Meilleures pratiques et fonctionnalités de chiffrement pour Services AWS

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Meilleures pratiques et fonctionnalités de chiffrement pour Services AWS

Table of Contents

Bonnes pratiques et fonctionnalités de chiffrement pour Services AWS

Kurt Kumar, Amazon Web Services

Janvier 2025 (historique du document)

Le chiffrement est un outil de cybersécurité fondamental pour protéger les données sensibles à l'ère numérique. Alors que les entreprises s'appuient de plus en plus sur les données pour piloter leurs opérations, y compris les déploiements d'IA générative, la protection de ces informations précieuses grâce à des pratiques de chiffrement robustes est un élément essentiel d'une stratégie complète de protection des données. Ce guide peut vous aider à comprendre les principes de chiffrement et les fonctionnalités de chiffrement qu'ils AWS offrent.

Les menaces de cybersécurité modernes incluent le risque de violation de données, c'est-à-dire lorsqu'un accès non autorisé à vos actifs informationnels entraîne la perte de données. Les données constituent un actif commercial propre à chaque organisation. Il peut s'agir des informations sur les clients, des business plans, des documents de conception ou du code. Protéger l'entreprise implique de protéger ses données.

Le chiffrement des données peut aider à protéger les données de votre entreprise même après une violation. Il fournit une couche de défense contre les divulgations involontaires. Pour accéder aux données chiffrées dans le AWS Cloud, les utilisateurs ont besoin d'autorisations afin d'utiliser la clé pour déchiffrer et d'autorisations pour utiliser le service sur lequel se trouvent les données. Sans ces deux autorisations, les utilisateurs ne sont pas en mesure de déchiffrer et de consulter les données.

En général, il existe trois types de données que vous pouvez chiffrer. Les données en transit sont les données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau. Les données au repos sont des données stationnaires et dormantes, telles que les données stockées. Les exemples incluent le stockage par blocs, le stockage d'objets, les bases de données, les archives et les appareils de l'Internet des objets (IoT). Les données utilisées font référence aux données que les applications ou les services traitent ou utilisent activement. En sécurisant les données au point d'utilisation, les entreprises peuvent contribuer à atténuer les risques de divulgation involontaire.

Ce guide décrit les points à prendre en compte et les meilleures pratiques en matière de chiffrement des données en transit et des données au repos. Il passe également en revue les fonctionnalités et les contrôles de cryptage disponibles dans de nombreux pays Services AWS. Vous pouvez

mettre en œuvre ces recommandations de chiffrement au niveau du service dans vos AWS Cloud environnements.

Public visé

Ce guide peut être utilisé par les petites, moyennes et grandes organisations des secteurs public et privé. Que votre organisation en soit aux premières étapes de l'évaluation et de la mise en œuvre d'une stratégie de protection des données ou qu'elle cherche à améliorer les contrôles de sécurité existants, les recommandations présentées dans ce guide sont les mieux adaptées aux publics suivants :

- Les dirigeants qui formulent les politiques de leur entreprise, tels que les directeurs généraux (CEOs), les directeurs de la technologie (CTOs), les directeurs informatiques (CIOs) et les responsables de la sécurité informatique (CISOs)
- Les responsables technologiques chargés de définir les normes techniques, tels que les vice-présidents et directeurs techniques
- Les parties prenantes de l'entreprise et les propriétaires d'applications qui ont les responsabilités suivantes :
  - Évaluation du niveau de risque, de la classification des données et des exigences de protection
  - Contrôle du respect des normes organisationnelles établies
- Responsables de la conformité, de l'audit interne et de la gouvernance chargés de contrôler le respect des politiques de conformité, y compris les régimes de conformité statutaires et volontaires

À propos des AWS services de cryptographie

Un algorithme de chiffrement est une formule ou une procédure qui convertit un message en texte brut en texte chiffré. Si le chiffrement ou sa terminologie ne vous sont pas familiers, nous vous recommandons de lire À propos du chiffrement des données avant de lire ce guide.

AWS les services de cryptographie s'appuient sur des algorithmes de chiffrement sécurisés et open source. Ces algorithmes sont approuvés par des organismes publics de normalisation et par des chercheurs universitaires. Certains AWS outils et services imposent l'utilisation d'un algorithme spécifique. Dans d'autres services, vous pouvez choisir entre plusieurs algorithmes et longueurs de clé disponibles ou utiliser les valeurs par défaut recommandées.

Cette section décrit certains des algorithmes pris en charge par les AWS outils et les services. Ils se répartissent en deux catégories, symétriques et asymétriques, selon le fonctionnement de leurs clés :

- Le chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer les données. Services AWS supportent l'Advanced Encryption Standard (AES) et le Triple Data Encryption Standard (3DES ou TDES), qui sont deux algorithmes symétriques largement utilisés.
- Le chiffrement asymétrique 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. Services AWS prennent généralement en charge le RSA et les algorithmes asymétriques de cryptographie à courbe elliptique (ECC).

AWS les services cryptographiques sont conformes à un large éventail de normes de sécurité cryptographique, ce qui vous permet de vous conformer aux réglementations gouvernementales ou professionnelles. Pour une liste complète des normes de sécurité des données Services AWS conformes, consultez les programmes de AWS conformité.

Bonnes pratiques générales de chiffrement

Cette section fournit des recommandations qui s'appliquent lors du chiffrement de données dans le AWS Cloud. Ces meilleures pratiques générales en matière de chiffrement ne sont pas spécifiques à Services AWS. Cette section comprend les rubriques suivantes:

- Classification des données
- Chiffrement des données en transit
- Chiffrement de données au repos

Classification des données

La classification des données est un processus qui permet 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 AWS Well-Architected Framework. Les catégories peuvent inclure hautement confidentiel, confidentiel, non confidentiel et public, mais les niveaux de classification et leurs noms peuvent varier d'une organisation à l'autre. Pour plus d'informations sur le processus, les considérations et les modèles de classification des données, consultez la section Classification des données (AWS livre blanc).

Après avoir classé vos données, vous pouvez créer une stratégie de chiffrement pour votre organisation en fonction du niveau de protection requis pour chaque catégorie. Par exemple, votre organisation peut décider que les données hautement confidentielles doivent utiliser un chiffrement asymétrique et que les données publiques ne nécessitent pas de chiffrement. Pour plus d'informations sur l'élaboration d'une stratégie de chiffrement, veuillez consulter Creating an enterprise encryption strategy for data at rest. Bien que les considérations techniques et les recommandations de ce guide soient propres aux données au repos, vous pouvez également utiliser l'approche progressive pour créer une stratégie de chiffrement pour les données en transit.

Chiffrement des données en transit

Toutes les données transmises Régions AWS sur le réseau AWS mondial sont automatiquement cryptées au niveau de la couche physique avant de quitter les installations AWS sécurisées. L'ensemble du trafic entre les zones de disponibilité est chiffré.

Les bonnes pratiques d'ordre général pour le chiffrement des données en transit dans le AWS Cloud sont les suivantes :

- Définissez une politique de chiffrement organisationnelle pour les données en transit, en fonction de la classification de vos données, des exigences organisationnelles et de toutes les normes réglementaires ou de conformité applicables. Nous vous recommandons vivement de chiffrer les données en transit classées comme hautement confidentielles ou confidentielles. Votre politique peut également spécifier le chiffrement pour d'autres catégories, telles que les données non confidentielles ou publiques, selon les besoins.
- Lorsque vous chiffrez des données en transit, nous vous recommandons d'utiliser des algorithmes de chiffrement, des modes de chiffrement par blocs et des longueurs de clé approuvés, tels que définis dans votre politique de chiffrement.
- Chiffrez le trafic entre les actifs d'information et les systèmes au sein du réseau et de l' AWS Cloud infrastructure de l'entreprise en utilisant l'une des méthodes suivantes :
  - AWS Site-to-Site VPNConnexions
  - Une combinaison de AWS Direct Connectconnexions AWS Site-to-Site VPN et, qui fournit une IPsec connexion privée cryptée
  - AWS Direct Connect connexions prenant en charge la sécurité MAC (MACsec) pour chiffrer les données des réseaux d'entreprise vers le site AWS Direct Connect
- Identifiez les politiques de contrôle d'accès pour vos clés de chiffrement en fonction du principe du moindre privilège. Le moindre privilège est la bonne pratique en matière de sécurité qui consiste à accorder aux utilisateurs l'accès minimum dont ils ont besoin pour exécuter leurs tâches. Pour plus d'informations sur l'application des autorisations du moindre privilège, veuillez consulter Bonnes pratiques de sécurité dans IAM et Bonnes pratiques pour les politiques IAM.

