant que l'état du snapshot est en attente.

Le processus de capture d'écran se poursuit en arrière-plan et la création d'instantanés est rapide et permet de capturer un moment précis. Les volumes que vous sauvegardez ne sont démontés que quelques secondes. Vous pouvez planifier une petite fenêtre de sauvegarde au cours de laquelle une panne est attendue et gérée par les clients avec élégance.

Lorsque vous créez un instantané pour un volume EBS qui sert de périphérique racine, arrêtez l'instance avant de prendre le cliché. Windows fournit le service Volume Shadow Copy (VSS) pour aider à créer des instantanés cohérents avec les applications. AWS fournit un document Systems Manager que vous pouvez exécuter pour effectuer des sauvegardes au niveau de l'image d'applications compatibles VSS. Les instantanés incluent des données de transactions en attente entre ces applications et le disque. Il n'est pas nécessaire d'arrêter vos instances ou de les déconnecter lorsque vous sauvegardez tous les volumes attachés. Pour en savoir plus, consultez la documentation AWS.

> **Note**
>
> Si vous créez une AMI Windows afin de déployer une autre instance similaire, utilisez EC2Config ou EC2Launch pour Sysprep votre instance. Créez ensuite une AMI à partir de l'instance arrêtée. Sysprep supprime les informations uniques de l'instance Windows Amazon EC2, notamment les SID, le nom de l'ordinateur et les pilotes. Les SID dupliqués peuvent entraîner des problèmes avec Active Directory, Windows Server Update Services (WSUS), des problèmes de connexion, l'activation des clés de volume Windows, Microsoft Office et les produits tiers. N'utilisez pas Sysprep avec votre instance si votre AMI est destinée à des fins de sauvegarde et si vous souhaitez restaurer la même instance avec toutes ses informations uniques intactes.

Création manuelle d'instantanés de volumes EBS à partir de la console

Créez des instantanés des volumes appropriés ou de l'instance complète avant d'apporter des modifications majeures qui n'ont pas été entièrement testées sur l'instance. Par exemple, vous souhaiterez peut-être créer un instantané avant de mettre à niveau ou d'appliquer un correctif à l'application ou au logiciel système de votre instance.

Vous pouvez créer un instantané manuellement à partir de la console. Sur la console Amazon EC2, sur la page Elastic Block Store Volumes, sélectionnez le volume que vous souhaitez sauvegarder. Ensuite, dans le menu Actions, choisissez Create Snapshot. Vous pouvez rechercher des volumes attachés à une instance spécifique en saisissant l'ID de l'instance dans le champ de filtre.

Entrez une description et ajoutez les balises appropriées. Ajoutez une `Name` balise pour retrouver plus facilement le volume ultérieurement. Ajoutez toute autre balise appropriée en fonction de votre stratégie de balisage.

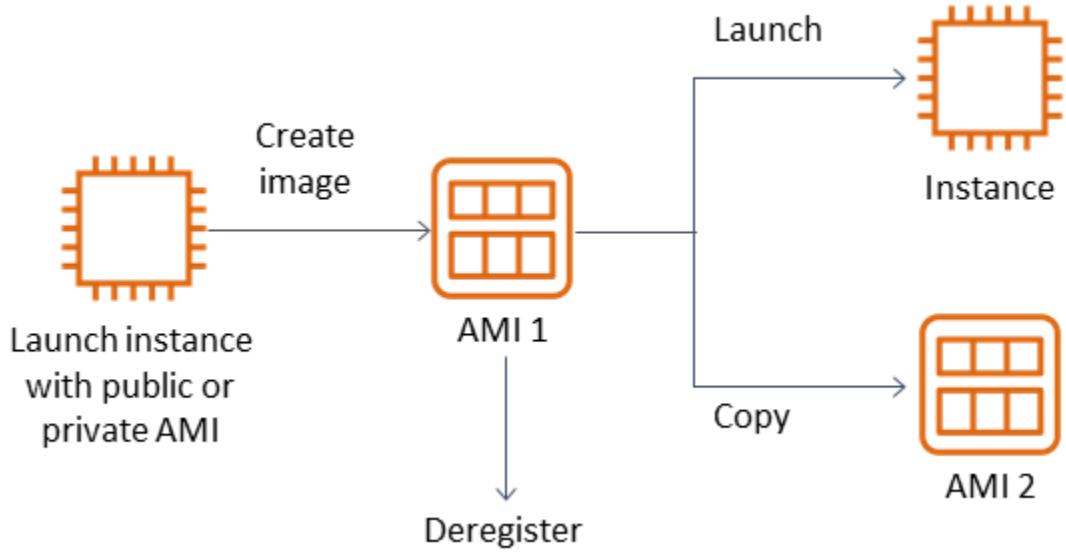
Création d'AMI

Une AMI fournit les informations nécessaires au lancement d'une instance. L'AMI inclut le volume racine et les instantanés des volumes EBS attachés à l'instance lors de la création de l'image. Vous ne pouvez pas lancer de nouvelles instances uniquement à partir de snapshots EBS ; vous devez lancer de nouvelles instances à partir d'une AMI.

Lorsque vous créez une AMI, elle est créée dans le compte et dans la région que vous utilisez. Le processus de création de l'AMI crée des instantanés Amazon EBS pour chaque volume attaché à

l'instance, et l'AMI fait référence à ces instantanés Amazon EBS. Ces instantanés se trouvent dans Amazon S3 et sont très durables.

Après avoir créé une AMI de votre instance EC2, vous pouvez utiliser l'AMI pour recréer l'instance ou lancer d'autres copies de l'instance. Vous pouvez également copier des AMI d'une région à une autre pour la migration d'applications ou la DR.



Une AMI doit être créée à partir d'une instance EC2, sauf si vous migrez une machine virtuelle, telle qu'une machine virtuelle VMWARE, vers. AWS Pour créer une AMI à partir de la console Amazon EC2, sélectionnez l'instance, choisissez Actions, choisissez Image, puis choisissez Create Image.

Amazon Data Lifecycle Manager

Pour automatiser la création, la conservation et la suppression des instantanés Amazon EBS, vous pouvez utiliser Amazon Data Lifecycle Manager. L'automatisation de la gestion des snapshots vous permet d'effectuer les opérations suivantes :

- protéger les données importantes en appliquant un planning de sauvegarde régulière ;
- conserver des sauvegardes comme exigé par les auditeurs ou les réglementations internes ;
- réduire les frais de stockage en supprimant les sauvegardes périmées.

À l'aide d'Amazon Data Lifecycle Manager, vous pouvez automatiser le processus de gestion des snapshots pour les instances EC2 (et leurs volumes EBS associés) ou pour les volumes EBS distincts. Il prend en charge des options telles que la copie entre régions, afin que vous puissiez copier des instantanés automatiquement vers d'autres AWS régions. La copie d'instantanés vers

d'autres régions est une approche permettant de soutenir les efforts de reprise après sinistre et de restaurer les options dans une autre région. Vous pouvez également utiliser Amazon Data Lifecycle Manager pour créer une politique de cycle de vie des instantanés prenant en charge la restauration rapide des instantanés.

Amazon Data Lifecycle Manager est une fonctionnalité incluse dans Amazon EC2 et Amazon EBS. Amazon Data Lifecycle Manager est gratuit.

AWS Backup

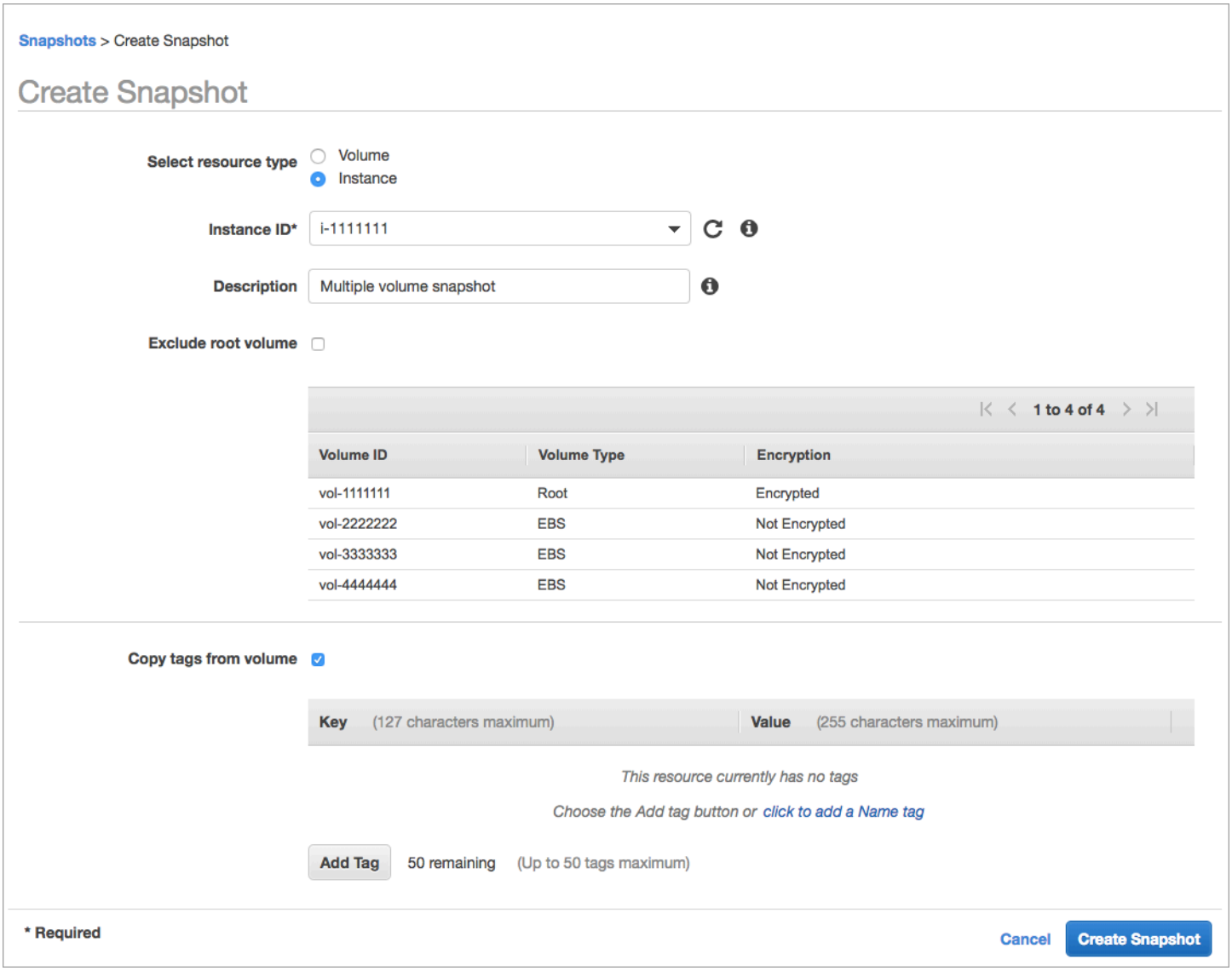
AWS Backup est unique par rapport à Amazon Data Lifecycle Manager, car vous pouvez créer un plan de sauvegarde qui inclut les ressources de plusieurs AWS services. Vous pouvez coordonner votre sauvegarde pour couvrir les ressources que vous utilisez ensemble plutôt que de coordonner les sauvegardes des ressources individuellement.

AWS Backup inclut également le concept de coffres-forts de sauvegarde, qui peut restreindre l'accès aux points de restauration pour vos sauvegardes terminées. Les opérations de restauration peuvent être lancées à partir de chaque ressource individuelle au AWS Backup lieu de procéder à la restauration de la sauvegarde créée. AWS Backup inclut également une multitude de fonctionnalités supplémentaires, telles que la gestion des audits et les rapports. Pour de plus amples informations, veuillez consulter la section Backup et restauration à l'aide deAWS Backup de ce guide.

Réalisation de sauvegardes sur plusieurs volumes

Si vous souhaitez sauvegarder les données des volumes EBS d'une matrice RAID à l'aide de snapshots, ceux-ci doivent être cohérents. La raison en est que les instantanés de ces volumes sont créés indépendamment. La restauration de volumes EBS dans une matrice RAID à partir de snapshots désynchronisés dégrade l'intégrité de la matrice.

Pour créer un ensemble cohérent d'instantanés pour votre matrice RAID, utilisez l'CreateSnapshotsAPI ou connectez-vous à la console Amazon EC2 et choisissez Elastic Block Store, Snapshots, Create Snapshot.



Les instantanés des instances auxquelles plusieurs volumes sont attachés dans une configuration RAID sont pris collectivement sous la forme d'un instantané multivolume. Les instantanés multivolumes fournissent des point-in-time instantanés coordonnés avec les données et cohérents en cas de crash sur plusieurs volumes EBS attachés à une instance EC2. Il n'est pas nécessaire d'arrêter votre instance pour coordonner les volumes afin d'assurer la cohérence, car les instantanés sont automatiquement pris sur plusieurs volumes EBS. Après le lancement de la capture instantanée des volumes (généralement une seconde ou deux), le système de fichiers peut poursuivre ses opérations.

Une fois les instantanés créés, chaque instantané est traité en tant qu'instantané individuel. Vous pouvez effectuer toutes les opérations de capture instantanée, telles que la restauration, la suppression et la copie entre régions et comptes, comme vous le feriez avec un instantané en

un seul volume. Vous pouvez également étiqueter vos instantanés en plusieurs volumes comme vous le feriez pour un instantané en un seul volume. Nous vous recommandons de baliser vos instantanés multivolumes afin de les gérer collectivement lors de la restauration, de la copie ou de la conservation. Pour plus d'informations, consultez la documentation AWS.

Vous pouvez également effectuer ces sauvegardes à partir d'un gestionnaire de volumes logiques ou d'une sauvegarde au niveau du système de fichiers. Dans ces cas, l'utilisation d'un agent de sauvegarde traditionnel permet de sauvegarder les données sur le réseau. Un certain nombre de solutions de sauvegarde basées sur des agents sont disponibles sur Internet et dans le. AWS Marketplace

Une autre approche consiste à créer une réplique des principaux volumes du système existant sur un seul grand volume. Cela simplifie le processus de sauvegarde, car un seul volume important doit être sauvegardé et la sauvegarde n'a pas lieu sur le système principal. Cependant, déterminez d'abord si le volume unique peut fonctionner suffisamment pendant la sauvegarde et si la taille maximale du volume convient à l'application.

Protection de vos sauvegardes Amazon EC2

Il est important de prendre en compte la sécurité de vos sauvegardes et d'empêcher leur suppression accidentelle ou malveillante. Vous pouvez utiliser un certain nombre d'approches collectivement pour y parvenir. Pour éviter la perte de vos sauvegardes critiques en raison d'une faille de sécurité, nous vous recommandons de copier vos sauvegardes sur un autre AWS compte. Si vous possédez plusieurs comptes AWS, vous pouvez désigner un compte distinct comme compte d'archivage sur lequel tous les autres comptes peuvent copier des sauvegardes. Par exemple, vous pouvez y parvenir avec une sauvegarde entre comptes dans AWS Backup.

Votre plan de reprise après sinistre peut également exiger que vous soyez en mesure de reproduire des instances EC2 dans une autre région AWS en cas de défaillance régionale. Vous pouvez atteindre cet objectif en copiant vos sauvegardes dans une autre région au sein du même compte. Cela peut fournir une couche supplémentaire de protection contre les suppressions accidentelles et soutenir les objectifs de reprise après sinistre (DR). AWS Backup prend en charge les sauvegardes interrégionales.