Chiffrement de données au repos

Tous les services de stockage de AWS données, tels qu'Amazon Simple Storage Service (Amazon S3) et Amazon Elastic File System (Amazon EFS), proposent des options pour chiffrer les données au repos. Le chiffrement est effectué à l'aide des services de chiffrement et de chiffrement par blocs AES-256 bits (Advanced Encryption Standard) 256 bits, AWS tels que () ou.AWS Key Management ServiceAWS KMSAWS CloudHSM

Vous pouvez chiffrer les données à l'aide du chiffrement côté client ou côté serveur, en fonction de facteurs tels que la classification des données, le besoin de end-to-end chiffrement ou les limitations techniques qui vous empêchent d'utiliser le chiffrement : end-to-end

- Le chiffrement côté client consiste à chiffrer les données en local avant que l'application ou le service cible ne les reçoive. L' Service AWS reçoit vos données chiffrées et ne joue aucun rôle dans leur chiffrement ou déchiffrement. Pour le chiffrement côté client, vous pouvez utiliser AWS KMS, l'AWS Encryption SDK ou d'autres outils ou services de chiffrement tiers.
- Le chiffrement côté serveur est l'action de chiffrement des données à leur destination par l'application ou le service qui les reçoit. Pour le chiffrement côté serveur, vous pouvez utiliser le chiffrement AWS KMS de l'ensemble du bloc de stockage. Vous pouvez également utiliser d'autres outils ou services de chiffrement tiers, tels que LUKS pour chiffrer un système de fichiers Linux au niveau du système d'exploitation (OS).

Les bonnes pratiques d'ordre général pour le chiffrement des données au repos dans le AWS Cloud sont les suivantes :

- Définissez une politique de chiffrement organisationnelle pour les données au repos, en fonction de la classification de vos données, des exigences organisationnelles et de toutes les normes réglementaires ou de conformité applicables. Pour plus d'informations, veuillez consulter Creating an enterprise encryption strategy for data at rest. Nous vous recommandons vivement de chiffrer les données au repos classées comme hautement confidentielles ou confidentielles. Votre politique peut également spécifier le chiffrement pour d'autres catégories, telles que les données non confidentielles ou publiques, selon les besoins.
- Lorsque vous chiffrez des données au repos, nous vous recommandons d'utiliser des algorithmes de cryptographie, des modes de chiffrement par blocs et des longueurs de clé approuvés.
- Identifiez les politiques de contrôle d'accès pour vos clés de chiffrement en fonction du principe du moindre privilège.

Bonnes pratiques de chiffrement pour Services AWS

Cette section inclut les meilleures pratiques et les recommandations concernant les points suivants Services AWS :

- AWS CloudTrail
- Amazon DynamoDB
- Amazon Elastic Compute Cloud (Amazon EC2) et Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service (Amazon RDS)
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (Amazon VPC)

Bonnes pratiques de chiffrement pour AWS CloudTrail

AWS CloudTrail vous aide à vérifier la gouvernance, la conformité et le risque opérationnel de votre Compte AWS.

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- CloudTrail les journaux doivent être chiffrés à l'aide d'un système géré par le client AWS KMS key. Choisissez une clé KMS située dans la même région que le compartiment S3 qui reçoit vos fichiers journaux. Pour plus d'informations, veuillez consulter Updating a trail to use your KMS key.
- Comme couche de sécurité supplémentaire, activez la validation des fichiers journaux pour les journaux de suivi. Cela vous permet de déterminer si un fichier journal a été modifié, supprimé

ou inchangé après CloudTrail sa livraison. Pour obtenir des instructions, consultez la section Activation de la validation de l'intégrité des fichiers journaux pour CloudTrail.

- Utilisez les points de terminaison VPC de l'interface pour permettre de CloudTrail communiquer avec des ressources situées dans d'autres pays VPCs sans passer par l'Internet public. Pour plus d'informations, veuillez consulter Utilisation d' AWS CloudTrail avec les points de terminaison de VPC d'interface.
- Ajoutez une clé de `aws:SourceArn` condition à la politique de clé KMS pour vous assurer que la clé KMS est CloudTrail utilisée uniquement pour un ou plusieurs sentiers spécifiques. Pour plus d'informations, consultez la section Configurer AWS KMS key les politiques pour CloudTrail.
- Dans AWS Config, implémentez la règle cloud-trail-encryption-enabled AWS gérée pour valider et appliquer le chiffrement des fichiers journaux.
- S'il CloudTrail est configuré pour envoyer des notifications via les rubriques Amazon Simple Notification Service (Amazon SNS), ajoutez `aws:SourceArn` une clé de condition (ou `aws:SourceAccount` facultativement) à la déclaration de politique afin d'empêcher CloudTrail l'accès non autorisé du compte à la rubrique SNS. Pour plus d'informations, consultez la politique relative aux rubriques Amazon SNS pour. CloudTrail
- Si vous en utilisez AWS Organizations, créez un journal d'organisation qui enregistre tous les événements relatifs Comptes AWS à cette organisation. Cela inclut le compte de gestion et tous les comptes membres de l'organisation. Pour en savoir plus, veuillez consulter Creating a trail for an organization.
- Créez un suivi qui s'applique à tous les Régions AWS endroits où vous stockez des données d'entreprise, afin Compte AWS d'enregistrer l'activité dans ces régions. Lors du AWS lancement d'une nouvelle région, inclut CloudTrail automatiquement la nouvelle région et enregistre les événements dans cette région.

Bonnes pratiques de chiffrement pour Amazon DynamoDB

Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives. Le chiffrement au repos de DynamoDB sécurise les données dans une table chiffrée incluant une clé primaire, des index secondaires locaux et globaux, des flux, des tables globales, des sauvegardes et des clusters DynamoDB Accelerator (DAX) chaque fois que les données sont stockées sur un support durable.

Conformément aux exigences de classification des données, la confidentialité et l'intégrité des données peuvent être préservées en implémentant un chiffrement côté serveur ou côté client :

Pour le chiffrement côté serveur, lorsque vous créez une table, vous pouvez utiliser AWS KMS keys pour chiffrer la table. Vous pouvez utiliser des clés AWS détenues, des clés AWS gérées ou des clés gérées par le client. Nous vous recommandons d'utiliser des clés gérées par le client, car votre organisation en a le contrôle total, et lorsque vous spécifiez ce type de clé, la clé de chiffrement au niveau de la table, la table DynamoDB, les index secondaires locaux et globaux, ainsi que les flux sont chiffrés avec la même clé. Pour plus d'informations sur ces types de clés, consultez la section Clés et AWS clés clients.

> **Note**
>
> Vous pouvez basculer entre une clé AWS détenue, une clé AWS gérée et une clé gérée par le client à tout moment.

Pour le chiffrement côté client et end-to-end la protection des données, à la fois au repos et en transit, vous pouvez utiliser le client de chiffrement Amazon DynamoDB. Outre le chiffrement, qui protège la confidentialité de la valeur de l'attribut de l'élément, le client de chiffrement DynamoDB signe l'élément. Cela fournit une protection de l'intégrité en permettant de détecter les modifications non autorisées apportées à l'élément, y compris l'ajout ou la suppression d'attributs, ou le remplacement d'une valeur chiffrée par une autre.

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Limitez les autorisations permettant de désactiver ou de planifier la suppression de la clé uniquement aux personnes qui doivent effectuer ces tâches. Ces états empêchent tous les utilisateurs et le service DynamoDB de chiffrer ou déchiffrer des données, ainsi que d'effectuer des opérations de lecture et d'écriture sur la table.
- DynamoDB chiffre les données en transit à l'aide du protocole HTTPS par défaut, mais des contrôles de sécurité supplémentaires sont recommandés. Vous pouvez utiliser les options suivantes :
  - AWS Site-to-Site VPN connexion utilisée IPsec pour le chiffrement.
  - AWS Direct Connect connexion pour établir une connexion privée.
  - AWS Direct Connect connexion avec AWS Site-to-Site VPN connexion pour une IPsec connexion privée cryptée.