Envisagez de bloquer les autorisations IAM pour les actions ec2 : DeleteSnapshot et ec2 :. DeregisterImage Vous pouvez plutôt laisser vos politiques et méthodes de rétention gérer le cycle de vie des instantanés EBS et des AMI Amazon EC2. Le blocage des actions de suppression est un moyen de mettre en œuvre une stratégie WORM (écriture unique, lecture multiple) pour vos

instantanés EBS. Vous pouvez également utiliser AWS Backup Vault Lock, qui prend en charge les instantanés EBS et d'autres AWS ressources.

En outre, pensez à empêcher les utilisateurs de partager des AMI et des instantanés EBS en bloquant les actions ec2 : ModifyImageAttribute et ec2 : IAM. ModifySnapshotAttribute Cela empêchera le partage de vos AMI et de vos instantanés avec AWS des comptes externes à votre organisation. Si vous en utilisez AWS Backup, empêchez les utilisateurs d'effectuer des opérations similaires sur les coffres-forts de sauvegarde. Pour de plus amples informations, veuillez consulter la section AWS Backup de ce guide.

Amazon EC2 inclut une fonction de corbeille qui peut vous aider à restaurer des instantanés EBS supprimés accidentellement. Si vous autorisez vos utilisateurs à supprimer des instantanés, activez cette fonctionnalité afin que les instantanés nécessaires ne soient pas définitivement supprimés. Les utilisateurs doivent être particulièrement attentifs à la suppression de plusieurs instantanés, car la console Amazon EC2 permet de sélectionner plusieurs instantanés et de les supprimer en une seule opération. En outre, soyez prudent lorsque vous utilisez des scripts de nettoyage et d'automatisation afin de ne pas supprimer involontairement les instantanés dont vous avez besoin. La fonction Corbeille permet de se protéger contre ce type de situations.

Archivage des instantanés EBS

L'archivage de vos instantanés EBS peut être une méthode rentable pour conserver une copie d'un volume à des fins de référence que vous n'avez pas l'intention de restaurer pendant 90 jours ou plus. Cela peut constituer une bonne étape intermédiaire avant de supprimer définitivement tous les instantanés associés à un volume EBS. Par exemple, vous pouvez envisager d'archiver des instantanés comme une end-of-lifecycle étape pour les volumes EBS qui ne sont plus utilisés. L'archivage plutôt que la suppression peut également être une méthode plus rentable de conservation des données supprimées au lieu d'utiliser la corbeille.

Automatiser la création de snapshots et d'AMI à l'aide de Systems Manager AWS CLI, du SDK et des kits de développement logiciel AWS

Votre approche de sauvegarde peut nécessiter des opérations avant et après la création d'un snapshot ou d'une AMI. Par exemple, il se peut que vous deviez arrêter et démarrer des services pour mettre le système de fichiers en veille. Il se peut également que vous deviez arrêter et démarrer votre instance lors de la création de l'AMI. Il se peut également que vous deviez créer des sauvegardes de plusieurs composants de votre architecture collectivement, chacune comportant ses propres étapes de pré-création et de post-création.

Vous pouvez réduire les délais de maintenance de vos sauvegardes en automatisant votre processus et en vérifiant qu'il est appliqué de manière cohérente. Pour automatiser vos opérations personnalisées de pré-création et de post-création, scriptez votre processus de sauvegarde à l'aide du SDK AWS CLI et du SDK.

Votre automatisation peut être définie dans un runbook de Systems Manager qui peut être exécuté à la demande ou pendant une fenêtre de maintenance de Systems Manager. Vous pouvez autoriser vos utilisateurs à exécuter des runbooks de Systems Manager sans avoir à leur accorder l'autorisation d'accéder aux commandes perturbatrices d'Amazon EC2. Cela peut également vous aider à vérifier que votre processus de sauvegarde et vos balises sont appliqués de manière cohérente par vos utilisateurs. Vous pouvez utiliser les CreateImage runbooks AWS CreateSnapshot et AWS pour créer des instantanés et des AMI, ou vous pouvez autoriser d'autres utilisateurs à les utiliser. Systems Manager inclut également les UpdateWindowsAmi runbooks AWS UpdateLinuxAmi et AWS pour automatiser l'application de correctifs et la création d'AMI.

Vous pouvez également utiliser le AWS CLI et AWS Tools for Windows PowerShellpour automatiser votre processus de création de snapshots et d'AMI. Vous pouvez utiliser la AWS CLI commande aws ec2 create-snapshot pour créer un instantané d'un volume EBS dans le cadre de votre automatisation. Vous pouvez utiliser la commande aws ec2 create-snapshots pour créer des instantanés synchronisés et cohérents en cas de crash de tous les volumes attachés à votre instance EC2.

Vous pouvez utiliser la AWS CLI pour créer de nouvelles AMI. Vous pouvez utiliser la commande aws ec2 register-image pour créer une nouvelle image pour votre instance EC2. Pour automatiser l'arrêt, la création d'images et le redémarrage de vos instances, combinez cette commande avec les commandes aws ec2 stop-instances et aws ec2 start-instances.

Restauration d'un volume Amazon EBS ou d'une instance EC2

Si vous ne devez restaurer qu'un seul volume attaché à une instance EC2, vous pouvez restaurer ce volume séparément, détacher le volume existant et attacher le volume restauré à votre instance EC2. Si vous devez restaurer une instance EC2 complète, y compris tous ses volumes associés, vous devez utiliser une sauvegarde Amazon Machine Image (AMI) de votre instance.

Pour réduire le temps de restauration et l'impact sur les applications et processus dépendants, votre processus de restauration doit prendre en compte la ressource qu'il remplace. Pour de meilleurs résultats, testez régulièrement votre processus de restauration dans des environnements de faible capacité (par exemple, hors production) afin de vérifier qu'il répond à votre objectif de point de

restauration (RPO) et à votre objectif de temps de restauration (RTO) et que le processus de restauration fonctionne comme prévu. Réfléchissez à l'impact du processus de restauration sur les applications et les services qui dépendent de l'instance que vous restaurez, puis coordonnez la restauration si nécessaire. Essayez d'automatiser et de tester le processus de restauration autant que possible afin de réduire le risque d'échec ou de mise en œuvre incohérente du processus de restauration.

Si vous utilisez Elastic Load Balancing, avec plusieurs instances gérant le trafic, vous pouvez mettre hors service une instance défaillante ou défectueuse. Vous pouvez ensuite restaurer une nouvelle instance pour la remplacer tandis que les autres instances continuent de traiter le trafic sans perturber les utilisateurs.

Les processus de restauration décrits ci-dessous concernent des instances qui n'utilisent pas Elastic Load Balancing :

- Restauration de fichiers et de répertoires individuels à partir de snapshots EBS
- Restauration d'un volume EBS à partir d'un instantané Amazon EBS
- Création ou restauration d'une instance EC2 à partir d'un instantané EBS
- Restauration d'une instance en cours d'exécution à partir d'une AMI

Restauration de fichiers et de répertoires à partir de snapshots EBS

Les instantanés EBS fournissent une réplique point-in-time exacte du volume d'origine utilisé pour créer l'instantané. Pour restaurer des fichiers ou des répertoires individuels, vous devez effectuer les opérations suivantes :

1. Restaurez d'abord le volume à partir de l'instantané EBS qui contient les fichiers ou les répertoires.
2. Attachez le volume à l'instance EC2 sur laquelle vous souhaitez restaurer les fichiers.
3. Copiez les fichiers du volume restauré vers votre volume d'instance EC2.
4. Détachez et supprimez le volume restauré.

Restauration d'un volume EBS à partir d'un instantané Amazon EBS

Vous pouvez restaurer un volume attaché à une instance EC2 existante en créant un volume à partir de son instantané et en l'attachant à votre instance. Vous pouvez utiliser les opérations de console

AWS CLI, de ou d'API pour créer un volume à partir d'un instantané existant. Vous pouvez ensuite monter le volume sur l'instance à l'aide du système d'exploitation.

Notez que les données d'un instantané Amazon EBS sont chargées de manière asynchrone dans un volume EBS. Si une application accède au volume sur lequel les données ne sont pas chargées, la latence est supérieure à la normale lorsque les données sont chargées depuis Amazon S3. Pour éviter cet impact sur les applications sensibles à la latence, deux options s'offrent à vous :

- Vous pouvez initialiser le volume EBS.
- Moyennant des frais supplémentaires, Amazon EBS prend en charge la restauration rapide des instantanés, ce qui évite d'avoir à initialiser votre volume.

Si vous remplacez un volume qui doit utiliser le même point de montage, démontez ce volume afin de pouvoir monter le nouveau volume à sa place. Pour démonter le volume, arrêtez d'abord tous les processus qui l'utilisent. Si vous remplacez le volume racine, vous devez d'abord arrêter l'instance avant de pouvoir le détacher.

Par exemple, procédez comme suit pour restaurer un volume à partir d'une point-in-time sauvegarde antérieure à l'aide de la console :

1. Sur la console Amazon EC2, dans le menu Elastic Block Store, choisissez Snapshots.
2. Recherchez l'instantané que vous souhaitez restaurer, puis sélectionnez-le.
3. Choisissez Actions, puis Create Volume.
4. Créez le nouveau volume dans la même zone de disponibilité que votre instance EC2.
5. Sur la console Amazon EC2, sélectionnez l'instance.
6. Dans les détails de l'instance, notez le nom de l'appareil que vous souhaitez remplacer dans les entrées Root device ou Block Devices.
7. Fixez le volume. Le processus est différent pour les volumes racine et pour les volumes non racines.

   Pour les volumes racine :

   a. Arrêtez l'instance EC2.
   b. Dans le menu EC2 Elastic Block Store Volumes, sélectionnez le volume racine que vous souhaitez remplacer.
   c. Choisissez Actions, puis Détacher le volume.
   d. Dans le menu EC2 Elastic Block Store Volumes, sélectionnez le nouveau volume.

e. Choisissez Actions, puis choisissez Attacher un volume.
f. Sélectionnez l'instance à laquelle vous souhaitez associer le volume et utilisez le même nom de périphérique que celui indiqué précédemment.

Pour les volumes autres que root :

a. Dans le menu EC2 Elastic Block Store Volumes, sélectionnez le volume non root que vous souhaitez remplacer.
b. Choisissez Actions, puis Détacher le volume.
c. Attachez le nouveau volume en le choisissant dans le menu EC2 Elastic Block Store Volumes, puis en choisissant Actions, Attacher un volume. Sélectionnez l'instance à laquelle vous souhaitez l'associer, puis sélectionnez un nom de périphérique disponible.
d. À l'aide du système d'exploitation de l'instance, démontez le volume existant, puis montez le nouveau volume à sa place.

   Sous Linux, vous pouvez utiliser la `umount` commande. Sous Windows, vous pouvez utiliser un gestionnaire de volumes logiques (LVM) tel que l'utilitaire système de gestion des disques.
e. Détachez tous les volumes précédents que vous êtes en train de remplacer en les sélectionnant dans le menu EC2 Elastic Block Store Volumes, puis en choisissant Actions, Détacher le volume.

Vous pouvez également utiliser les commandes du système d'exploitation AWS CLI en combinaison avec les commandes du système d'exploitation pour automatiser ces étapes.

Création ou restauration d'une instance EC2 à partir d'un instantané EBS

Pour créer une sauvegarde qui sera utilisée pour restaurer une instance EC2 complète, nous vous recommandons de créer une Amazon Machine Image (AMI). Les AMI capturent des informations sur les machines, telles que le type de virtualisation. Ils créent également des instantanés pour chaque volume attaché à l'instance EC2, y compris leurs mappages de périphériques, afin qu'ils puissent être restaurés dans la même configuration.

Toutefois, si vous devez utiliser un instantané EBS pour restaurer une instance, créez d'abord une AMI à partir d'un instantané EBS qui deviendra le volume racine de votre nouvelle instance EC2 :

1. Sur la console Amazon EC2, dans le menu Elastic Block Store, choisissez Snapshots.
2. Recherchez l'instantané qui sera utilisé pour créer le volume racine de votre nouvelle instance EC2, puis sélectionnez-le.

3. Choisissez Actions, puis sélectionnez Créer une image à partir d'un instantané.
4. Entrez un nom pour votre image (par exemple,`YYYYMMDD-restore-for-i-012345678998765de`) et choisissez les options appropriées pour votre nouvelle image.

Une fois l'image créée et disponible, vous pouvez lancer une nouvelle instance EC2 qui utilisera l'instantané EBS pour le volume racine.

Restauration d'une instance en cours d'exécution à partir d'une AMI

Vous pouvez créer une nouvelle instance à partir de la sauvegarde de votre AMI pour remplacer une instance existante en cours d'exécution. L'une des approches consiste à arrêter l'instance existante, à la maintenir hors ligne pendant que vous lancez une nouvelle instance depuis votre AMI et à effectuer les mises à jour nécessaires. Cette approche réduit le risque de conflits liés à l'exécution simultanée des deux instances. Cette approche est acceptable si les services fournis par votre instance sont hors service ou si vous effectuez la restauration pendant une période de maintenance. Après avoir testé votre nouvelle instance, vous pouvez réattribuer toutes les adresses IP élastiques allouées à l'ancienne instance. Vous pouvez ensuite mettre à jour tous les enregistrements DNS (Domain Name Service) pour qu'ils pointent vers la nouvelle instance.

Toutefois, si, au cours d'une restauration, vous devez minimiser le temps d'arrêt de votre instance en service, envisagez de lancer et de tester une nouvelle instance à partir de votre sauvegarde AMI. Remplacez ensuite l'instance existante par la nouvelle instance.

Pendant que les deux instances sont en cours d'exécution, vous devez empêcher la nouvelle instance de provoquer des collisions au niveau de la plate-forme ou au niveau de l'application. Par exemple, vous pouvez rencontrer des problèmes avec des instances Windows jointes à un domaine qui s'exécutent avec le même SID et le même nom d'ordinateur. Vous pouvez rencontrer des problèmes similaires avec les applications et services réseau qui nécessitent des identifiants uniques.

Pour empêcher d'autres serveurs et services de se connecter à votre nouvelle instance avant qu'elle ne soit prête, utilisez des groupes de sécurité pour bloquer temporairement toutes les connexions entrantes pour votre nouvelle instance, à l'exception de votre propre adresse IP pour l'accès et les tests. Vous pouvez également bloquer temporairement les connexions sortantes pour la nouvelle instance afin d'empêcher les services et les applications d'établir des connexions ou de mettre à jour d'autres ressources. Lorsque la nouvelle instance est prête, arrêtez l'instance existante, démarrez les services et les processus sur la nouvelle instance, puis débloquez les connexions réseau entrantes ou sortantes que vous avez implémentées.

Sauvegarde et restauration depuis une infrastructure sur site versAWS

Vous pouvez utiliserAWSpour un stockage hors site durable des sauvegardes de votre infrastructure sur site. En utilisantAWSservices de stockage Dans ce scénario, vous pouvez vous concentrer sur les tâches de sauvegarde et d'archivage. Vous n'avez pas à vous soucier du provisionnement, de la mise à l'échelle ou de la capacité de l'infrastructure de stockage pour vos tâches de sauvegarde.