  - Si vous n'avez besoin d'accéder à DynamoDB qu'à partir d'un cloud privé virtuel (VPC), vous pouvez utiliser un point de terminaison de passerelle VPC pour limiter l'accès uniquement à partir du VPC requis. Cela empêche le trafic de passer par l'Internet public.
- Si vous utilisez des points de terminaison d'un VPC, limitez les politiques de point de terminaison et les politiques IAM associées au point de terminaison aux utilisateurs, ressources et services autorisés. Pour plus d'informations, veuillez consulter Contrôle de l'accès à l'aide de politiques IAM et Utilisation des politiques de point de terminaison pour contrôler l'accès à des points de terminaison d'un VPC.
- Vous pouvez implémenter le chiffrement des données au niveau des colonnes au niveau de l'application pour les données nécessitant un chiffrement, conformément à votre politique de chiffrement.
- Configurez les clusters DAX pour chiffrer les données au repos, telles que les données du cache, les données de configuration et les fichiers journaux, au moment de la configuration du cluster. Vous ne pouvez pas activer le chiffrement au repos sur un cluster existant. Ce chiffrement côté serveur permet de protéger les données contre tout accès non autorisé via le stockage sous-jacent. Le chiffrement DAX au repos s'intègre automatiquement à AWS KMS pour gérer la clé par défaut à service unique utilisée pour chiffrer les clusters. Si aucune clé de service par défaut n'existe lors de la création d'un cluster DAX chiffré, une nouvelle clé AWS gérée est AWS KMS automatiquement créée. Pour plus d'informations, veuillez consulter Chiffrement au repos DAX.

    > **Note**
    >
    > Les clés gérées par le client ne peuvent pas être utilisées avec les clusters DAX.

- Configurez les clusters DAX pour chiffrer les données en transit au moment de la configuration du cluster. Vous ne pouvez pas activer le chiffrement en transit sur un cluster existant. DAX utilise le protocole TLS pour chiffrer les demandes et les réponses entre l'application et le cluster, et il utilise le certificat x509 du cluster pour authentifier l'identité du cluster. Pour plus d'informations, veuillez consulter Chiffrement DAX en transit.
- Dans AWS Config, implémentez la règle dax-encryption-enabled AWS gérée pour valider et maintenir le chiffrement des clusters DAX.

Bonnes pratiques de chiffrement pour Amazon EC2 et Amazon EBS

Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement. Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances. EC2

Tenez compte des bonnes pratiques de chiffrement suivantes pour ces services :

- Marquez tous les volumes EBS avec la clé et la valeur de classification de données appropriées. Cela vous permet de déterminer et de mettre en œuvre les exigences de sécurité et de chiffrement appropriées, conformément à votre politique.
- En fonction de votre politique de chiffrement et de la faisabilité technique, configurez le chiffrement des données en transit entre les EC2 instances ou entre les EC2 instances et votre réseau sur site.
- Chiffrez les volumes de démarrage et de données EBS d'une EC2 instance. Un volume EBS chiffré protège les données suivantes :
  - Données au repos à l'intérieur du volume
  - Toutes les données circulant entre le volume et l'instance
  - Tous les instantanés créés à partir du volume
  - Tous les volumes créés à partir de ces instantanés

  Pour plus d'informations, veuillez consulter Fonctionnement du chiffrement EBS.
- Activez actuellement Région AWS le chiffrement par défaut pour les volumes EBS de votre compte. Cela impose le chiffrement de tous les nouveaux volumes EBS et de toutes les copies d'instantanés. Cela n'a aucun effet sur les instantanés ni les volumes EBS existants. Pour plus d'informations, consultez la section Activer le chiffrement par défaut.
- Chiffrez le volume racine du stockage d'instance pour une EC2 instance Amazon. Cela vous permet de protéger les fichiers de configuration et les données stockées dans le système d'exploitation. Pour plus d'informations, consultez Comment protéger les données au repos avec le chiffrement du magasin d' EC2 instances Amazon (article de AWS blog)
- Dans AWS Config, implémentez la règle des volumes chiffrés pour les contrôles automatisés qui valident et appliquent les configurations de chiffrement appropriées.

Bonnes pratiques de chiffrement pour Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneur géré, sécurisé, évolutif et fiable.

Amazon ECR stocke les images dans des compartiments Amazon S3 gérés par Amazon ECR. Chaque référentiel Amazon ECR dispose d'une configuration de chiffrement, qui est définie lors de la création du référentiel. Par défaut, Amazon ECR utilise un chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (SSE-S3). Pour plus d'informations, veuillez consulter Chiffrement au repos (documentation Amazon ECR).

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Au lieu d'utiliser le chiffrement côté serveur par défaut avec des clés de chiffrement gérées par Amazon S3 (SSE-S3), utilisez des clés KMS gérées par le client et stockées dans AWS KMS. Ce type de clé fournit les options de contrôle les plus détaillées.

  > **Note**
  >
  > La clé KMS doit se trouver au même Région AWS endroit que le référentiel.

- Ne révoquez pas les octrois créés par défaut par Amazon ECR lorsque vous allouez un référentiel. Cela peut affecter les fonctionnalités, telles que l'accès aux données, le chiffrement des nouvelles images envoyées au référentiel ou leur déchiffrement lors de leur extraction.
- AWS CloudTrail À utiliser pour enregistrer les demandes auxquelles Amazon ECR envoie AWS KMS. Les entrées de journal contiennent une clé de contexte de chiffrement afin de les rendre plus facilement identifiables.
- Configurez les politiques Amazon ECR pour contrôler l'accès depuis des points de terminaison Amazon VPC spécifiques ou spécifiques. VPCs En effet, cela permet d'isoler l'accès réseau vers une ressource Amazon ECR spécifique, ce qui offre un accès depuis le VPC spécifique. En établissant une connexion de réseau privé virtuel (VPN) avec un point de terminaison d'un VPC Amazon, vous pouvez chiffrer les données en transit.
- Amazon ECR prend en charge les politiques basées sur les ressources. À l'aide de ces politiques, vous pouvez restreindre l'accès en fonction de l'adresse IP source ou de l'adresse IP spécifique Service AWS.

Bonnes pratiques de chiffrement pour Amazon ECS

Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.

Avec Amazon ECS, vous pouvez chiffrer les données en transit en utilisant l'une des approches suivantes :

- Créez un maillage de services. À l'aide de AWS App Mesh, configurez les connexions TLS entre les proxys Envoy déployés et les points de terminaison maillés, tels que les nœuds virtuels ou les passerelles virtuelles. Vous pouvez utiliser des certificats TLS fournis par le client AWS Private Certificate Authority ou des certificats fournis par celui-ci. Pour plus d'informations et des procédures pas à pas, voir Activer le chiffrement du trafic entre les services à AWS App Mesh l'aide de certificats AWS Certificate Manager (ACM) ou fournis par le client (article de blog).AWS
- Si cette option est prise en charge, utilisez AWS Nitro Enclaves. AWS Nitro Enclaves est EC2 une fonctionnalité d'Amazon qui vous permet de créer des environnements d'exécution isolés, appelés enclaves, à partir d'instances Amazon. EC2 Ils sont conçus pour protéger vos données les plus sensibles. En outre, ACM pour Nitro Enclaves vous permet d'utiliser des certificats SSL/TLS publics et privés avec vos applications Web et vos serveurs Web exécutés sur des instances Amazon avec Nitro Enclaves. EC2 AWS Pour plus d'informations, consultez AWS Nitro Enclaves — EC2 Environnements isolés pour traiter des données confidentielles (article de AWS blog).
- Utilisez le protocole SNI (Server Name Indication) avec les équilibreurs de charge d'application. Vous pouvez déployer plusieurs applications derrière un seul écouteur HTTPS pour un Application Load Balancer. Chaque écouteur possède son propre certificat TLS. Vous pouvez utiliser des certificats fournis par ACM ou des certificats auto-signés. Application Load Balancer et Network Load Balancer prennent en charge le protocole SNI. Pour plus d'informations, voir les équilibreurs de charge d'application prennent désormais en charge plusieurs certificats TLS avec sélection intelligente à l'aide du SNI (AWS article de blog).
- Pour améliorer la sécurité et la flexibilité, AWS Private Certificate Authority utilisez-le pour déployer un certificat TLS avec la tâche Amazon ECS. Pour plus d'informations, voir Gérer le protocole TLS jusqu'à votre conteneur, partie 2 : Utilisation AWS Private CA (article de AWS blog).
- Implémentez le protocole TLS mutuel (MTL) dans App Mesh à l'aide du service de découverte secret (Envoy) ou de certificats hébergés dans ACM (). GitHub

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Lorsque cela est techniquement possible, pour renforcer la sécurité, configurez des points de terminaison d'un VPC de l'interface Amazon ECS dans AWS PrivateLink. L'accès à ces points de terminaison sur une connexion VPN chiffre les données en transit.
- Stockez le matériel sensible, tels que les clés d'API ou les informations d'identification de base de données, en toute sécurité. Vous pouvez les stocker sous forme de paramètres chiffrés dans Parameter Store, une fonctionnalité d' AWS Systems Manager. Cependant, nous vous recommandons de l'utiliser AWS Secrets Manager car ce service vous permet de faire pivoter automatiquement les secrets, de générer des secrets aléatoires et de partager des secrets entre eux Comptes AWS.
- Pour atténuer le risque de fuite de données provenant de variables d'environnement, nous vous recommandons d'utiliser le pilote CSI AWS Secrets Manager and Config Provider for Secret Store (GitHub). Ce pilote vous permet de faire en sorte que les secrets stockés dans Secrets Manager et les paramètres stockés dans Parameter Store apparaissent sous forme de fichiers montés dans des pods Kubernetes.

> **Note**
>
> AWS Fargate n'est pas pris en charge.

- Si des utilisateurs ou des applications de votre centre de données ou d'un tiers externe sur le Web envoient des demandes d'API HTTPS directes à Services AWS, signez ces demandes à l'aide des informations de sécurité temporaires obtenues auprès de AWS Security Token Service (AWS STS).

Bonnes pratiques de chiffrement pour Amazon EFS

Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le AWS Cloud.

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Dans AWS Config, implémentez la règle efs-encrypted-check AWS gérée. Cette règle vérifie si Amazon EFS est configuré pour chiffrer les données du fichier à l'aide AWS KMS de.
- Appliquez le chiffrement aux systèmes de fichiers Amazon EFS en créant une CloudWatch alarme Amazon qui surveille les CloudTrail journaux pour détecter les `CreateFileSystem` événements

et déclenche une alarme si un système de fichiers non chiffré est créé. Pour plus d'informations, veuillez consulter Walkthrough: Enforcing Encryption on an Amazon EFS File System at Rest.

- Montez le système de fichiers à l'aide de l'assistant de montage EFS. Cela permet de configurer et de gérer un tunnel TLS 1.2 entre le client et le service Amazon EFS et d'acheminer tout le trafic NFS (Network File System) via ce tunnel chiffré. La commande suivante implémente l'utilisation du protocole TLS pour le chiffrement en transit.

```
sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
```

  Pour plus d'informations, veuillez consulter Using EFS mount helper to mount EFS file systems.
- En utilisant AWS PrivateLink et en implémentant des points de terminaison VPC d'interface pour établir une connexion privée entre et VPCs l'API Amazon EFS. Les données en transit via la connexion VPN vers et depuis le point de terminaison sont chiffrées. Pour plus d'informations, veuillez consulter Accédez à un Service AWS à l'aide d'un point de terminaison de VPC d'interface.
- Utilisez la clé de condition `elasticfilesystem:Encrypted` dans les politiques basées sur l'identité IAM pour empêcher les utilisateurs de créer des systèmes de fichiers EFS non chiffrés. Pour plus d'informations, veuillez consulter Using IAM to enforce creating encrypted file systems.
- Les clés KMS utilisées pour le chiffrement EFS doivent être configurées pour un accès sur la base du moindre privilège en utilisant des politiques de clé basées sur les ressources.
- Utilisez la clé de condition `aws:SecureTransport` dans la politique du système de fichiers EFS pour imposer l'utilisation du protocole TLS pour les clients NFS lors de la connexion à un système de fichiers EFS. Pour plus d'informations, consultez Chiffrement des données en transit dans Encrypting File Data with Amazon Elastic File System (AWS livre blanc).

Bonnes pratiques de chiffrement pour Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes. Dans Kubernetes, les secrets vous aident à gérer des informations sensibles, telles que les certificats utilisateur, les mots de passe ou les clés d'API. Par défaut, ces secrets sont stockés non chiffrés dans l'entrepôt de données sous-jacent du serveur d'API, appelé etcd. Sur Amazon EKS, les volumes Amazon Elastic Block Store (Amazon EBS) `etcd` pour les nœuds sont chiffrés avec le chiffrement Amazon EBS. Tout utilisateur disposant d'un accès à une API ou d'un accès à `etcd` peut récupérer ou modifier un secret. En outre, toute personne autorisée à créer un pod dans un espace de noms peut utiliser cet accès pour lire n'importe quel secret dans cet espace de noms. Vous pouvez chiffrer

ces secrets au repos dans Amazon EKS à l'aide AWS KMS keys de clés gérées ou de clés AWS gérées par le client. Une autre approche consiste à utiliser `etcd` AWS Secrets and Config Provider (ASCP) (GitHub référentiel). ASCP s'intègre aux politiques IAM et basées sur les ressources pour limiter et restreindre l'accès aux secrets uniquement au sein de pods Kubernetes spécifiques au sein d'un cluster.

Vous pouvez utiliser les services de AWS stockage suivants avec Kubernetes :

- Pour Amazon EBS, vous pouvez utiliser le pilote de stockage intégré ou le pilote Amazon EBS CSI. Ils incluent tous deux des paramètres permettant de chiffrer les volumes et de fournir une clé gérée par le client.
- Pour Amazon Elastic File System (Amazon EFS), vous pouvez utiliser le pilote CSI Amazon EFS avec prise en charge de l'allocation dynamique et statique.

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Si vous utilisez `etcd`, qui stocke les objets secrets non chiffrés par défaut, procédez comme suit pour protéger les secrets :
  - Encrypt secret data at rest (documentation Kubernetes).
  - AWS KMS À utiliser pour le chiffrement des enveloppes des secrets Kubernetes. Cela vous permet de chiffrer vos secrets avec une clé de données unique. Vous pouvez utiliser une AWS KMS clé de chiffrement pour chiffrer la clé de données. Vous pouvez automatiquement faire pivoter la clé de chiffrement selon un calendrier récurrent. Avec le AWS KMS plugin pour Kubernetes, tous les secrets de Kubernetes sont stockés sous forme de texte chiffré. `etcd` Ils ne peuvent être déchiffrés que par le serveur d'API Kubernetes. Pour plus d'informations, consultez Utiliser le support du fournisseur de chiffrement Amazon EKS pour une défense approfondie et Chiffrer les secrets Kubernetes sur des AWS KMS clusters existants.
  - Activez ou spécifiez l'autorisation via des règles de contrôle d'accès basé sur les rôles (RBAC) qui limitent la lecture et l'écriture du secret. Limitez les autorisations pour créer des secrets ou remplacer des secrets existants. Pour plus d'informations, veuillez consulter Authorization overview (documentation Kubernetes).
  - Si vous définissez plusieurs conteneurs dans un pod et qu'un seul de ces conteneurs a besoin d'accéder à un secret, définissez le montage du volume afin que les autres conteneurs n'aient pas accès à ce secret. Les secrets montés en tant que volumes sont instanciés en tant que volumes `tmpfs` et sont automatiquement retirés du nœud lorsque le pod est supprimé. Vous pouvez également utiliser des variables d'environnement, mais nous ne recommandons pas

cette approche, car les valeurs des variables d'environnement peuvent apparaître dans les journaux. Pour plus d'informations, veuillez consulter Secrets (documentation Kubernetes).

- Dans la mesure du possible, évitez d'accorder l'accès aux demandes `watch` et `list` pour des secrets dans un espace de noms. Dans l'API Kubernetes, ces demandes sont performantes, car elles permettent au client d'inspecter les valeurs de chaque secret de cet espace de noms.
- Autorisez uniquement les administrateurs du cluster à accéder à `etcd`, y compris l'accès en lecture seule.
- S'il existe plusieurs instances `etcd`, assurez-vous qu'`etcd` utilise le protocole TLS pour la communication entre pairs `etcd`.

- Si vous utilisez le protocole ASCP, procédez comme suit pour protéger les secrets :
  - Utilisez des rôles IAM pour les comptes de service pour limiter l'accès au secret aux seuls pods autorisés.
  - Activez le chiffrement des secrets Kubernetes en utilisant le fournisseur de AWS chiffrement (GitHub référentiel) pour implémenter le chiffrement des enveloppes avec une clé KMS gérée par le client.
- Créez un filtre de CloudWatch métriques Amazon et une alarme pour envoyer des alertes pour les opérations spécifiées par l'administrateur, telles que la suppression secrète ou l'utilisation d'une version secrète pendant la période d'attente avant la suppression. Pour plus d'informations, veuillez consulter Creating an alarm based on anomaly detection.