Amazon S3 et Amazon S3 Glacier fournissent des opérations d'API et des kits de développement logiciel complets pour intégrer ces services dans vos approches de sauvegarde et de restauration nouvelles et existantes. Cela permet également aux fournisseurs de logiciels de sauvegarde d'intégrer directement leurs applications àAWSsolutions de stockage.

Dans ce scénario, le logiciel de sauvegarde et d'archivage que vous utilisez dans votre infrastructure sur site s'interface directement avecAWSvia les opérations de l'API. Parce que le logiciel de sauvegarde estAWS-aware, il sauvegarde les données des serveurs locaux directement sur Amazon S3 ou Amazon S3 Glacier.

Si votre logiciel de sauvegarde existant ne prend pas en charge de manière native leAWSCloud, vous pouvez utiliser Storage Gateway. Service de stockage dans le cloud, Storage Gateway permet à vos systèmes sur site d'accéder à un stockage cloud évolutif. Il prend en charge les protocoles de stockage standard ouverts qui fonctionnent avec vos applications existantes tout en stockant en toute sécurité vos données cryptées dans Amazon S3 ou Amazon S3 Glacier. Vous pouvez utiliser Storage Gateway dans le cadre d'une approche de sauvegarde et de restauration pour vos charges de travail de stockage par blocs locales.

Storage Gateway est utile dans les scénarios hybrides dans lesquels vous souhaitez passer à un stockage basé sur le cloud pour vos sauvegardes. Storage Gateway vous aide également à réduire les investissements en capital dans le stockage sur site. Vous déployez Storage Gateway en tant que machine virtuelle ou appliance matérielle dédiée. Ce guide explique comment Storage Gateway s'applique à la sauvegarde et à la restauration.

Storage Gateway propose trois options différentes pour répondre à différentes exigences :

- Une passerelle de fichiers permettant de stocker des fichiers de données d'applications et des images de sauvegarde sous forme d'objets durables sur le stockage cloud Amazon S3 à l'aide d'un accès SMB ou NFS.

- Une passerelle de volumes pour présenter des volumes de stockage par blocs iSCSI basés sur le cloud à vos applications sur site. Une passerelle de volumes fournit soit un cache local, soit des volumes complets sur site, tout en stockant des copies complètes de vos volumes dansAWSNuage.
- Une passerelle sur bande permettant de pointer un logiciel de sauvegarde fiable vers une passerelle de stockage sur site qui, à son tour, se connecte à Amazon S3 et à Amazon S3 Glacier. Cette option offre l'évolutivité et la durabilité du cloud pour une rétention sûre et à long terme sans perturber les investissements ou les processus existants.

Passerelle de fichiers

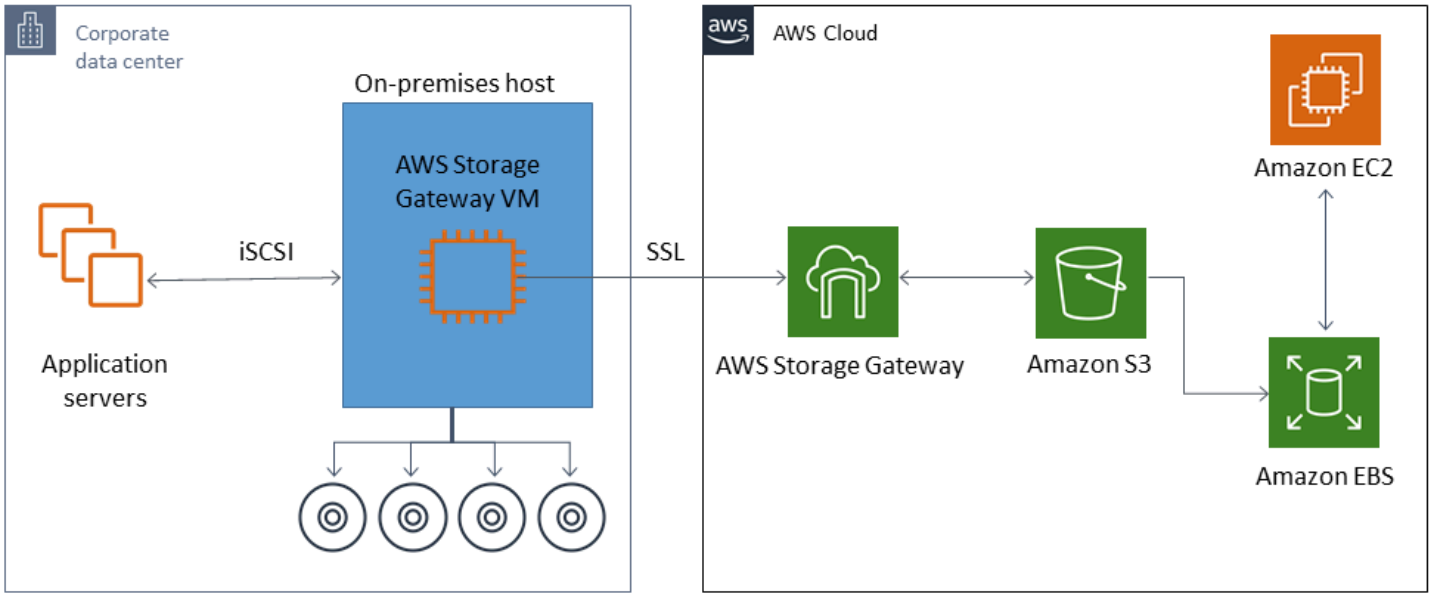
De nombreuses entreprises commencent leur transition vers le cloud en y transférant des données secondaires et tertiaires, telles que des sauvegardes. La prise en charge des interfaces SMB et NFS d'une passerelle de fichiers permet aux groupes informatiques de transférer les tâches de sauvegarde des systèmes de sauvegarde sur site existants vers le cloud. Les applications de sauvegarde, les outils de base de données natifs ou les scripts qui peuvent écrire sur SMB ou NFS peuvent écrire sur une passerelle de fichiers. La passerelle de fichiers stocke les sauvegardes sous forme d'objets Amazon S3 d'une taille maximale de 5 TiB. Avec un cache local de taille adéquate, les sauvegardes récentes peuvent être utilisées pour des restaurations rapides sur site. Les besoins de rétention à long terme sont satisfaits en hiérarchisant les sauvegardes selon les niveaux de stockage à faible coût S3 Standard-Infrequent Access et Amazon S3 Glacier.

La passerelle de fichiers fournit une passerelle entre votre stockage par blocs et Amazon S3 pour des sauvegardes hors site hautement durables. Elle est particulièrement utile pour les scénarios dans lesquels un fichier récemment sauvegardé doit être restauré rapidement. Comme une passerelle de fichiers prend en charge les protocoles SMB et NFS, les utilisateurs peuvent accéder aux fichiers de la même manière qu'ils accèderaient à un partage de fichiers réseau. Vous pouvez également tirer parti des fonctionnalités de gestion des versions des objets d'Amazon S3. La gestion des versions d'objets vous permet de restaurer les versions d'objet précédentes d'un fichier, puis d'y accéder facilement à l'aide de SMB ou NFS.

Passerelle de volumes

Une passerelle de volumes vous permet de provisionner des volumes de stockage par blocs iSCSI basés sur le cloud pour vos serveurs sur site. La passerelle de volume stocke les données de vos volumes sur Amazon S3 pour un stockage hors site durable et évolutif basé sur le cloud. Une

passerelle de volume facilite la prise en charge complètepoint-in-timedes instantanés de vos volumes et leur stockage dans le cloud sous forme d'instantanés Amazon EBS. Une fois qu'ils sont stockés sous forme d'instantanés, des volumes entiers peuvent être restaurés en tant que volumes EBS et attachés à des instances EC2, accélérant ainsi la mise en place d'une solution de reprise après sinistre basée sur le cloud. Les volumes peuvent également être restaurés sur Storage Gateway, ce qui permet à vos applications locales de revenir à un état antérieur.



Étant donné qu'une passerelle de volume s'intègre à la fonctionnalité de volume Amazon EBS d'Amazon EC2, vous pouvez utiliserAWS Backuppour automatiser et planifier votre processus de capture instantanée. Une passerelle de volume vous offre les avantages supplémentaires d'instantanés Amazon EBS durables et de fonctionnalités de balisage compatibles avec Amazon S3. Pour plus d'informations, consultez leDocumentation sur les instantanés Amazon EBS.

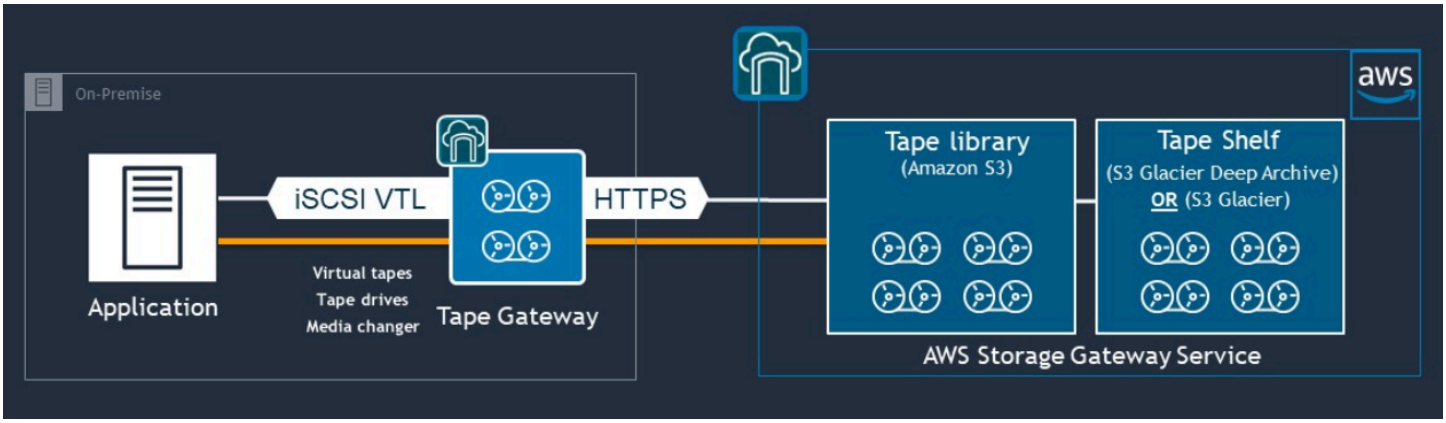
Passerelle de bandes

Une passerelle de bande offre la durabilité élevée, le stockage hiérarchisé à faible coût et les fonctionnalités étendues d'Amazon S3 et d'Amazon S3 Glacier pour votre magasin de sauvegarde sur bande virtuelle hors site. Toutes vos bandes virtuelles stockées dans Amazon S3 et Amazon S3 Glacier sont répliquées et stockées dans au moins trois zones de disponibilité géographiquement dispersées. Vos bandes virtuelles sont protégées par une durabilité de 11 neuf.

AWSeffectue également des contrôles de fixité sur une base régulière pour confirmer que vos données peuvent être lues et qu'aucune erreur n'a été introduite. Toutes les bandes stockées dans Amazon S3 sont protégées par un chiffrement côté serveur à l'aide de clés par défaut ou de

votreAWS KMSclés. De plus, vous évitez les risques de sécurité physique liés à la portabilité des bandes. Avec une passerelle de bande, vous obtenez des données correctes, contrairement à l'entreposage de bandes hors site, où vous pourriez recevoir une bande incorrecte ou cassée lors de la restauration.

Vous pouvez économiser sur les coûts de stockage mensuels lorsque vous stockez vos données dans Amazon S3. Vous pouvez économiser encore davantage pour répondre à vos besoins d'archivage à long terme en utilisant S3 Glacier Deep Archive.



Une passerelle de bande agit comme une bibliothèque de bandes virtuelles (VTL) qui s'étend de votre environnement sur site à des services de stockage hautement évolutifs, redondants et durables : Amazon S3, S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive.

La passerelle de bande présente Storage Gateway vers votre application de sauvegarde existante sous la forme d'une VTL basée sur iSCSI aux normes ouvertes, dotée d'un changeur de média virtuel et de lecteurs de bande virtuels. Vous pouvez continuer à utiliser vos applications et flux de travail de sauvegarde existants tout en écrivant sur une collection de bandes virtuelles stockées sur Amazon S3 extrêmement évolutif. Lorsque vous n'avez plus besoin d'un accès immédiat ou fréquent aux données d'une bande virtuelle, votre application de sauvegarde peut les archiver dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, réduisant ainsi encore les coûts de stockage.

Vous pouvez récupérer une bande archivée dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive en général en 3 à 5 heures ou 12 heures, respectivement. La passerelle de bande peut être utilisée avec une application de sauvegarde compatible avec l'interface de la bibliothèque de bandes basée sur iSCSI pour accéder aux bandes virtuelles. Tenez également compte de la taille de stockage minimale de 100 Go par bande. Pour plus d'informations, consultez la liste desapplications de sauvegarde tiercesqui prennent en charge les passerelles sur bande.

Backup et restauration d'applications depuisAWSvers votre centre de données

Une stratégie vous oblige peut-être à implémenter un scénario tel que la reprise après sinistre ou la continuité de l'activité pour vos charges de travail basées sur le cloud et votre infrastructure locale. Si vous disposez déjà d'une infrastructure de sauvegarde de données pour vos serveurs sur site, vous pouvez l'étendre à votreAWSressources via une connexion VPN ou viaAWS Direct Connect. Vous pouvez installer l'agent de sauvegarde sur les instances EC2 et sauvegarder vos données et applications conformément à vos politiques de protection des données. Vous pouvez également utiliser Amazon S3 comme service intermédiaire pour stocker vos sauvegardes au niveau de l'application. Vous pouvez ensuite utiliser les opérations API, les kits SDK ou leAWS CLIpour restaurer les données dans votre environnement sur site.

Pour sauvegarder des données dansAWSservices autres qu'Amazon EC2, utilisez leAWS CLI, SDK et opérations API pour extraire les données dans le format souhaité. Copiez ensuite les données vers Amazon S3 et copiez-les depuis Amazon S3 vers votre environnement sur site. Certains services fournissent une exportation directe vers Amazon S3. Amazon RDS prend par exemple en chargesauvegarde nativedes bases de données Microsoft SQL Server vers Amazon S3.

Backup et restauration deAWS services cloud natifs

Votre approche de sauvegarde et de restauration doit couvrir lesAWS services utilisés dans vos charges de travail. AWSfournit des fonctionnalités et des options spécifiques aux services pour gérer et interagir avec vos données. Vous pouvez utiliser la consoleAWS CLI, les SDK et les opérations d'API pour implémenter la sauvegarde et la restaurationAWS des services que vous utilisez. Ce guide présente Amazon RDS et Amazon DynamoDB à titre d'exemples. AWS Backupprend en charge DynamoDB et Amazon RDS et doit être utilisé s'il répond à vos besoins.

Backup et restauration pour Amazon RDS

Amazon RDS inclut des fonctionnalités permettant d'automatiser les sauvegardes de bases de données. Amazon RDS crée un instantané du volume de stockage de votre instance de données, en sauvegardant l'intégralité de ce dernier et pas uniquement les bases de données. À l'aide d'Amazon RDS, vous pouvez créer une fenêtre de sauvegarde pour les sauvegardes automatisées, créer des instantanés d'instances de base de données, et partager et copier des instantanés entre les régions et les comptes.

Amazon RDS propose deux options différentes pour sauvegarder et restaurer vos instances de base de données :

- Les sauvegardes automatisées assurent point-in-time la restauration (PITR) de votre instance de base de données. Les sauvegardes automatiques sont activées par défaut lorsque vous créez une nouvelle instance de base de données.