Bonnes pratiques de chiffrement pour AWS Encryption SDK

L'AWS Encryption SDK est une bibliothèque de chiffrement côté client open source. Il utilise les normes du secteur et les meilleures pratiques pour prendre en charge la mise en œuvre et l'interopérabilité dans plusieurs langages de programmation. AWS Encryption SDK chiffre les données à l'aide d'un algorithme de clé symétrique sécurisé et authentifié et propose une implémentation par défaut conforme aux meilleures pratiques de cryptographie. Pour plus d'informations, veuillez consulter Supported algorithm suites in the AWS Encryption SDK.

L'une des principales caractéristiques du AWS Encryption SDK est la prise en charge du chiffrement des données en cours d'utilisation. En adoptant une encrypt-then-use approche, vous pouvez chiffrer les données sensibles avant qu'elles ne soient traitées par la logique de votre application. Cela permet de protéger les données contre toute exposition ou altération potentielle, même si l'application elle-même est affectée par un événement de sécurité.

Tenez compte des bonnes pratiques suivantes pour ce service :

- Respectez toutes les recommandations de Best practices for the AWS Encryption SDK.
- Sélectionnez une ou plusieurs clés d'encapsulage pour protéger vos clés de données. Pour plus d'informations, veuillez consulter Select wrapping keys.
- Transmettez le `KeyId` paramètre à l'ReEncryptopération pour empêcher l'utilisation d'une clé KMS non fiable. Pour plus d'informations, voir Chiffrement amélioré côté client : engagement explicite KeyIds et clé (article de AWS blog).
- Lorsque vous utilisez le AWS Encryption SDK with AWS KMS, utilisez le `KeyId` filtrage local. Pour plus d'informations, voir Chiffrement amélioré côté client : engagement explicite KeyIds et clé (article de AWS blog).
- Pour les applications dont le trafic nécessite un chiffrement ou un déchiffrement importants, ou si votre compte dépasse les quotas de AWS KMS demandes, vous pouvez utiliser la fonction de mise en cache des clés de données du. AWS Encryption SDK Notez les bonnes pratiques suivantes pour la mise en cache des clés de données :
  - Configurez des seuils de sécurité du cache pour limiter la durée d'utilisation de chaque clé de données mise en cache et la quantité de données protégée par chaque clé de données. Pour obtenir des recommandations concernant la configuration de ces seuils, veuillez consulter Setting cache security thresholds.
  - Limitez le cache local au plus petit nombre de clés de données nécessaires pour améliorer les performances de votre cas d'utilisation d'application spécifique. Pour obtenir des instructions et un exemple de configuration des limites pour le cache local, voir Utilisation de la mise en cache des clés de données : Step-by-step.

  Pour plus d'informations, voir AWS Encryption SDK: Comment déterminer si la mise en cache des clés de données convient à votre application (article de AWS blog).

Bonnes pratiques de chiffrement pour AWS Key Management Service

AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données. AWS KMS s'intègre à la plupart des autres systèmes Services AWS capables de chiffrer vos données. Pour une liste complète, voir Services AWS intégré à AWS KMS. AWS KMS s'intègre également AWS CloudTrail pour enregistrer l'utilisation de vos clés KMS à des fins d'audit, de réglementation et de conformité.

Les clés KMS constituent la ressource principale et sont des représentations logiques d'une clé cryptographique. AWS KMS Il existe trois principaux types de clés KMS :

- Les clés KMS que vous créez sont des clés gérées par le client.
- AWS les clés gérées sont des clés KMS Services AWS créées dans votre compte, en votre nom.
- AWS les clés détenues sont des clés KMS qu'un Service AWS utilisateur possède et gère, destinées à être utilisées dans plusieurs applications Comptes AWS.

Pour plus d'informations sur ces types de clés, veuillez consulter Clés de client et clés AWS.

Dans le AWS Cloud, les politiques sont utilisées pour contrôler qui peut accéder aux ressources et aux services. Par exemple, dans AWS Identity and Access Management (IAM), les politiques basées sur l'identité définissent les autorisations pour les utilisateurs, les groupes d'utilisateurs ou les rôles, et les politiques basées sur les ressources s'attachent à une ressource, telle qu'un compartiment S3, et définissent les principaux auxquels l'accès est autorisé, les actions prises en charge et toute autre condition qui doit être remplie. À l'instar des politiques IAM, AWS KMS utilise des politiques clés pour contrôler l'accès à une clé KMS. Chaque clé KMS doit avoir une politique de clé et chaque clé ne peut avoir qu'une seule politique de clé. Lorsque vous définissez des politiques autorisant ou refusant l'accès aux clés KMS, tenez compte des points suivants :

- Vous pouvez contrôler la politique clé pour les clés gérées par le client, mais vous ne pouvez pas contrôler directement la politique clé pour les clés AWS gérées ou pour les clés AWS détenues.
- Les politiques clés permettent d'accorder un accès granulaire aux appels d' AWS KMS API au sein d'un Compte AWS. À moins que la politique de clé ne l'autorise explicitement, vous ne pouvez pas utiliser de politiques IAM pour autoriser l'accès à une clé KMS. Sans autorisation de la politique de clé, les politiques IAM qui octroient des autorisations n'ont aucun effet. Pour plus d'informations, veuillez consulter Autorise l'accès au Compte AWS et active les politiques IAM.
- Vous pouvez utiliser une politique IAM pour refuser l'accès à une clé gérée par le client sans l'autorisation correspondante de la politique de clé.
- Lors de la conception de politiques de clé et de politiques IAM pour les clés multi-région, tenez compte de ce qui suit :
  - Les politiques de clé ne sont pas des propriétés partagées des clés multi-région et ne sont pas copiées ou synchronisées entre les clés multi-région associées.

- Lorsqu'une clé multi-région est créée à l'aide des actions `CreateKey` et `ReplicateKey`, la politique de clé par défaut est appliquée, sauf si une politique de clé est spécifiée dans la demande.
- Vous pouvez implémenter des clés de condition, telles que aws : RequestedRegion, pour limiter les autorisations à une personne en particulier Région AWS.
- Vous pouvez utiliser des octrois pour autoriser des autorisations sur une clé principale ou une clé de réplica multi-région. Toutefois, vous ne pouvez pas utiliser un seul octroi pour autoriser des autorisations sur plusieurs clés KMS, même s'il s'agit de clés multi-région associées.

Lorsque vous utilisez AWS KMS et créez des politiques clés, tenez compte des meilleures pratiques de chiffrement et autres bonnes pratiques de sécurité suivantes :

- Respectez les recommandations des ressources suivantes pour connaître les AWS KMS meilleures pratiques :
  - Bonnes pratiques en matière de AWS KMS subventions (AWS KMS documentation)
  - Best practices for IAM policies (documentation AWS KMS)
- Conformément aux bonnes pratiques en matière de séparation des tâches, maintenez des identités distinctes pour ceux qui administrent les clés et ceux qui les utilisent :
  - Les rôles d'administrateur qui créent et suppriment des clés ne doivent pas être autorisés à utiliser la clé.
  - Certains services peuvent uniquement avoir besoin de chiffrer les données et ne devraient pas être autorisés à les déchiffrer à l'aide de la clé.
- Les politiques de clé devraient toujours suivre le modèle du moindre privilège. N'utilisez pas `kms:*` pour les actions dans des politiques IAM ou des politiques de clé, car cela donne aux principaux les autorisations nécessaires à la fois pour administrer et utiliser la clé.
- Limitez l'utilisation des clés gérées Services AWS par le client à des éléments spécifiques en utilisant la clé de ViaService condition kms : dans le cadre de la politique des clés.
- Si vous avez le choix entre plusieurs types de clé, les clés gérées par le client sont préférables, car elles fournissent les options de contrôle les plus détaillées, dont les suivantes :
  - Gestion des authentifications et des contrôles d'accès
  - Activation et désactivation des clés
  - Rotation des AWS KMS keys
  - Clés de balisage

  - Création d'alias
  - Suppression d' AWS KMS keys
- AWS KMS les autorisations d'administration et de modification doivent être explicitement refusées aux principaux non approuvés et les autorisations de AWS KMS modification ne doivent pas exister dans une instruction d'autorisation pour les principaux non autorisés. Pour de plus amples informations, consultez Actions, ressources et clés de condition pour AWS Key Management Service
- Afin de détecter toute utilisation non autorisée des clés KMS AWS Config, implémentez les règles iam-customer-policy-blocked-kms-actions et iam-inline-policy-blocked -kms-actions. Cela empêche les principaux d'utiliser les actions de AWS KMS déchiffrement sur toutes les ressources.
- Mettez en œuvre des politiques de contrôle des services (SCPs) AWS Organizations pour empêcher les utilisateurs ou les rôles non autorisés de supprimer des clés KMS, soit directement sous forme de commande, soit via la console. Pour plus d'informations, voir Utilisation SCPs comme contrôles préventifs (article de AWS blog).
- AWS KMS Consignez les appels d'API dans un CloudTrail journal. Cela permet d'enregistrer les attributs d'événement pertinents, tels que les demandes qui ont été effectuées, l'adresse IP source à partir de laquelle la demande a été faite, ainsi que l'auteur de la demande. Pour plus d'informations, consultez la section Journalisation des appels d' AWS KMS API avec AWS CloudTrail.
- Si vous utilisez un contexte de chiffrement, celui-ci ne doit contenir aucune information sensible. CloudTrail stocke le contexte de chiffrement dans des fichiers JSON en texte brut, qui peuvent être consultés par toute personne ayant accès au compartiment S3 contenant les informations.
- Lorsque vous surveillez l'utilisation des clés gérées par le client, configurez des événements pour vous avertir si des actions spécifiques sont détectées, telles que la création de clés, les mises à jour apportées à des politiques de clés gérées par le client ou l'importation d'éléments de clé. Il est également recommandé de mettre en œuvre des réponses automatisées, telles qu'une fonction AWS Lambda qui désactive la clé ou exécute toute autre action de réponse aux incidents conformément à vos politiques organisationnelles.
- Les clés multi-région sont recommandées pour des scénarios spécifiques, tels que la conformité, la reprise après sinistre ou les sauvegardes. Les propriétés de sécurité des clés multi-région sont très différentes de celles des clés à région unique. Les recommandations suivantes s'appliquent lors de l'autorisation de la création, de la gestion et de l'utilisation de clés multi-région :
  - Autoriser les principaux à répliquer une clé multi-région uniquement dans les Régions AWS qui l'exigent.

- Donnez l'autorisation pour les clés multi-région uniquement aux principaux qui en ont besoin et uniquement pour les tâches qui en ont besoin.

Bonnes pratiques de chiffrement pour AWS Lambda

AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Pour sécuriser vos variables d'environnement, vous pouvez utiliser le chiffrement côté serveur pour protéger vos données au repos, et le chiffrement côté client pour protéger vos données en transit.

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Lambda fournit toujours le chiffrement côté serveur au repos grâce à une AWS KMS key. Par défaut, Lambda utilise une clé AWS gérée. Nous vous recommandons d'utiliser une clé gérée par le client, car vous avez un contrôle total sur la clé, y compris la gestion, la rotation et la vérification.
- Pour les données en transit qui nécessitent un chiffrement, activez les assistants, qui garantissent que les variables d'environnement sont chiffrées côté client pour une meilleure protection pendant le transit avec la clé KMS préférée. Pour plus d'informations, veuillez consulter Sécurité pendant le transit dans Sécurisation des variables d'environnement.
- Les variables d'environnement des fonctions Lambda contenant des données sensibles ou critiques doivent être chiffrées pendant le transit afin de protéger les données transmises de façon dynamique aux fonctions (généralement les informations d'accès) contre tout accès non autorisé.
- Pour empêcher un utilisateur d'afficher des variables d'environnement, ajoutez une instruction aux autorisations de cet utilisateur dans la politique IAM ou la politique de clé qui refuse l'accès à la clé par défaut, à une clé gérée par le client ou à toutes les clés. Pour plus d'informations, consultez Utilisation des variables d'environnement AWS Lambda.

Bonnes pratiques de chiffrement pour Amazon RDS

Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et mettre à l'échelle une base de données relationnelle dans le AWS Cloud. Les données qui sont chiffrées au repos incluent le stockage sous-jacent pour des instances de base de données, les sauvegardes automatisées, les réplicas en lecture et les instantanés.

Voici les approches que vous pouvez utiliser pour chiffrer les données au repos dans les instances de base de données RDS :

- Vous pouvez chiffrer les instances de base de données Amazon RDS à l'aide AWS KMS keys d'une clé AWS gérée ou d'une clé gérée par le client. Pour plus d'informations, consultez AWS Key Management Service dans ce guide.
- Amazon RDS for Oracle et Amazon RDS for SQL Server prennent en charge le chiffrement d'instances de base de données à l'aide du chiffrement TDE (Transparent Data Encryption). Pour plus d'informations, veuillez consulter Oracle Transparent Data Encryption ou Prise en charge de Transparent Data Encryption dans SQL Server.

  Vous pouvez utiliser les clés TDE et KMS pour chiffrer les instances de base de données. Toutefois, cela peut affecter légèrement les performances de votre base de données, et vous devez gérer ces clés séparément.

Voici les approches que vous pouvez utiliser pour chiffrer les données en transit vers ou depuis les instances de base de données RDS :

- Pour une instance de base de données Amazon RDS exécutant MariaDB, Microsoft SQL Server, MySQL, Oracle ou PostgreSQL, vous pouvez utiliser le protocole SSL pour chiffrer la connexion. Pour plus d'informations, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données.
- Amazon RDS for Oracle prend également en charge Oracle Native Network Encryption (NNE), qui chiffre les données lors de leur déplacement vers ou depuis une instance de base de données. Les chiffrements NNE et SSL ne peuvent pas être utilisés simultanément. Pour plus d'informations, consultez Chiffrement du réseau natif Oracle.

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Lorsque vous vous connectez à des instances de base de données Amazon RDS for SQL Server ou Amazon RDS for PostgreSQL afin de traiter, de stocker ou de transmettre des données nécessitant un chiffrement, utilisez la fonctionnalité RDS Transport Encryption pour chiffrer la connexion. Vous pouvez implémenter cela en définissant le paramètre `rds.force_ssl` sur 1 dans le groupe de paramètres. Pour plus d'informations, veuillez consulter Utilisation des groupes de paramètres. Amazon RDS for Oracle utilise le chiffrement de réseau natif de la base de données Oracle.
- Les clés gérées par le client pour le chiffrement d'instances de base de données RDS doivent être utilisées uniquement à cette fin et avec aucun autre Services AWS.

- Avant de chiffrer une instance de base de données RDS, définissez les exigences relatives aux clés KMS. La clé utilisée par l'instance ne peut pas être modifiée ultérieurement. Par exemple, dans votre politique de chiffrement, définissez les normes d'utilisation et de gestion des clés AWS gérées ou des clés gérées par le client, en fonction des besoins de votre entreprise.
- Lorsque vous autorisez l'accès à une clé KMS gérée par le client, respectez le principe du moindre privilège en utilisant des clés de condition dans les politiques IAM. Par exemple, pour autoriser l'utilisation d'une clé gérée par le client uniquement pour les demandes provenant d'Amazon RDS, utilisez la clé de ViaService condition kms : avec la `rds.<region>.amazonaws.com` valeur. En outre, vous pouvez utiliser des clés ou des valeurs dans le contexte de chiffrement Amazon RDS comme condition d'utilisation de la clé gérée par le client.
- Il est vivement recommandé d'activer les sauvegardes pour les instances de base de données RDS chiffrées. Amazon RDS peut perdre l'accès à la clé KMS pour une instance de base de données, comme lorsque la clé n'est pas activée ou lorsque l'accès RDS à une clé KMS est révoqué. Dans ce cas, l'instance de base de données chiffrée passe à un état récupérable pendant sept jours. Si l'instance de base de données ne retrouve pas l'accès à la clé au bout de sept jours, la base de données devient définitivement inaccessible et doit être restaurée à partir d'une sauvegarde. Pour plus d'informations, veuillez consulter Chiffrement d'une instance de base de données.
- Si une réplique en lecture et son instance de base de données cryptée se trouvent dans la même pièce Région AWS, vous devez utiliser la même clé KMS pour chiffrer les deux.
- Dans AWS Config, implémentez la règle rds-storage-encrypted AWS gérée pour valider et appliquer le chiffrement pour les instances de base de données RDS et la rds-snapshots-encryptedrègle pour valider et appliquer le chiffrement pour les instantanés de base de données RDS.
- AWS Security Hub À utiliser pour évaluer si vos ressources Amazon RDS respectent les meilleures pratiques en matière de sécurité. Pour plus d'informations, consultez la section Contrôles du Security Hub pour Amazon RDS.