  Amazon RDS effectue une sauvegarde quotidienne complète de vos données au cours d'une fenêtre de sauvegarde que vous définissez lorsque vous créez l'instance de base de données. Vous pouvez configurer une période de rétention allant jusqu'à 35 jours pour la sauvegarde automatique. Amazon RDS charge également les journaux de transaction pour les instances de données Amazon S3 toutes les 5 minutes. Amazon RDS utilise vos sauvegardes quotidiennes ainsi que vos journaux de transactions de base de données pour restaurer votre instance de base de données. Vous pouvez restaurer l'instance à tout moment pendant votre période de rétention, jusqu'à`LatestRestorableTime` (généralement, les cinq dernières minutes).

  Pour connaître l'heure de restauration la plus récente pour vos instances de base de données, utilisez l'appel`DescribeDBInstances` d'API. Vous pouvez également consulter l'onglet Description pour accéder à la base de données sur la console Amazon RDS.

Lorsque vous lancez un PITR, les journaux de transactions sont combinés à la sauvegarde quotidienne la plus appropriée pour restaurer votre instance de base de données à l'heure requise.

- Les snapshots DB sont des sauvegardes initiées par l'utilisateur que vous pouvez utiliser pour restaurer l'instance de données à un état connu aussi souvent que vous le souhaitez. Vous pouvez ensuite revenir à cet état à tout moment. Vous pouvez utiliser la console Amazon RDS ou l'appel d'`CreateDBSnapshot`API pour créer des instantanés de base de données. Ces instantanés sont conservés jusqu'à ce que vous utilisiez la console ou l'appel d'`DeleteDBSnapshot`API pour les supprimer explicitement.

Ces deux options de sauvegarde sont prises en charge par Amazon RDS inAWS Backup, qui fournit également d'autres fonctionnalités. AWS BackupEnvisagez de configurer un plan de sauvegarde standard pour vos bases de données Amazon RDS et d'utiliser les options de sauvegarde d'instance initiées par l'utilisateur lorsque vos plans de sauvegarde pour une base de données particulière sont uniques.

Amazon RDS empêche l'accès direct au stockage sous-jacent utilisé par l'instance de base de données. Cela vous empêche également d'exporter directement la base de données d'une instance de base de données RDS vers son disque local. Dans certains cas, vous pouvez utiliser des fonctions de sauvegarde et de restauration natives à l'aide d'utilitaires clients. Par exemple, vous pouvez utiliser la commande mysqldump avec une base de données MySQL Amazon RDS pour exporter une base de données vers votre ordinateur client local. Dans certains cas, Amazon RDS propose également des options avancées pour effectuer une sauvegarde et une restauration natives d'une base de données. Par exemple, Amazon RDS fournit des procédures stockées pour exporter et importer des sauvegardes de bases de données SQL Server dans les bases de données RDS.

Assurez-vous de tester minutieusement votre processus de restauration de base de données et son impact sur les clients de base de données dans le cadre de votre approche globale de sauvegarde et de restauration.

Utilisation d'enregistrements DNS CNAME pour réduire l'impact sur le client lors d'une restauration de base de données

Lorsque vous restaurez une base de données à l'aide du PITR ou d'un instantané d'instance de base de données RDS, une nouvelle instance de base de données avec un nouveau point de terminaison est créée. De cette façon, vous pouvez créer plusieurs instances de base de données à partir d'un instantané de base de données ou d'un moment précis. Des considérations particulières s'appliquent

lorsque vous restaurez une instance de base de données RDS pour remplacer une instance de base de données RDS active. Par exemple, vous devez déterminer comment vous allez rediriger vos clients de base de données existants vers la nouvelle instance avec un minimum d'interruptions et de modifications. Vous devez également garantir la continuité et la cohérence des données au sein de la base de données en tenant compte du temps de restauration des données et du temps de restauration lorsque la nouvelle instance commence à recevoir des écritures.

Vous pouvez créer un enregistrement DNS CNAME distinct qui pointe vers le point de terminaison de votre instance de base de données et demander à vos clients d'utiliser ce nom DNS. Vous pouvez ensuite mettre à jour le CNAME pour qu'il pointe vers un nouveau point de terminaison restauré sans avoir à mettre à jour vos clients de base de données.

Réglez la durée de vie (TTL) pour votre enregistrement CNAME à une valeur appropriée. Le TTL que vous spécifiez détermine la durée pendant laquelle l'enregistrement est mis en cache auprès des résolveurs DNS avant qu'une autre demande ne soit effectuée. Il est important de noter que certains résolveurs ou applications DNS peuvent ne pas respecter le TTL et qu'ils peuvent mettre en cache l'enregistrement plus longtemps que le TTL. Pour Amazon Route 53, si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, ou deux jours), vous réduirez le nombre d'appels que les résolveurs récursifs DNS doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Cela réduit la latence et votre facture pour le service Route 53. Pour plus d'd'd'informations, consultez Comment Amazon Route 53 achemine le trafic de votre domaine.

Les applications et les systèmes d'exploitation clients peuvent également mettre en cache les informations DNS que vous devez vider ou redémarrer pour lancer une nouvelle demande de résolution DNS et récupérer l'enregistrement CNAME mis à jour.

Lorsque vous lancez une restauration de base de données et que vous transférez le trafic vers votre instance restaurée, vérifiez que tous vos clients écrivent sur votre instance restaurée plutôt que sur votre instance précédente. Votre architecture de données peut prendre en charge la restauration de votre base de données, la mise à jour du DNS pour transférer le trafic vers votre instance restaurée, puis la correction de toutes les données qui peuvent encore être écrites sur votre instance précédente. Si ce n'est pas le cas, vous pouvez arrêter votre instance existante avant de mettre à jour l'enregistrement DNS CNAME. Tous les accès se font alors à partir de votre instance récemment restaurée. Cela peut entraîner temporairement des problèmes de connexion pour certains de vos clients de base de données que vous pouvez gérer individuellement. Pour réduire l'impact sur le client, vous pouvez effectuer la restauration de la base de données pendant une fenêtre de maintenance.

Écrivez vos applications de manière à gérer les échecs de connexion à la base de données avec élégance, en réessayant en utilisant un backoff exponentiel. Cela permet à votre application de se rétablir lorsqu'une connexion à la base de données devient indisponible lors d'une restauration sans provoquer de panne inattendue de votre application.

Une fois le processus de restauration terminé, vous pouvez conserver votre instance précédente dans un état arrêté. Vous pouvez également utiliser les règles des groupes de sécurité pour limiter le trafic vers votre instance précédente jusqu'à ce que vous soyez certain qu'elle n'est plus nécessaire. Pour une approche de mise hors service progressive, limitez d'abord l'accès du groupe de sécurité à une base de données en cours d'exécution. Vous pouvez éventuellement arrêter l'instance quand elle n'est plus nécessaire. Enfin, prenez un instantané de l'instance de données et supprimez-la.

Backup et restauration pour DynamoDB

DynamoDB fournit un PITR, qui permet d'effectuer des sauvegardes presque continues des données de votre table DynamoDB. Lorsque cette option est activée, DynamoDB conserve des sauvegardes incrémentielles de votre table au cours des 35 derniers jours jusqu'à ce que vous la désactiviez explicitement.

Vous pouvez également créer des sauvegardes à la demande de votre table DynamoDB à l'aide de la console DynamoDBAWS CLI, de l'API DynamoDB. Pour plus d'd'd'informations, consultez Sauvegarde d'une table DynamoDB. Vous pouvez programmer des sauvegardes périodiques ou future à l'aide des fonctions LambdaAWS Backup, ou vous pouvez personnaliser et automatiser votre approche de sauvegarde à l'aide des fonctions Lambda. Pour plus d'd'informations sur l'utilisation des fonctions Lambda pour la Backup de DynamoDB, consultez le billet de blog A schedule your Amazon DynamoDB On-Demand backup. Si vous ne souhaitez pas créer des scripts de planification et des tâches de nettoyage, vous pouvez utiliserAWS Backup pour créer des plans de sauvegarde. Les plans de sauvegarde incluent des calendriers et des politiques de conservation pour vos tables DynamoDB. AWS Backupcrée les sauvegardes et supprime les sauvegardes précédentes en fonction de votre calendrier de conservation. AWS Backupinclut également des options de sauvegarde DynamoDB avancées qui ne sont pas disponibles dans le service DynamoDB, notamment un stockage hiérarchisé à moindre coût et une copie entre comptes et entre régions. Pour plus d'd'd'informations, consultez Sauvegarde DynamoDB avancée.

Vous devez configurer manuellement les éléments suivants sur une table DynamoDB restaurée :

- Politiques de scaling automatique
- Politiques IAM

- CloudWatch Métriques et alarmes Amazon
- Étiquettes
- Paramètres de flux
- Paramètres TTL

Vous ne pouvez restaurer que l'intégralité des données d'une table vers une nouvelle table à partir d'une sauvegarde. Vous pouvez écrire sur la table restaurée seulement lorsque celle-ci est devenue active.

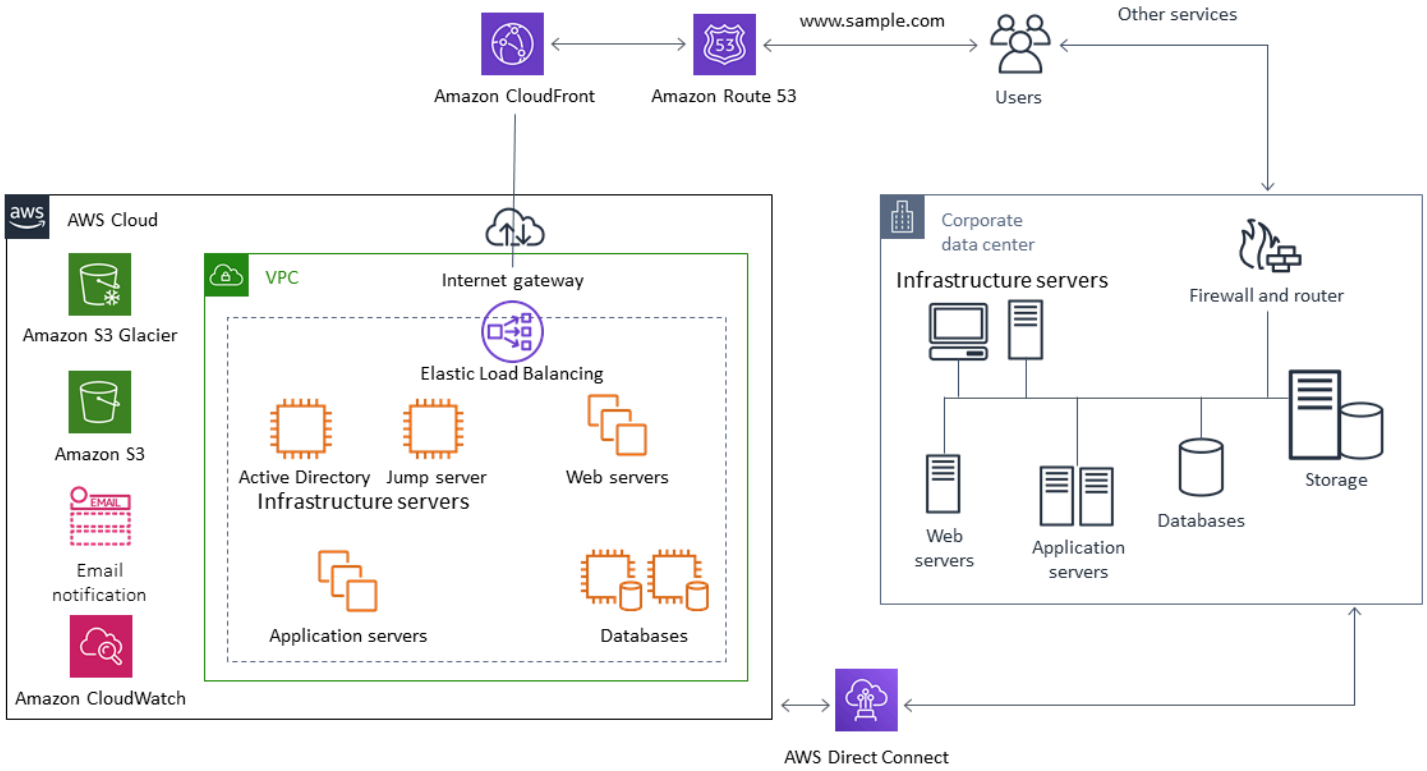
Votre processus de restauration doit tenir compte de la manière dont les clients seront redirigés pour utiliser le nom de la table récemment restaurée. Vous pouvez configurer vos applications et clients pour récupérer le nom de la table DynamoDB à partir d'un fichier de configuration, d'une valeur de la banque deAWS Systems Manager paramètres ou d'une autre référence pouvant être mise à jour dynamiquement pour refléter le nom de table que le client doit utiliser.

Dans le cadre du processus de restauration, vous devez examiner attentivement votre processus de transition. Vous pouvez choisir de refuser l'accès à votre table DynamoDB existante via des autorisations IAM et d'autoriser l'accès à votre nouvelle table. Vous pouvez ensuite mettre à jour la configuration de l'application et du client pour utiliser la nouvelle table. Vous devrez peut-être également réconcilier les différences entre votre table DynamoDB existante et la table DynamoDB récemment restaurée.

Backup et restauration pour architectures hybrides

Les déploiements cloud natifs et locaux décrits dans ce guide peuvent être combinés dans des scénarios hybrides dans lesquels l'environnement de charge de travail a été installé sur site etAWScomposants de l'infrastructure. Les ressources, y compris les serveurs Web, les serveurs d'applications, les serveurs de surveillance, les bases de données et Microsoft Active Directory, sont hébergées dans le centre de données client ou surAWS. Applications exécutées dans leAWSLe cloud est connecté à des applications exécutées sur site.

Ce scénario est en train de devenir courant pour les charges de travail d'entreprise. De nombreuses entreprises ont leurs propres centres de données et utilisent leurs propres centres de donnéesAWSpour augmenter la capacité. Ces centres de données clients sont souvent connectés auAWSréseau par liaisons réseau haute capacité. Par exemple, avecAWS Direct Connect, vous pouvez établir une connectivité privée et dédiée à partir de votre centre de données sur site àAWS. Cela fournit la bande passante et la latence cohérente nécessaires au téléchargement des données dans le cloud à des fins de protection des données. Il offre également des performances et une latence constantes pour les charges de travail hybrides. Le diagramme suivant fournit un exemple d'approche environnementale hybride.