Bonnes pratiques de chiffrement pour AWS Secrets Manager

AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation. Secrets Manager s'intègre AWS KMS pour chiffrer chaque version de chaque valeur secrète à l'aide d'une clé de données unique protégée par un AWS KMS key. Cette intégration protège les secrets stockés avec des clés de chiffrement qui ne restent jamais AWS KMS

non chiffrées. Vous pouvez également définir des autorisations personnalisées sur la clé KMS afin d'auditer les opérations qui génèrent, chiffrent et déchiffrent les clés de données qui protègent les secrets stockés. Pour plus d'informations, veuillez consulter Chiffrement et déchiffrement de secret dans AWS Secrets Manager.

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Dans la plupart des cas, nous recommandons d'utiliser la clé `aws/secretsmanager` AWS gérée pour chiffrer les secrets. Son utilisation est gratuite.
- Pour accéder à un secret depuis un autre compte ou pour appliquer une politique de clé à la clé de chiffrement, utilisez une clé gérée par le client pour chiffrer le secret.
  - Dans la politique clé, attribuez la valeur `secretsmanager.<region>.amazonaws.com` à la clé de ViaService condition kms :. Cela limite l'utilisation de la clé aux seules demandes provenant de Secrets Manager.
  - Pour limiter davantage l'utilisation de la clé aux seules demandes émanant de Secrets Manager présentant le contexte approprié, utilisez des clés ou des valeurs dans le contexte de chiffrement de Secrets Manager comme condition d'utilisation de la clé KMS en créant :
    - Un opérateur de condition de chaîne dans une politique IAM ou une politique clé
    - Une contrainte d'octroi dans un octroi

Bonnes pratiques de chiffrement pour Amazon S3

Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Pour le chiffrement côté serveur dans Amazon S3, il existe trois options :

- Chiffrement côté serveur avec clés de chiffrement gérées par Amazon S3 (SSE-S3)
- Chiffrement côté serveur avec AWS Key Management Service (SSE-KMS)
- Chiffrement côté serveur à l'aide des clés de chiffrement fournies par le client (SSE-C)

Amazon S3 applique le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) comme niveau de chiffrement de base pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d’objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état de chiffrement automatique pour la

configuration de chiffrement par défaut du compartiment S3 et pour les téléchargements de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans les AWS Command Line Interface (AWS CLI) et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Si le chiffrement côté serveur est utilisé pour chiffrer un objet au moment du chargement, ajoutez l'en-tête `x-amz-server-side-encryption` à la demande pour indiquer à Amazon S3 de chiffrer l'objet à l'aide de SSE-S3, SSE-KMS ou SSE-C. Les valeurs possibles pour l'en-tête `x-amz-server-side-encryption` sont les suivantes :

- `AES256`, qui indique à Amazon S3 d'utiliser les clés gérées par Amazon S3.
- `aws:kms`, qui indique à Amazon S3 d'utiliser des clés AWS KMS gérées.
- Définition de la valeur sur `True` ou `False` pour SSE-C

Pour plus d'informations, consultez l'Defense-in-depth exigence 1 : les données doivent être chiffrées au repos et pendant le transit dans Comment utiliser les politiques relatives Defense-in-Depth aux compartiments et les appliquer pour sécuriser vos données Amazon S3 (article de AWS blog).

Pour le chiffrement côté client dans Amazon S3, il existe deux options :

- Une clé stockée dans AWS KMS
- Une clé stockée dans l'application

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Dans AWS Config, implémentez la règle AWS gérée bucket-server-side-encryptioncompatible s3 pour valider et appliquer le chiffrement des compartiments S3.
- Déployez une politique de compartiment Amazon S3 qui confirme que tous les objets chargés sont chiffrés à l'aide de la condition `s3:x-amz-server-side-encryption`. Pour plus d'informations, veuillez consulter l'exemple de politique de compartiment dans Protection des données dans SSE-S3 et les instructions dans Ajout d'une politique de compartiment.
- Autorisez uniquement les connexions chiffrées sur HTTPS (TLS) avec la condition `aws:SecureTransport` sur les politiques de compartiment S3. Pour plus d'informations, consultez Quelle politique de compartiment S3 dois-je utiliser pour me conformer à la AWS Config règle s3- bucket-ssl-requests-only ?

- Dans AWS Config, implémentez la règle bucket-ssl-requests-only AWS gérée par s3 pour obliger les demandes à utiliser le protocole SSL.
- Utilisez une clé gérée par le client si vous devez accorder un accès intercompte à vos objets Amazon S3. Configurez la politique de clé pour autoriser l'accès depuis un autre Compte AWS.

Bonnes pratiques de chiffrement pour Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Tenez compte des bonnes pratiques de chiffrement suivantes pour ce service :

- Chiffrez le trafic entre les actifs d'information et les systèmes au sein du réseau de l'entreprise en VPCs utilisant l'une des méthodes suivantes :
  - AWS Site-to-Site VPN connexions
  - Une combinaison de AWS Direct Connect connexions AWS Site-to-Site VPN et, qui fournit une IPsec connexion privée cryptée
  - AWS Direct Connect connexions prenant en charge la sécurité MAC (MACsec) pour crypter les données des réseaux d'entreprise vers le site AWS Direct Connect
- Utilisez les points de terminaison VPC pour vous VPCs connecter en privé AWS PrivateLink à ceux pris en charge Services AWS sans utiliser de passerelle Internet. Vous pouvez utiliser AWS Direct Connect nos AWS VPN services pour établir cette connexion. Le trafic entre votre VPC et l'autre service ne quitte pas le AWS réseau. Pour plus d'informations, consultez la section Accès Services AWS via AWS PrivateLink.
- Configurez des règles du groupe de sécurité qui autorisent le trafic uniquement à partir de ports associés à des protocoles sécurisés, tels que HTTPS sur TCP/443. Vérifiez régulièrement les groupes de sécurité et leurs règles.

Ressources

- Création d'une stratégie de chiffrement d'entreprise pour les données au repos (directives AWS prescriptives)
- Bonnes pratiques de sécurité pour AWS Key Management Service (AWS KMS documentation)
- Mode Services AWS d'utilisation AWS KMS (AWS KMS documentation)
- Pilier de sécurité : protection des données (AWS Well-Architected Framework)

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Mises à jour d'Amazon EKS	Nous avons mis à jour les meilleures pratiques en matière de chiffrement pour Amazon Elastic Kubernetes Service (Amazon EKS).	7 janvier 2025
Mises à jour de Secrets Manager	Nous avons mis à jour les informations et les recommandations pour AWS Secrets Manager.	9 septembre 2024
Service AWS mises à jour	Nous avons mis à jour les informations et les recommandations pour Amazon EKS AWS Encryption SDK, Amazon Relational Database Service (Amazon RDS) et Amazon Simple Storage Service (Amazon S3).	4 septembre 2024
Publication initiale	—	2 décembre 2022

AWS Glossaire des directives prescriptives

Les termes suivants sont couramment utilisés dans les stratégies, les guides et les modèles fournis par les directives AWS prescriptives. 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 l'édition compatible avec Amazon Aurora 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) pour Oracle dans le. AWS Cloud
- 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 locale vers Oracle sur une EC2 instance du AWS Cloud.
- 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. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers 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 son AIOps utilisation dans la stratégie de AWS migration, consultez 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, consultez ABAC pour 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

Un emplacement distinct au sein d'un Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, 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, la 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 Cadre de qualification de la charge de travail (AWS WQF)

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le 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

mauvais bot

Un bot destiné à perturber ou à nuire à des individus ou à des organisations.

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.

déploiement bleu/vert

Stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Vous exécutez la version actuelle de l'application dans un environnement (bleu) et la nouvelle version de l'application dans l'autre environnement (vert). Cette stratégie vous permet de revenir rapidement en arrière avec un impact minimal.

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, appelés « bots malveillants », sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

Réseaux de robots infectés par des logiciels malveillants et contrôlés par une seule entité, connue sous le nom d'herder ou d'opérateur de bots. Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact.

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-Architected AWS .

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.

déploiement de Canary

Diffusion lente et progressive d'une version pour les utilisateurs finaux. Lorsque vous êtes sûr, vous déployez la nouvelle version et remplacez la version actuelle dans son intégralité.

CCo E

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 localement, avant que la cible ne les Service AWS reçoive.

Centre d'excellence du 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, consultez les CCoarticles électroniques du blog sur la stratégie AWS Cloud d'entreprise.

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 entreprises traversent généralement lorsqu'elles migrent vers AWS Cloud :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour accélérer votre adoption du cloud (par exemple, créer une zone de landing zone, définir un CCo E, établir 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 publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le guide de préparation à la migration.