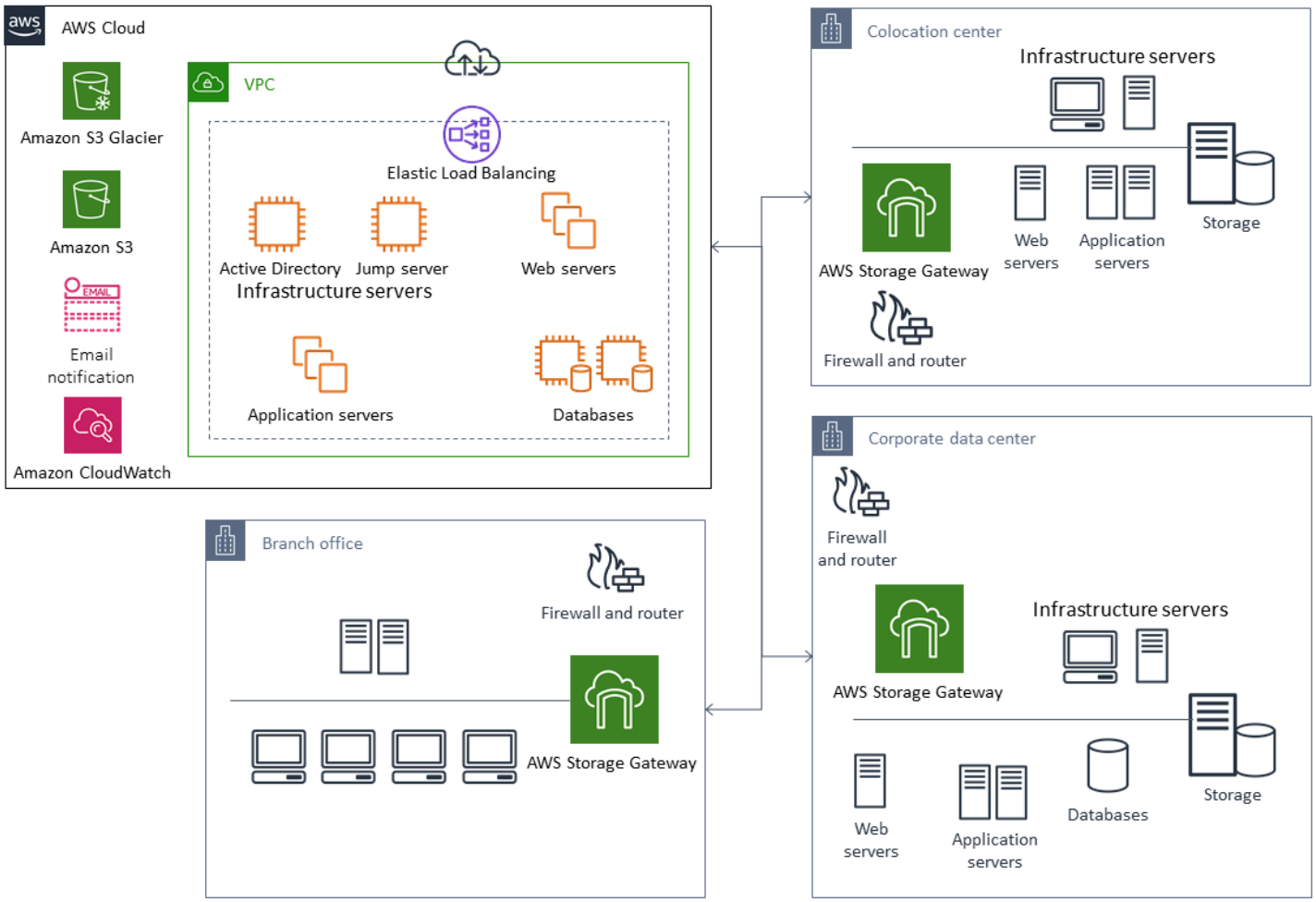
Les solutions de protection des données bien conçues utilisent généralement une combinaison des options décrites dans les solutions cloud natives et locales de ce guide. De nombreux ISV fournissent des solutions de sauvegarde et de restauration leader sur le marché pour l'infrastructure sur site et ont étendu leurs solutions pour prendre en charge les approches hybrides.

Déplacement de solutions de gestion centralisée des sauvegardes vers le cloud pour une plus grande disponibilité

En utilisant les investissements de votre solution de gestion des sauvegardes existante avecAWS, vous pouvez améliorer la résilience et l'architecture de votre approche. Il se peut que vous ayez un serveur de sauvegarde principal et un ou plusieurs serveurs de stockage ou de médias situés sur site sur plusieurs emplacements proches des serveurs et des services qu'ils protègent. Dans ce cas, envisagez de déplacer le serveur de sauvegarde principal vers une instance EC2 pour le protéger contre les catastrophes locales et pour une haute disponibilité.

Pour gérer les flux de données de sauvegarde, vous pouvez créer un ou plusieurs serveurs multimédias sur des instances EC2 dans la même région que les serveurs qu'ils vont protéger. Les serveurs multimédias situés à proximité des instances EC2 vous permettent d'économiser de l'argent sur le transfert Internet. Lorsque vous effectuez une sauvegarde sur Amazon S3 ou Amazon S3 Glacier, les serveurs multimédia augmentent les performances globales de sauvegarde et de restauration.

Vous pouvez également utiliser Storage Gateway pour fournir un accès cloud centralisé aux données provenant de centres de données et de bureaux géographiquement dispersés. Par exemple, une passerelle de fichiers vous donne un accès à la demande et à faible latence aux données stockées dansAWSpour les flux de travail d'applications pouvant s'étendre sur le monde entier. Vous pouvez utiliser des fonctionnalités telles que l'actualisation du cache pour actualiser les données dans des emplacements distribués géographiquement afin que le contenu puisse être facilement partagé entre vos bureaux.


AWS Cloud
Amazon S3 Glacier
Amazon S3
Email notification
Amazon CloudWatch
VPC
Elastic Load Balancing
Active Directory
Jump server
Infrastructure servers
Web servers
Application servers
Databases
Colocation center
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Storage
Firewall and router
Corporate data center
Firewall and router
AWS Storage Gateway
Infrastructure servers
Web servers
Application servers
Databases
Storage
Branch office
Firewall and router
AWS Storage Gateway

Reprise après sinistre avecAWS

Les approches de sauvegarde et de restauration ainsi que les services et technologies de support peuvent être utilisés pour mettre en œuvre votre solution de reprise après sinistre (DR). De nombreuses entreprises utilisent leAWSCloud pour la sauvegarde et la restauration et en tant que site DR.AWSfournit un certain nombre de services et de fonctionnalités qui soutiennent la reprise après sinistre et la continuité des activités.

Rubriques

- DR sur site pourAWS
- DR pour les charges de travail natives au cloud

DR sur site pourAWS

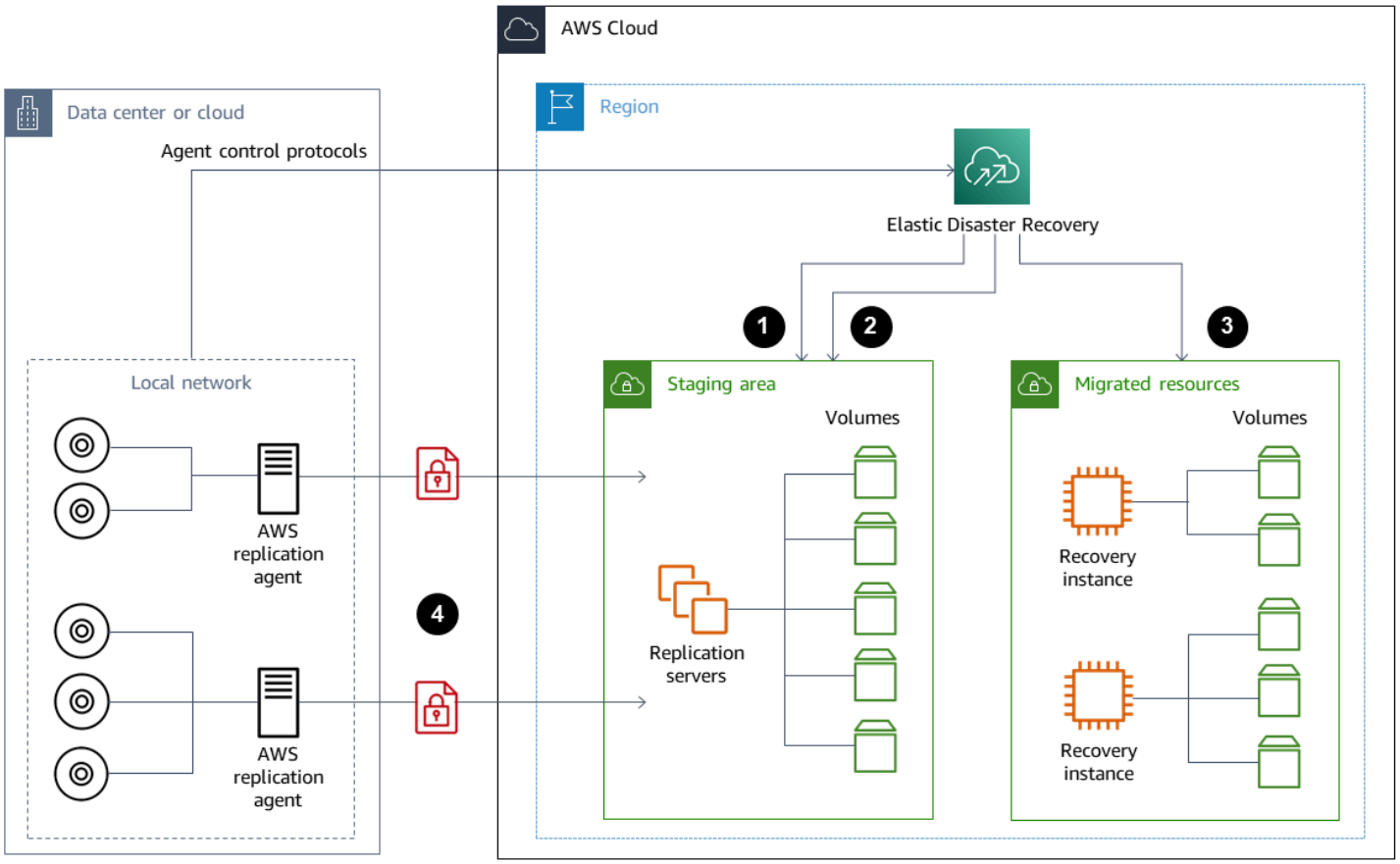
En utilisantAWSen tant qu'environnement de reprise après sinistre (DR) hors site pour les charges de travail sur site est un scénario hybride courant. Définissez vos objectifs de reprise après sinistre, y compris le temps de restauration requis et les objectifs de point de restauration, avant de sélectionner les technologies à utiliser. Pour vous aider à définir cette définition, vous pouvez utiliserListe de contrôle du plan DR.

Un certain nombre d'options sont disponibles pour vous aider à configurer et à provisionner rapidement un environnement DR surAWS. Assurez-vous de prendre en compte toutes les dépendances de votre charge de travail et testez votre plan et votre solution DR de manière approfondie et régulière pour vérifier leur intégrité.

AWSfournitAWS Elastic Disaster Recoverypour créer une réplique complète de vos serveurs locaux, y compris le volume racine et le système d'exploitation, surAWS. Elastic Disaster Recovery réplique en continu vos machines dans une zone intermédiaire peu coûteuse au sein de votre compte AWS cible et de votre compte préféréRégion AWS. La réplication au niveau des blocs est une réplique exacte du stockage de vos serveurs, y compris le système d'exploitation, la configuration de l'état du système, les bases de données, les applications et les fichiers. En cas de sinistre, vous pouvez demander à Elastic Disaster Recovery de lancer rapidement des milliers de vos machines dans leur état entièrement provisionné en quelques minutes.

Elastic Disaster Recovery utilise un agent installé sur chacun de vos serveurs locaux. Les agents synchronisent l'état de vos serveurs locaux avec les équivalents Amazon EC2 de moindre puissance

exécutés surAWS. Vous pouvez également automatiser votre processus de reprise après sinistre et de restauration avec Elastic Disaster Recovery. L'automatisation de votre processus de basculement et de restauration peut vous aider à atteindre un objectif de temps de restauration (RTO) plus bas et plus cohérent.



1. Rapports sur l'état du serveur de réplication
2. Ressources de la zone de test créées et supprimées automatiquement
3. Instances de restauration lancées avec un RTO de minutes et un RPO de secondes
4. Réplication continue au niveau des blocs (compressée et cryptée)

Il est important de tester le processus de reprise après sinistre et de vérifier que l'environnement de live staging ne crée pas de conflits avec l'environnement sur site. Par exemple, vérifiez que les licences appropriées sont disponibles et fonctionnent dans votre environnement de reprise après sinistre sur site, intermédiaire et initié. Vérifiez également que tous les processus de type travailleur susceptibles d'interroger et d'extraire du travail d'une base de données centrale sont configurés de manière appropriée pour éviter les chevauchements ou les conflits. Dans votre processus de reprise après sinistre, incluez toutes les étapes nécessaires qui doivent être effectuées avant que vos

instances de serveur de restauration ne soient mises en ligne. Incluez également les étapes à suivre une fois que les instances du serveur de restauration sont en ligne et disponibles. Vous pouvez utiliser des solutions telles queAWS Elastic Disaster RecoverySolution d'automatisation des plansou une autre approche pour vous aider à automatiser vos plans de reprise après sinistre.

Vous pouvez utiliser unpasserelle de volume Storage Gatewaypour fournir à vos serveurs locaux des volumes basés sur le cloud. Ces volumes peuvent également être rapidement provisionnés pour être utilisés avec Amazon EC2 à l'aide des instantanés Amazon EBS. En particulier, les passerelles de volumes stockés fournissent à vos applications locales un accès à faible latence à l'intégralité de leurs ensembles de données. Les passerelles de volume fournissent également des sauvegardes durables basées sur des instantanés qui peuvent être restaurées pour une utilisation sur site ou pour une utilisation avec Amazon EC2. Vous pouvez planifierpoint-in-timedes instantanés basés sur l'objectif de point de restauration (RPO) pour votre charge de travail.

> **Important**
>
> Les volumes de passerelle de volumes sont destinés à être utilisés comme volumes de données et non comme volumes de démarrage.

Vous pouvez utiliser une Amazon Machine Image (AMI) Amazon EC2 avec une configuration qui correspond à vos serveurs locaux et spécifie vos volumes de données séparément. Après avoir configuré et testé l'AMI, provisionnez les instances EC2 à partir de l'AMI ainsi que les volumes de données en fonction des instantanés de la passerelle de volumes. Cette approche nécessite que vous testiez minutieusement votre environnement pour vérifier que votre instance EC2 fonctionne correctement, en particulier pour les charges de travail Windows.

DR pour les charges de travail natives au cloud

Déterminez comment vos charges de travail natives du cloud s'alignent sur vos objectifs de reprise après sinistre.AWSfournit plusieurs zones de disponibilité dans différentes régions du monde. De nombreuses entreprises utilisent leAWSLe cloud aligne ses architectures de charge de travail et ses objectifs de reprise après sinistre pour résister à la perte d'une zone de disponibilité. LePilier de fiabilitédans leAWSLe Well-Architected Framework soutient cette bonne pratique. Vous pouvez concevoir vos charges de travail et leurs dépendances entre les services et les applications de manière à utiliser plusieurs zones de disponibilité. Vous pouvez ensuite automatiser votre DR et atteindre vos objectifs de DR avec peu ou pas d'intervention.

Dans la pratique, toutefois, il se peut que vous ne parveniez pas à établir une architecture redondante, active et automatisée pour tous vos composants. Examinez chaque couche de votre architecture afin de déterminer les processus de reprise après sinistre nécessaires pour atteindre vos objectifs. Cela peut varier d'une charge de travail à l'autre, avec des exigences architecturales et de service différentes. Ce guide couvre les considérations et les options relatives à Amazon EC2. Pour d'autresAWSservices, vous pouvez vous référer auAWSdocumentationpour déterminer les options de haute disponibilité et de reprise après sinistre.

DR pour Amazon EC2 dans une zone de disponibilité unique

Essayez de concevoir vos charges de travail de manière à soutenir et à servir activement les clients issus de plusieurs zones de disponibilité. Vous pouvez utiliser Amazon EC2 Auto Scaling et Elastic Load Balancing pour créer une architecture de serveur multi-AZ pour Amazon EC2 et d'autres services.

Si votre architecture comporte des instances EC2 qui ne peuvent pas être équilibrées et qu'une seule instance peut être exécutée à un moment donné, vous pouvez utiliser l'une des options suivantes.

- Créez un groupe Auto Scaling dont la taille minimale, maximale et souhaitée est de 1 et qui est configuré pour plusieurs zones de disponibilité. Créez une AMI qui pourra être utilisée pour remplacer l'instance en cas de défaillance. Assurez-vous de définir l'automatisation et la configuration appropriées afin qu'une instance nouvellement provisionnée à partir de l'AMI puisse être automatiquement configurée et fournir le service. Créez un équilibreur de charge qui pointe vers le groupe Auto Scaling et qui est configuré pour plusieurs zones de disponibilité. Vous pouvez également créer un alias Amazon Route 53 qui pointe vers le point de terminaison de l'équilibreur de charge.
- Créez un enregistrement Route 53 pour votre instance active et demandez à vos clients de se connecter à l'aide de cet enregistrement. Créez un script qui crée une nouvelle AMI de votre instance active et utilise l'AMI pour provisionner une nouvelle instance EC2 à l'état arrêté dans une zone de disponibilité distincte. Configurez le script pour qu'il s'exécute régulièrement et pour mettre fin à la précédente instance arrêtée. En cas de défaillance d'une zone de disponibilité, démarrez votre instance de sauvegarde dans votre zone de disponibilité alternative. Mettez ensuite à jour l'enregistrement Route 53 pour qu'il pointe vers cette nouvelle instance.

Testez minutieusement votre solution en simulant la panne contre laquelle la solution a été conçue pour se protéger. Tenez également compte des mises à jour dont votre solution DR aura besoin à mesure que l'architecture de votre charge de travail évoluera.

DR pour Amazon EC2 en cas de panne régionale

Bien queAWSles défaillances régionales sont rares, il est possible qu'unAWSLa région pourrait échouer à un moment ou à un autre. Les clients doivent évaluer avec soin la complexité, le coût et les efforts nécessaires pour établir et maintenir un plan de reprise après sinistre multirégional par rapport aux avantages.AWSfournit des fonctionnalités qui prennent en charge les architectures multirégionales pour la disponibilité globale, le basculement et le DR. Ce guide présente quelques-unes des fonctionnalités disponibles spécifiques à la sauvegarde et à la restauration pour Amazon EC2.

AWSLes AMI et les instantanés Amazon EBS sont des ressources régionales qui peuvent être utilisées pour provisionner de nouvelles instances au sein d'une même région. Vous pouvez toutefois copier vos instantanés et vos AMI vers une autre région et les utiliser pour provisionner de nouvelles instances dans cette région. Pour soutenir un plan régional de reprise après sinistre, vous pouvez automatiser le processus de copie des AMI et des instantanés vers d'autres régions.AWS Backupet Amazon Data Lifecycle Manager prennent en charge la copie entre régions dans le cadre de votre configuration de sauvegarde.

AWS Elastic Disaster Recoverypeut être utilisé pour automatiser et répliquer en continu vos serveurs Amazon EC2 d'une région vers une autre région DR. Elastic Disaster Recovery peut simplifier votre approche de reprise après sinistre multirégion et vous aider à tester régulièrement votre plan de reprise après sinistre Amazon EC2 entre régions à l'aide d'exercices. Elastic Disaster Recovery peut vous aider lorsque la sauvegarde et la restauration ne sont pas en mesure d'atteindre vos objectifs de RTO et de RPO. Elastic Disaster Recovery peut vous aider à réduire votre RTO à quelques minutes et votre RPO à moins d'une seconde.

Quelle que soit la solution que vous utilisez, vous devez déterminer le processus de provisionnement, de basculement et de restauration à utiliser en cas de panne. Vous pouvez utiliser Route 53 avec des contrôles de santé et un basculement du système de noms de domaine pour vous aider à prendre en charge votre solution.

Nettoyage des sauvegardes

Pour réduire les coûts, nettoyez les sauvegardes qui ne sont plus nécessaires à des fins de restauration ou de conservation. Vous pouvez utiliserAWS Backupet Amazon Data Lifecycle Manager pour automatiser votre politique de rétention pour une partie de vos sauvegardes. Toutefois, même avec ces outils en place, vous avez toujours besoin d'une approche de nettoyage pour les sauvegardes effectuées séparément.

Une stratégie de balisage est une condition préalable à une stratégie de nettoyage. Utilisez le balisage pour identifier les ressources qui doivent être nettoyées, informer les propriétaires de manière appropriée et automatiser votre processus de nettoyage. Sauvegardes créées parAWSles dates de création correspondent à celles-ci, mais le balisage est important pour établir une corrélation entre les sauvegardes et vos charges de travail, vos exigences de conservation et l'identification des points de restauration.

Vous pouvez implémenter un processus de nettoyage pour les instantanés à l'aide de l'automatisation. Par exemple, vous pouvez scanner votre compte à la recherche d'instantanés et déterminer si les volumes correspondants sont dans un état attaché ou dans un état disponible. Vous pouvez filtrer davantage les résultats en fonction d'un seuil temporel que vous spécifiez. À l'aide des balises associées au volume, vous pouvez envoyer automatiquement un e-mail aux propriétaires des instantanés pour les avertir que la suppression de leurs instantanés a été planifiée. Cette correction automatique peut être mise en œuvre en utilisantAWS Configrègles, un script utilisantAWS CLI, ou une fonction Lambda utilisantAWSSDK.

Le gestionnaire de systèmes fournitAWS - Supprimer EBSVolumeSnapshotsetAS-DeleteSnapshotdocuments pour vous aider à lancer et à automatiser le nettoyage des instantanés Amazon EBS. Vous pouvez également utiliserAWS CLIetAWSSDK pour automatiser le nettoyage d'autresAWSdes ressources telles que des instantanés Amazon RDS.

FAQ sur la sauvegarde et la restauration

Quel calendrier de sauvegarde dois-je sélectionner ?

Définissez une fréquence de planification des sauvegardes qui correspond à votre objectif de point de restauration (RPO). Définissez une heure de sauvegarde lorsque votre charge de travail est inférieure à la charge la plus faible et à laquelle l'impact sur les utilisateurs peut être réduit. Créez unpoint-in-timeinstantané chaque fois que vous allez apporter une modification significative à votre charge de travail.

Dois-je créer des sauvegardes dans mes comptes de développement ?

Testez les modifications potentiellement importantes apportées à vos comptes de développement pour vos charges de travail et créez des sauvegardes avant d'effectuer des modifications de fond. Vous en avez peut-être bien d'autrespoint-in-timesauvegardes de restauration (PITR) sur vos comptes de développement et hors production à partir des activités de développement et de test.

Puis-je mettre à niveau des applications et continuer à utiliser un volume EBS pendant la création d'un instantané sans aucun impact ?

Les instantanés se produisent de manière asynchrone ; lepoint-in-timeun instantané est créé immédiatement, mais son état est en attente jusqu'à ce que tous les blocs modifiés aient été transférés vers Amazon S3. Pour les instantanés initiaux volumineux ou les instantanés suivants dans lesquels de nombreux blocs ont été modifiés, le transfert peut prendre plusieurs heures. Pendant le transfert, un instantané en cours n'est pas affecté par les opérations de lecture et d'écriture en cours sur le volume. Pour en savoir plus, consultez la documentation AWS.

Étapes suivantes

Commencez par évaluer, implémenter et tester votre approche de sauvegarde et de restauration dans un environnement hors production. Il est important de tester minutieusement votre processus de restauration et de vérifier que vos charges de travail restaurées fonctionnent comme prévu.

Testez le processus de restauration d'un seul composant de votre architecture en plus de tous les composants de votre architecture. Validez le temps de restauration pour chacun. Validez également l'impact de votre processus de sauvegarde et de restauration sur les dépendances en amont et en aval. Vérifiez l'impact de toute interruption de service sur vos dépendances en amont et confirmez l'impact en aval sur vos sauvegardes.

Ressources supplémentaires

Ressources AWS

- AWSDirectives prescriptives
- Documentation AWS
- Référence générale AWS
- Glossaire AWS

Services AWS

- AWS Backup
- Amazon CloudWatch
- AmazonCloudWatchÉvènements
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- IAM
- Amazon RDS
- Amazon S3
- Amazon S3 Glacier
- Passerelle de stockage
- AWS Systems Manager

Autres ressources

- Sauvegarde et restauration avecAWS Backup(solution)
- Reprise après sinistre des charges de travail surAWS: Restauration dans le cloud(livre blanc)
- Série Disaster Recovery(Articles de blog sur l'architecture AWS)
- Liste de contrôle du plan DR
- Approches de sauvegarde et de restauration utilisantAWS(document technique — archivé)

- Démarrer avec AWS Backup
- AWSMarketplace — Sauvegarde et restauration

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Si vous souhaitez être informé des future mises à jour, vous pouvez vous abonner à un fil RSS.

Modification	Description	Date
Informations mises à jour	Informations mises à jour dans laAWS section DR sur site vers.	13 avril 2023
Ajout d'une section	Ajout de conseils et d'étapes pour créer ou restaurer une instance à partir d'un instantané.	7 mars 2023
Ajout d'informations sur Elastic Disaster Recovery et précisions supplémentaires	Dans les sections Reprise après sinistre avecAWS et ChoixAWS des services pour la protection des données, des informations supplémentaires surAWS Elastic Disaster Recovery. Dans les sections Sauvegarde et restauration Amazon EC2 avec instantanés et AMI, Préparation d'un volume EBS avant de créer un instantané ou une AMI et Restauration à partir d'un instantané Amazon EBS ou d'une AMI, des précisions ont été ajoutées. Ajouté à la FAQ sur la Backup et la restauration.	19 janvier 2023
Ajout d'un lien	Ajout d'un lien vers la documentation Amazon Data	31 octobre 2022

	Lifecycle Manager dans la section Amazon Data Lifecycle Manager.	
Informations mises à jour	Les informations relatives à la restauration des volumes ont été mises à jour.	30 août 2022
Informations mises à jour et ajout d'une nouvelle section	Dans la section ChoixAWS des services pour la protection des données, des services ont été ajoutés. Ajout de la section Sauvegarde et restauration à l'aide d'AWS Backup. Dans la section Backup et restauration à l'aide d'Amazon S3 et Amazon S3 Glacier, des informations supplémentaires sur les nouvelles classes de stockage Amazon S3 Glacier ont été ajoutées. Dans la section Backup et restauration pour Amazon EC2 avec volumes EBS, des liens vers la documentation et des informations supplémentaires ont été ajoutés. Dans la section Backup et restauration desAWS services cloud natifs, une recommandation d'utilisation a été ajoutéeAWS Backup. Dans la section Ressources supplémentaires, ressources ajoutées.	28 janvier 2022

Informations mises à jour	Ajout d'informations sur la définition des classes de stockage dans la section S3 Glacier Flexible Retrieval. Ajout d'informations sur la récupération des instantanés dans la section Sauvegarde et restauration Amazon EC2 avec instantanés et AMI.	9 septembre 2021
Informations mises à jour	Dans la AWS Backupsection, des informations supplémen taires sur lesAWS services prisAWS Backup en charge ont été ajoutées.	1er juin 2021
Publication initiale	—	29 juillet 2020

Glossaire des recommandations AWS

Les termes suivants sont couramment utilisés dans les politiques, les guides et les modèles fournis par les recommandations AWS. Pour suggérer des entrées, veuillez utiliser le lien Faire un commentaire à la fin du glossaire.

Nombres

7 R

Sept politiques de migration courantes pour transférer des applications vers le cloud. Ces politiques s'appuient sur les 5 R identifiés par Gartner en 2011 et sont les suivantes :

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers Amazon Aurora Édition compatible avec PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) for Oracle dans le Cloud AWS.
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Oracle sur une instance EC2 dans le Cloud AWS.
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Ce scénario de migration est propre à VMware Cloud on AWS, qui prend en charge la compatibilité des machines virtuelles (VM) et la portabilité de la charge de travail entre votre environnement sur site et AWS. Vous pouvez utiliser les technologies VMware Cloud Foundation à partir de vos centres de données sur site lorsque vous migrez votre infrastructure vers VMware Cloud on AWS. Exemple : relocalisez l'hyperviseur hébergeant votre base de données Oracle vers VMware Cloud on AWS.

- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.
- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue (à l'aide d'un outil de réplication bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration active-passive.

migration active-passive

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue, mais seule la base de données source gère les transactions provenant de la connexion d'applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

Fonction SQL qui agit sur un groupe de lignes et calcule une valeur de retour unique pour le groupe. Des exemples de fonctions d'agrégation incluent `SUM` et`MAX`.

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

Processus de suppression définitive d'informations personnelles dans un ensemble de données. L'anonymisation peut contribuer à protéger la vie privée. Les données anonymisées ne sont plus considérées comme des données personnelles.

anti-motif

Solution fréquemment utilisée pour un problème récurrent lorsque la solution est contre-productive, inefficace ou moins efficace qu'une alternative.

contrôle des applications

Une approche de sécurité qui permet d'utiliser uniquement des applications approuvées afin de protéger un système contre les logiciels malveillants.

portefeuille d'applications

Ensemble d'informations détaillées sur chaque application utilisée par une organisation, y compris le coût de génération et de maintenance de l'application, ainsi que sa valeur métier. Ces informations sont essentielles pour le processus de découverte et d'analyse du portefeuille et permettent d'identifier et de prioriser les applications à migrer, à moderniser et à optimiser.

intelligence artificielle (IA)

Domaine de l'informatique consacré à l'utilisation des technologies de calcul pour exécuter des fonctions cognitives généralement associées aux humains, telles que l'apprentissage, la résolution de problèmes et la reconnaissance de modèles. Pour plus d'informations, veuillez consulter Qu'est-ce que l'intelligence artificielle ?

opérations d'intelligence artificielle (AIOps)

Processus consistant à utiliser des techniques de machine learning pour résoudre les problèmes opérationnels, réduire les incidents opérationnels et les interventions humaines, mais aussi améliorer la qualité du service. Pour plus d'informations sur la façon dont les AIOps sont utilisées dans la stratégie de migration AWS, veuillez consulter le guide d'intégration des opérations.

chiffrement asymétrique

Algorithme de chiffrement qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint.

atomicité, cohérence, isolement, durabilité (ACID)

Ensemble de propriétés logicielles garantissant la validité des données et la fiabilité opérationnelle d'une base de données, même en cas d'erreur, de panne de courant ou d'autres problèmes.

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, veuillez consulter ABAC for AWS dans la documentation AWS Identity and Access Management (IAM).

source de données faisant autorité

Emplacement où vous stockez la version principale des données, considérée comme la source d'information la plus fiable. Vous pouvez copier les données de la source de données officielle vers d'autres emplacements à des fins de traitement ou de modification des données, par exemple en les anonymisant, en les expurgant ou en les pseudonymisant.

Zone de disponibilité

Emplacement distinct au sein d'une Région AWS qui est à l'abri des dysfonctionnements d'autres zones de disponibilité et offre une connectivité réseau peu coûteuse et de faible latence par rapport aux autres zones de disponibilité de la même région.

Framework d'adoption du Cloud AWS (AWS CAF)

Un cadre de directives et de bonnes pratiques d'AWS pour aider les entreprises à élaborer un plan efficient et efficace pour réussir leur migration vers le Cloud AWS. Le CAF organise ses conseils en six domaines prioritaires appelés perspectives : l'entreprise, les personnes, la gouvernance, la plateforme, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications

afin de préparer l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

AWS Workload Qualification Framework (AWS WQF)

Outil qui évalue les charges de travail de migration de base de données, recommande des politiques de migration et fournit des estimations de travail. AWS WQF est inclus avec AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

Vue unifiée et interactive des comportements des ressources et des interactions au fil du temps. Vous pouvez utiliser un graphique de comportement avec Amazon Detective pour examiner les tentatives de connexion infructueuses, les appels d'API suspects et les actions similaires. Pour plus d'informations, veuillez consulter Data in a behavior graph dans la documentation Detective.

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi endianité.

classification binaire

Processus qui prédit un résultat binaire (l'une des deux classes possibles). Par exemple, votre modèle de machine learning peut avoir besoin de prévoir des problèmes tels que « Cet e-mail est-il du spam ou non ? » ou « Ce produit est-il un livre ou une voiture ? ».

filtre de Bloom

Structure de données probabiliste et efficace en termes de mémoire qui est utilisée pour tester si un élément fait partie d'un ensemble.

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche

que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez À propos des branches (GitHub documentation).

accès par brise-vitre

Dans des circonstances exceptionnelles et par le biais d'un processus approuvé, c'est un moyen rapide pour un utilisateur d'accéder à un accès auquel Compte AWS il n'est généralement pas autorisé. Pour plus d'informations, consultez l'indicateur Implementation break-glass procedures dans le guide Well-ArchitectedAWS.

stratégie existante (brownfield)

L'infrastructure existante de votre environnement. Lorsque vous adoptez une stratégie existante pour une architecture système, vous concevez l'architecture en fonction des contraintes des systèmes et de l'infrastructure actuels. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

cache de tampon

Zone de mémoire dans laquelle sont stockées les données les plus fréquemment consultées.

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

Plan qui tient compte de l'impact potentiel d'un événement perturbateur, tel qu'une migration à grande échelle, sur les opérations, et qui permet à une entreprise de reprendre ses activités rapidement.

C

CAF

Voir le cadre d'adoption du AWS cloud.

CCoE

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

Processus de suivi des modifications apportées à une source de données, telle qu'une table de base de données, et d'enregistrement des métadonnées relatives à ces modifications. Vous pouvez utiliser la CDC à diverses fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.

ingénierie du chaos

Introduire intentionnellement des défaillances ou des événements perturbateurs pour tester la résilience d'un système. Vous pouvez utiliser AWS Fault Injection Service(AWS FIS) pour effectuer des expériences qui stressent vos AWS charges de travail et évaluer leur réponse.

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

Processus de catégorisation qui permet de générer des prédictions. Les modèles de ML pour les problèmes de classification prédisent une valeur discrète. Les valeurs discrètes se distinguent toujours les unes des autres. Par exemple, un modèle peut avoir besoin d'évaluer la présence ou non d'une voiture sur une image.

chiffrement côté client

Chiffrement des données en local, avant que le Service AWS cible ne les reçoive.

Centre d'excellence cloud (CCoE)

Une équipe multidisciplinaire qui dirige les efforts d'adoption du cloud au sein d'une organisation, notamment en développant les bonnes pratiques en matière de cloud, en mobilisant des ressources, en établissant des délais de migration et en guidant l'organisation dans le cadre de transformations à grande échelle. Pour plus d'informations, veuillez consulter les publications du CCoE sur le blog AWS Cloud Enterprise Strategy.

cloud computing

Technologie cloud généralement utilisée pour le stockage de données à distance et la gestion des appareils IoT. Le cloud computing est généralement associé à la technologie informatique de pointe.

modèle d'exploitation du cloud

Dans une organisation informatique, modèle d'exploitation utilisé pour créer, faire évoluer et optimiser un ou plusieurs environnements cloud. Pour plus d'informations, consultez la section Création de votre modèle d'exploitation cloud.

étapes d'adoption du cloud

Les quatre phases que les organisations traversent généralement lorsqu'elles migrent vers le Cloud AWS :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog The Journey Toward Cloud-First & the Stages of Adoption sur le blog AWS Cloud Enterprise Strategy. Pour en savoir plus sur la façon dont elles sont liées à stratégie de migration AWS, veuillez consulter le guide de préparation à la migration.

CMDB

Consultez la base de données de gestion des configurations.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub ouAWS CodeCommit. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

Cache tampon vide, mal rempli ou contenant des données obsolètes ou non pertinentes. Cela affecte les performances, car l'instance de base de données doit lire à partir de la mémoire principale ou du disque, ce qui est plus lent que la lecture à partir du cache tampon.

données gelées

Données rarement consultées et généralement historiques. Lorsque vous interrogez ce type de données, les requêtes lentes sont généralement acceptables. Le transfert de ces données vers des niveaux ou classes de stockage moins performants et moins coûteux peut réduire les coûts.

vision par ordinateur

Domaine de l'IA utilisé par les machines pour identifier des personnes, des lieux et des objets sur des images avec une précision égale ou supérieure à celle de l'être humain. Souvent conçu à partir de modèles d'apprentissage profond, il automatise l'extraction, l'analyse, la classification et la compréhension des informations utiles à partir d'une seule image ou d'une séquence d'images.

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

Une collection de règles AWS Config et d'actions correctives que vous pouvez mettre en place pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans un Compte AWS et une région, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, veuillez consulter Conformance packs dans la documentation AWS Config.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes source, de génération, de test, intermédiaire et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

D

données au repos

Données stationnaires dans votre réseau, telles que les données stockées.

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du cadre AWS Well-Architected. Pour plus d'informations, veuillez consulter Classification des données.

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

Données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau.

minimisation des données

Le principe de collecte et de traitement des seules données strictement nécessaires. La pratique de la minimisation des données AWS Cloud peut réduire les risques liés à la confidentialité, les coûts et l'empreinte carbone de vos analyses.

périmètre de données

Ensemble de garde-fous préventifs dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Pour plus d'informations, voir Création d'un périmètre de données sur AWS.

prétraitement des données

Pour transformer les données brutes en un format facile à analyser par votre modèle de ML. Le prétraitement des données peut impliquer la suppression de certaines colonnes ou lignes et le traitement des valeurs manquantes, incohérentes ou en double.

provenance des données

Le processus de suivi de l'origine et de l'historique des données tout au long de leur cycle de vie, par exemple la manière dont les données ont été générées, transmises et stockées.

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt de données

Un système de gestion des données qui prend en charge les informations commerciales, telles que les analyses. Les entrepôts de données contiennent généralement de grandes quantités de données historiques et sont généralement utilisés pour les requêtes et les analyses.

langage de définition de base de données (DDL)

Instructions ou commandes permettant de créer ou de modifier la structure des tables et des objets dans une base de données.

langage de manipulation de base de données (DML)

Instructions ou commandes permettant de modifier (insérer, mettre à jour et supprimer) des informations dans une base de données.

DDL

Voir langage de définition de base de données.

ensemble profond

Sert à combiner plusieurs modèles de deep learning à des fins de prédiction. Vous pouvez utiliser des ensembles profonds pour obtenir une prévision plus précise ou pour estimer l'incertitude des prédictions.

deep learning

Un sous-champ de ML qui utilise plusieurs couches de réseaux neuronaux artificiels pour identifier le mappage entre les données d'entrée et les variables cibles d'intérêt.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie sur AWS, vous ajoutez plusieurs contrôles à différentes couches de

la structure AWS Organizations afin de protéger les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte membre AWS pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique Services qui fonctionnent avec AWS Organizations dans la documentation AWS Organizations.

déploiement

Processus de mise à disposition d'une application, de nouvelles fonctionnalités ou de corrections de code dans l'environnement cible. Le déploiement implique la mise en œuvre de modifications dans une base de code, puis la génération et l'exécution de cette base de code dans les environnements de l'application.

environnement de développement

Voir environnement.

contrôle de détection

Contrôle de sécurité conçu pour détecter, journaliser et alerter après la survenue d'un événement. Ces contrôles constituent une deuxième ligne de défense et vous alertent en cas d'événements de sécurité qui ont contourné les contrôles préventifs en place. Pour plus d'informations, veuillez consulter la rubrique Contrôles de détection dans Implementing security controls on AWS.

cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSM étend le processus de cartographie de la chaîne de valeur initialement conçu pour les pratiques de production allégée. Il met l'accent sur les étapes et les équipes nécessaires pour créer et transférer de la valeur tout au long du processus de développement logiciel.

jumeau numérique

Représentation virtuelle d'un système réel, tel qu'un bâtiment, une usine, un équipement industriel ou une ligne de production. Les jumeaux numériques prennent en charge la maintenance prédictive, la surveillance à distance et l'optimisation de la production.

tableau des dimensions

Dans un schéma en étoile, table plus petite contenant les attributs de données relatifs aux données quantitatives d'une table de faits. Les attributs des tables de dimensions sont généralement des champs de texte ou des nombres discrets qui se comportent comme du texte. Ces attributs sont couramment utilisés pour la contrainte des requêtes, le filtrage et l'étiquetage des ensembles de résultats.

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

La stratégie et le processus que vous utilisez pour minimiser les temps d'arrêt et les pertes de données causés par un sinistre. Pour plus d'informations, consultez Disaster Recovery of Workloads on AWS : Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

Approche visant à développer un système logiciel complexe en connectant ses composants à des domaines évolutifs, ou objectifs métier essentiels, que sert chaque composant. Ce concept a été introduit par Eric Evans dans son ouvrage Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur l'utilisation du design piloté par domaine avec le modèle de figuier étrangleur, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

DR

Voir reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

informatique de périphérie

Technologie qui augmente la puissance de calcul des appareils intelligents en périphérie d'un réseau IoT. Comparé au cloud computing, l'informatique de pointe peut réduire la latence des communications et améliorer le temps de réponse.

chiffrement

Processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré.

clé de chiffrement

Chaîne cryptographique de bits aléatoires générée par un algorithme cryptographique. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique.

endianisme

Ordre selon lequel les octets sont stockés dans la mémoire de l'ordinateur. Les systèmes de poids fort stockent d'abord l'octet le plus significatif. Les systèmes de poids faible stockent d'abord l'octet le moins significatif.

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou aux principaux AWS Identity and Access Management (IAM). Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, veuillez consulter la rubrique Envelope encryption dans la documentation AWS Key Management Service (AWS KMS).

environment

Instance d'une application en cours d'exécution. Les types d'environnement les plus courants dans le cloud computing sont les suivants :

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un pipeline CI/CD, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les épopées AWS CAF en matière de sécurité comprennent la gestion des identités et des accès, les contrôles de détection, la sécurité de l'infrastructure, la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS, veuillez consulter le guide d'implémentation du programme.

analyse exploratoire des données (EDA)

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. L'EDA est réalisée en calculant des statistiques récapitulatives et en créant des visualisations de données.

F

tableau des faits

La table centrale dans un schéma en étoile. Il stocke des données quantitatives sur les opérations commerciales. Généralement, une table de faits contient deux types de colonnes : celles qui contiennent des mesures et celles qui contiennent une clé étrangère pour une table de dimensions.

échouer rapidement

Une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement. C'est un élément essentiel d'une approche agile.

limite d'isolation des défauts

Dans leAWS Cloud, une limite telle qu'une zone de disponibilitéRégion AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir succursale.

fonctionnalités

Les données d'entrée que vous utilisez pour faire une prédiction. Par exemple, dans un contexte de fabrication, les fonctionnalités peuvent être des images capturées périodiquement à partir de la ligne de fabrication.

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec : AWS.

transformation de fonctionnalité

Optimiser les données pour le processus de ML, notamment en enrichissant les données avec des sources supplémentaires, en mettant à l'échelle les valeurs ou en extrayant plusieurs ensembles d'informations à partir d'un seul champ de données. Cela permet au modèle de ML de tirer parti des données. Par exemple, si vous décomposez la date « 2021-05-27 00:15:37 » en

« 2021 », « mai », « jeudi » et « 15 », vous pouvez aider l'algorithme d'apprentissage à apprendre des modèles nuancés associés à différents composants de données.

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

Utilisation de plusieurs conditions pour autoriser ou refuser une demande d'accès.

migration instantanée (flash-cut)

Méthode de migration de base de données qui utilise la réplication continue des données par le biais de la capture des données de modification afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

G

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Flux de travail Gitflow

Approche dans laquelle les environnements inférieurs et supérieurs utilisent différentes branches dans un référentiel de code source. Le flux de travail Gitflow est considéré comme existant, et le flux de travail basé sur les troncs est l'approche moderne préférée.

stratégie inédite

L'absence d'infrastructures existantes dans un nouvel environnement. Lorsque vous adoptez une stratégie inédite pour une architecture système, vous pouvez sélectionner toutes les nouvelles technologies sans restriction de compatibilité avec l'infrastructure existante, également appelée brownfield. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités d'organisation (UO). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub GuardDutyAWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. AWS propose AWS SCT qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation des historiens

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS

for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l'identité

Politique attachée à un ou plusieurs principaux IAM qui définit leurs autorisations au sein de l'environnement AWS Cloud.

application inactive

Application dont l'utilisation moyenne du processeur et de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

IIoT

Voir Internet industriel des objets.

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures mutables. Pour plus d'informations, consultez les meilleures pratiques de déploiement à l'aide d'une infrastructure immuable dans le AWS Well-Architected Framework.

VPC entrant (d'entrée)

Dans une architecture à comptes multiples AWS, VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture de référence de sécurité AWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

VPC d'inspection

Dans une architecture AWS à comptes multiples, VPC centralisé qui gère les inspections du trafic réseau entre des VPC (dans des Régions AWS identiques ou différentes), Internet et les réseaux sur site. L'architecture de référence de sécurité AWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section Qu'est-ce que l'IoT ?.

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, veuillez consulter Machine learning model interpretability with AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. L'ITIL constitue la base de l'ITSM.

gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux outils ITSM, veuillez consulter le guide d'intégration des opérations.

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone de destination est un environnement AWS à comptes multiples Well-Architected évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.

lift and shift

Voir 7 Rs.

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi endianité.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter Machine Learning.

branche principale

Voir succursale.

services gérés

Services AWSqui AWS gère la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également connus sous le nom de services abstraits.

MAP

Voir Migration Acceleration Program.

mécanisme

Processus complet au cours duquel vous créez un outil, favorisez son adoption, puis inspectez les résultats afin de procéder aux ajustements nécessaires. Un mécanisme est un cycle qui se renforce et s'améliore au fur et à mesure de son fonctionnement. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.

compte membre

Tous les Comptes AWS autres que le compte de gestion qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

microservice

Petit service indépendant qui communique via des API bien définies et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement,

la réutilisation du code et la résilience. Pour plus d'informations, veuillez consulter Integrating microservices by using AWS serverless services.

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie à l'aide d'API légères. Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, veuillez consulter Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

Programme AWS qui fournit un support de conseil, des formations et des services pour aider les entreprises à générer une base opérationnelle solide pour passer au cloud et pour aider à compenser le coût initial des migrations. MAP inclut une méthodologie de migration pour exécuter les migrations héritées de manière méthodique, ainsi qu'un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague. Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la stratégie de migration AWS.

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement les opérations, les analystes commerciaux et les propriétaires, les ingénieurs de migration, les développeurs et les DevOps professionnels travaillant dans le cadre de sprints. Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le compte AWS.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réhéberger la migration vers Amazon EC2 avec AWS Application Migration Service.

Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le Cloud AWS. La MPA propose une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, comparaison du coût total de possession, analyse des coûts de migration), ainsi que la planification de la migration (analyse et collecte des données d'applications, regroupement des applications, priorisation des migrations et planification des vagues). L'outil MPA (connexion requise) est mis gratuitement à la disposition de tous les consultants AWS et consultants partenaires APN.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation au cloud d'une entreprise, à identifier les forces et les faiblesses, ainsi qu'à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide d'AWS CAF. Pour plus d'informations, veuillez consulter le guide de préparation à la migration. La MRA est la première phase de la stratégie de migration AWS.

stratégie de migration

Approche utilisée pour migrer une charge de travail vers le Cloud AWS. Pour plus d'informations, reportez-vous aux 7 R de ce glossaire et à Mobiliser votre organisation pour accélérer les migrations à grande échelle.

ML

Voir apprentissage automatique.

MPA

Voir Évaluation du portefeuille de migration.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, veuillez consulter Strategy for modernizing applications in the AWS Cloud.

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, veuillez consulter Evaluating modernization readiness for applications in the AWS Cloud.

applications monolithiques (monolithes)

Applications qui s'exécutent en tant que service unique avec des processus étroitement couplés. Les applications monolithiques ont plusieurs inconvénients. Si une fonctionnalité de l'application connaît un pic de demande, l'architecture entière doit être mise à l'échelle. L'ajout ou l'amélioration des fonctionnalités d'une application monolithique devient également plus complexe lorsque la base de code s'élargit. Pour résoudre ces problèmes, vous pouvez utiliser une architecture de microservices. Pour plus d'informations, veuillez consulter Decomposing monoliths into microservices.

classification multi-classes

Processus qui permet de générer des prédictions pour plusieurs classes (prédiction d'un résultat parmi plus de deux). Par exemple, un modèle de ML peut demander « Ce produit est-il un livre, une voiture ou un téléphone ? » ou « Quelle catégorie de produits intéresse le plus ce client ? ».

infrastructure mutable

Modèle qui met à jour et modifie l'infrastructure existante pour les charges de travail de production. Pour améliorer la cohérence, la fiabilité et la prévisibilité, le AWS Well-Architected Framework recommande l'utilisation d'une infrastructure immuable comme meilleure pratique.

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

Méthode de migration dans laquelle la charge de travail source est supprimée au cours du processus de migration. Cette méthode implique un temps d'arrêt prolongé et est généralement utilisée pour de petites charges de travail non critiques.

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

Méthode de migration dans laquelle la charge de travail source est copiée sur le système cible sans être mise hors ligne. Les applications connectées à la charge de travail peuvent continuer à fonctionner pendant la migration. Cette méthode implique un temps d'arrêt nul ou minimal et est généralement utilisée pour les charges de travail de production critiques.

accord au niveau opérationnel (OLA)

Accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de prendre en charge un contrat de niveau de service (SLA).

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, à évaluer, à prévenir ou à réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

intégration des opérations (OI)

Processus de modernisation des opérations dans le cloud, qui implique la planification de la préparation, l'automatisation et l'intégration. Pour en savoir plus, veuillez consulter le guide d'intégration des opérations.

journal de suivi d'organisation

Journal de suivi créé par AWS CloudTrail qui journalise tous les événements pour tous les Comptes AWS dans une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de migration AWS, ce cadre s'appelle accélération des personnes, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

Dans CloudFront, une option améliorée pour restreindre l'accès afin de sécuriser votre contenu Amazon Simple Storage Service (Amazon S3). OAC prend en charge tous les compartiments S3 dans toutes les Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS), ainsi que les demandes `PUT` et `DELETE` dynamiques adressées au compartiment S3.

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés ne peuvent accéder au contenu d'un compartiment S3 que par le biais d'une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

OU

Voir l'examen de l'état de préparation opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS à comptes multiples, VPC qui gère les connexions réseau initiées depuis une application. L'architecture de référence de sécurité AWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

P

limite des autorisations

Politique de gestion IAM attachée aux principaux IAM pour définir les autorisations maximales que peut avoir l'utilisateur ou le rôle. Pour plus d'informations, veuillez consulter la rubrique Limites des autorisations dans la documentation IAM.

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

PII

Voir les informations personnelles identifiables.

manuel stratégique

Ensemble d'étapes prédéfinies qui capturent le travail associé aux migrations, comme la fourniture de fonctions d'opérations de base dans le cloud. Un manuel stratégique peut revêtir la forme de scripts, de runbooks automatisés ou d'un résumé des processus ou des étapes nécessaires au fonctionnement de votre environnement modernisé.

politique

Objet capable de définir les autorisations (voir la politique basée sur l'identité), de spécifier les conditions d'accès (voir la politique basée sur les ressources) ou de définir les autorisations maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des services).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

Processus de découverte, d'analyse et de priorisation du portefeuille d'applications afin de planifier la migration. Pour plus d'informations, veuillez consulter Evaluating migration readiness.

predicate

Une condition de requête qui renvoie `true` ou`false`, généralement située dans une `WHERE` clause.

prédicat pushdown

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela réduit la quantité de données qui doivent être extraites et traitées à partir de la base de données relationnelle et améliore les performances des requêtes.

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter Preventative controls dans Implementing security controls on AWS.

principal

Une entité d'AWS qui peut exécuter des actions et accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS, un rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

Confidentialité dès la conception

Une approche de l'ingénierie des systèmes qui prend en compte la confidentialité tout au long du processus d'ingénierie.

zones hébergées privées

Conteneur qui contient des informations concernant la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines dans un ou plusieurs VPC. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

environnement de production

Voir environnement.

pseudonymisation

Processus de remplacement des identifiants personnels dans un ensemble de données par des valeurs fictives. La pseudonymisation peut contribuer à protéger la vie privée. Les données pseudonymisées sont toujours considérées comme des données personnelles.

Q

plan de requête

Série d'étapes, telles que des instructions, utilisées pour accéder aux données d'un système de base de données relationnelle SQL.

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

Matrice RACI

Voir responsable, responsable, consulté, informé (RACI).

rançongiciel

Logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à ce qu'un paiement soit effectué.

Matrice RASCI

Voir responsable, responsable, consulté, informé (RACI).

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

Copie d'une base de données utilisée en lecture seule. Vous pouvez acheminer les requêtes vers le réplica de lecture pour réduire la charge sur votre base de données principale.

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Cela permet de déterminer ce qui est considéré comme une perte de données acceptable entre le dernier point de restauration et l'interruption du service.

objectif de temps de récupération (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service.

refactoriser

Voir 7 Rs.

Région

Ensemble de ressources AWS dans une zone géographique. Chaque Région AWS est isolée et indépendante des autres pour assurer la tolérance aux pannes, la stabilité et la résilience. Pour plus d'informations, veuillez consulter Managing Régions AWS dans Références générales AWS.

régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir 7 Rs.

version

Dans un processus de déploiement, action visant à promouvoir les modifications apportées à un environnement de production.

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

politique basée sur les ressources

Politique attachée à une ressource, comme un compartiment Amazon S3, un point de terminaison ou une clé de chiffrement. Ce type de politique précise les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

matrice responsable, redevable, consulté et informé (RACI)

Une matrice qui définit les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), consulté (C) et informé (I). Le type de support (S) est facultatif. Si vous incluez le support, la matrice est appelée matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

contrôle réactif

Contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Pour plus d'informations, veuillez consulter la rubrique Responsive controls dans Implementing security controls on AWS.

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

rotation

Processus de mise à jour périodique d'un secret pour empêcher un attaquant d'accéder aux informations d'identification.

contrôle d'accès aux lignes et aux colonnes (RCAC)

Utilisation d'expressions SQL simples et flexibles dotées de règles d'accès définies. Le RCAC comprend des autorisations de ligne et des masques de colonnes.

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif relatif au temps de rétablissement.

runbook

Ensemble de procédures manuelles ou automatisées nécessaires à l'exécution d'une tâche spécifique. Elles visent généralement à rationaliser les opérations ou les procédures répétitives présentant des taux d'erreur élevés.

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité active l'authentification unique (SSO) fédérée, permettant aux utilisateurs de se connecter à AWS Management Console ou d'appeler les opérations d'API AWS sans qu'il soit nécessaire de créer un utilisateur dans IAM pour chaque membre de l'organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCP

Voir la politique de contrôle des services.

secret

Dans AWS Secrets Manager des informations confidentielles ou restreintes, telles qu'un mot de passe ou des informations d'identification utilisateur, que vous stockez sous forme cryptée. Il comprend la valeur secrète et ses métadonnées. La valeur secrète peut être binaire, une chaîne unique ou plusieurs chaînes. Pour plus d'informations, consultez la section Secret dans la documentation de Secrets Manager.

contrôle de sécurité

Barrière de protection technique ou administrative qui empêche, détecte ou réduit la capacité d'un assaillant d'exploiter une vulnérabilité de sécurité. Il existe quatre principaux types de contrôles de sécurité : préventifs, détectifs, réactifs et proactifs.

renforcement de la sécurité

Processus qui consiste à réduire la surface d'attaque pour la rendre plus résistante aux attaques. Cela peut inclure des actions telles que la suppression de ressources qui ne sont plus requises, la mise en œuvre des bonnes pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

système de gestion des informations et des événements de sécurité (SIEM)

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs qui vous aident à mettre en œuvre les meilleures pratiques AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une instance Amazon EC2 ou la rotation des informations d'identification.

chiffrement côté serveur

Chiffrement des données à destination, par le Service AWS qui les reçoit.

Politique de contrôle des services (SCP)

Politique qui propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. Les SCP définissent des barrières de protection ou des

limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer les services ou les actions autorisés ou interdits. Pour plus d'informations, veuillez consulter la rubrique Politiques de contrôle de service dans la documentation AWS Organizations.

point de terminaison du service

URL du point d'entrée pour un Service AWS. Pour vous connecter par programmation au service cible, vous pouvez utiliser un point de terminaison. Pour plus d'informations, veuillez consulter la rubrique Service AWS endpoints dans Références générales AWS.

contrat de niveau de service (SLA)

Accord qui précise ce qu'une équipe informatique promet de fournir à ses clients, comme le temps de disponibilité et les performances des services.

indicateur de niveau de service (SLI)

Mesure d'un aspect des performances d'un service, tel que son taux d'erreur, sa disponibilité ou son débit.

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de niveau de service.

modèle de responsabilité partagée

Modèle décrivant la responsabilité que vous partagez avec AWS pour la conformité et la sécurité du cloud. AWS est responsable de la sécurité du cloud, tandis que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

SIEM

Consultez les informations de sécurité et le système de gestion des événements.

point de défaillance unique (SPOF)

Défaillance d'un seul composant critique d'une application susceptible de perturber le système.

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

Modèle permettant de mettre à l'échelle et d'accélérer les projets de modernisation. Au fur et à mesure que les nouvelles fonctionnalités et les nouvelles versions de produits sont définies, l'équipe principale se divise pour créer des équipes de produit. Cela permet de mettre à l'échelle les capacités et les services de votre organisation, d'améliorer la productivité des développeurs et de favoriser une innovation rapide. Pour plus d'informations, consultez la section Approche progressive de la modernisation des applications dans le. AWS Cloud

SPOF

Voir point de défaillance unique.

schéma en étoile

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un entrepôt de données ou à des fins de business intelligence.

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

Plage d'adresses IP dans votre VPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité.

chiffrement symétrique

Algorithme de chiffrement qui utilise la même clé pour chiffrer et déchiffrer les données.

tests synthétiques

Tester un système de manière à simuler les interactions des utilisateurs afin de détecter les problèmes potentiels ou de surveiller les performances. Vous pouvez utiliser Amazon CloudWatch Synthetics pour créer ces tests.

T

balises

Des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources.

variable cible

La valeur que vous essayez de prédire dans le cadre du ML supervisé. Elle est également qualifiée de variable de résultat. Par exemple, dans un environnement de fabrication, la variable cible peut être un défaut du produit.

liste de tâches

Outil utilisé pour suivre les progrès dans un runbook. Liste de tâches qui contient une vue d'ensemble du runbook et une liste des tâches générales à effectuer. Pour chaque tâche générale, elle inclut le temps estimé nécessaire, le propriétaire et l'avancement.

environnement de test

Voir environnement.

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

Hub de transit de réseau que vous pouvez utiliser pour relier vos VPC et vos réseaux sur site. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce qu'une passerelle de transit ? dans la documentation AWS Transit Gateway.

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

Octroi d'autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation dans AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, veuillez consulter la rubrique Utilisation d'AWS Organizations avec d'autres services AWS dans la documentation AWS Organizations.

réglage

Pour modifier certains aspects de votre processus d'entraînement afin d'améliorer la précision du modèle de ML. Par exemple, vous pouvez entraîner le modèle de ML en générant un ensemble d'étiquetage, en ajoutant des étiquettes, puis en répétant ces étapes plusieurs fois avec différents paramètres pour optimiser le modèle.

équipe de deux pizzas

Une petite DevOps équipe que vous pouvez nourrir avec deux pizzas. Une équipe de deux pizzas garantit les meilleures opportunités de collaboration possible dans le développement de logiciels.

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données.

Pour plus d'informations, veuillez consulter le guide Quantifying uncertainty in deep learning systems.

tâches indifférenciées

Également connu sous le nom de « levage de charges lourdes », ce travail est nécessaire pour créer et exploiter une application, mais qui n'apporte pas de valeur directe à l'utilisateur final ni d'avantage concurrentiel. Les exemples de tâches indifférenciées incluent l'approvisionnement, la maintenance et la planification des capacités.

environnements supérieurs

Voir environnement.

V

mise à vide

Opération de maintenance de base de données qui implique un nettoyage après des mises à jour incrémentielles afin de récupérer de l'espace de stockage et d'améliorer les performances.

contrôle de version

Processus et outils permettant de suivre les modifications, telles que les modifications apportées au code source dans un référentiel.

Appairage de VPC

Connexion entre deux VPC qui vous permet d'acheminer le trafic à l'aide d'adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées. L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

Données rarement consultées. Lorsque vous interrogez ce type de données, des requêtes modérément lentes sont généralement acceptables.

fonction de fenêtre

Fonction SQL qui effectue un calcul sur un groupe de lignes liées d'une manière ou d'une autre à l'enregistrement en cours. Les fonctions de fenêtre sont utiles pour traiter des tâches, telles que le calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

Ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend.

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir écrire une fois, lire plusieurs.

WQF

Consultez le cadre de qualification des charges de travail AWS.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire, mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'une vulnérabilité de type « jour zéro ».

vulnérabilité « jour zéro »

Une faille ou une vulnérabilité non atténuée dans un système de production. Les acteurs malveillants peuvent utiliser ce type de vulnérabilité pour attaquer le système. Les développeurs prennent souvent conscience de la vulnérabilité à la suite de l'attaque.

application zombie

Application dont l'utilisation moyenne du processeur et de la mémoire est inférieure à 5 %. Dans un projet de migration, il est courant de retirer ces applications.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.