CMDB

Voir base de données de gestion de configuration.

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 ouBitbucket Cloud. 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 (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, Amazon SageMaker AI fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

Pour une charge de travail, une modification de configuration par rapport à l'état attendu. Cela peut entraîner une non-conformité de la charge de travail, et cela est généralement progressif et involontaire.

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

Ensemble de AWS Config règles et d'actions correctives que vous pouvez assembler pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans une région Compte AWS et, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, consultez la section Packs de conformité dans la AWS Config documentation.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD is commonly described as a pipeline. CI/CDpeut 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.

CV

Voir vision par ordinateur.

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 AWS Well-Architected Framework. 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.

maillage de données

Un cadre architectural qui fournit une propriété des données distribuée et décentralisée avec une gestion et une gouvernance centralisées.

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 des 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 AWS, vous ajoutez plusieurs contrôles à différentes couches de

la AWS Organizations structure afin de sécuriser 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 AWS membre 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.

EDI

Voir échange de données informatisé.

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.

échange de données informatisé (EDI)

L'échange automatique de documents commerciaux entre les organisations. Pour plus d'informations, voir Qu'est-ce que l'échange de données informatisé ?

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 à AWS Identity and Access Management (IAM) principaux. 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).

planification des ressources d'entreprise (ERP)

Système qui automatise et gère les principaux processus métier (tels que la comptabilité, le MES et la gestion de projet) pour une entreprise.

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section Chiffrement des enveloppes 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.

époppée

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 points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, 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.

ERP

Voir Planification des ressources d'entreprise.

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 le AWS Cloud, une limite telle qu'une zone de disponibilité Région 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.

invitation en quelques coups

Fournir à un LLM un petit nombre d'exemples illustrant la tâche et le résultat souhaité avant de lui demander d'effectuer une tâche similaire. Cette technique est une application de l'apprentissage contextuel, dans le cadre de laquelle les modèles apprennent à partir d'exemples (prises de vue) intégrés dans des instructions. Les instructions en quelques clics peuvent être efficaces pour les tâches qui nécessitent un formatage, un raisonnement ou des connaissances de domaine spécifiques. Voir également l'invite Zero-Shot.

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.

FM

Voir le modèle de fondation.

modèle de fondation (FM)

Un vaste réseau neuronal d'apprentissage profond qui s'est entraîné sur d'énormes ensembles de données généralisées et non étiquetées. FMs sont capables d'effectuer une grande variété de tâches générales, telles que comprendre le langage, générer du texte et des images et converser en langage naturel. Pour plus d'informations, voir Que sont les modèles de base ?

G

IA générative

Sous-ensemble de modèles d'IA qui ont été entraînés sur de grandes quantités de données et qui peuvent utiliser une simple invite textuelle pour créer de nouveaux contenus et artefacts, tels que des images, des vidéos, du texte et du son. Pour plus d'informations, consultez Qu'est-ce que l'IA générative.

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.

image dorée

Un instantané d'un système ou d'un logiciel utilisé comme modèle pour déployer de nouvelles instances de ce système ou logiciel. Par exemple, dans le secteur de la fabrication, une image dorée peut être utilisée pour fournir des logiciels sur plusieurs appareils et contribue à améliorer la vitesse, l'évolutivité et la productivité des opérations de fabrication des appareils.

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 organisationnelles (OUs). 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 GuardDuty AWS 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.

données de rétention

Partie de données historiques étiquetées qui n'est pas divulguée dans un ensemble de données utilisé pour entraîner un modèle d'apprentissage automatique. Vous pouvez utiliser les données de blocage pour évaluer les performances du modèle en comparant les prévisions du modèle aux données de blocage.

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' AWS Cloud environnement.

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.

IIo T

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 AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes

et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'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.

Industry 4.0

Terme introduit par Klaus Schwab en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

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, voir Élaboration d'une stratégie de transformation numérique de l'Internet des objets (IIoT) industriel.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau

avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'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, voir Interprétabilité du modèle d'apprentissage automatique avec 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 d'atterrissage est un AWS environnement multi-comptes bien conçu, 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.

grand modèle de langage (LLM)

Un modèle d'intelligence artificielle basé sur le deep learning qui est préentraîné sur une grande quantité de données. Un LLM peut effectuer plusieurs tâches, telles que répondre à des questions, résumer des documents, traduire du texte dans d'autres langues et compléter des phrases. Pour plus d'informations, voir Que sont LLMs.

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.

LLM

Voir le grand modèle de langage.

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.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

Services AWS pour lequel AWS fonctionnent 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.

système d'exécution de la fabrication (MES)

Un système logiciel pour le suivi, la surveillance, la documentation et le contrôle des processus de production qui convertissent les matières premières en produits finis dans l'atelier.

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, à l' Comptes AWS exception du 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.

MAILLES

Voir le système d'exécution de la fabrication.

Transport télémétrique en file d'attente de messages (MQTT)

Protocole de communication léger machine-to-machine (M2M), basé sur le modèle de publication/d'abonnement, pour les appareils IoT aux ressources limitées.

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs 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, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

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 en utilisant Lightweight. APIs 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, consultez la section Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

Un AWS programme qui fournit un support de conseil, des formations et des services pour aider les entreprises à établir 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 des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des 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 AWS compte.

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 : réorganisez la migration vers Amazon EC2 avec le service de migration AWS d'applications.

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. AWS Cloud 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 disponible gratuitement pour tous les AWS consultants et consultants APN Partner.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une organisation au cloud, à identifier les forces et les faiblesses et à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide du 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

L'approche utilisée pour migrer une charge de travail vers le AWS Cloud. 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.

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, consultez la section Stratégie de modernisation des applications dans le 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, consultez la section Évaluation de l'état de préparation à la modernisation des applications dans le 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.

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

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.

OPC-UA

Voir Open Process Communications - Architecture unifiée.

Communications par processus ouvert - Architecture unifiée (OPC-UA)

Un protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle. L'OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

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, évaluer, prévenir ou réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

Systèmes matériels et logiciels qui fonctionnent avec l'environnement physique pour contrôler les opérations, les équipements et les infrastructures industriels. Dans le secteur manufacturier, l'intégration des systèmes OT et des technologies de l'information (IT) est au cœur des transformations de l'industrie 4.0.

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

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'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 AWS migration, ce cadre est appelé accélération du personnel, 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). L'OAC prend en charge tous les compartiments S3 dans leur ensemble Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les requêtes dynamiques `PUT` adressées au compartiment S3. `DELETE`

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.

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'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.

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

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

Entité capable d'effectuer AWS des actions et d'accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS 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 d'ingénierie système qui prend en compte la confidentialité tout au long du processus de développement.

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs

VPCs domaines. 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.

gestion du cycle de vie des produits (PLM)

Gestion des données et des processus d'un produit tout au long de son cycle de vie, depuis la conception, le développement et le lancement, en passant par la croissance et la maturité, jusqu'au déclin et au retrait.

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

Dans le secteur manufacturier, un ordinateur hautement fiable et adaptable qui surveille les machines et automatise les processus de fabrication.

chaînage rapide

Utiliser le résultat d'une invite LLM comme entrée pour l'invite suivante afin de générer de meilleures réponses. Cette technique est utilisée pour décomposer une tâche complexe en sous-tâches ou pour affiner ou développer de manière itérative une réponse préliminaire. Cela permet d'améliorer la précision et la pertinence des réponses d'un modèle et permet d'obtenir des résultats plus précis et personnalisés.

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.

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices

peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

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).

CHIFFON

Voir Retrieval Augmented Generation.

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. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise 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

Un ensemble de AWS ressources dans une zone géographique. Chacun Région AWS est isolé et indépendant des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir Spécifier ce que Régions AWS votre compte peut utiliser.

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.

résilience

La capacité d'une application à résister aux perturbations ou à s'en remettre. La haute disponibilité et la reprise après sinistre sont des considérations courantes lors de la planification de la résilience dans le AWS Cloud. Pour plus d'informations, consultez la section AWS Cloud Résilience.

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.

Génération augmentée de récupération (RAG)

Technologie d'IA générative dans laquelle un LLM fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une

réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir Qu'est-ce que RAG ?

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 permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre 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.

SCADA

Voir Contrôle de supervision et acquisition de données.

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, voir Que contient le secret d'un Secrets Manager ? dans la documentation de Secrets Manager.

sécurité dès la conception

Une approche d'ingénierie système qui prend en compte la sécurité tout au long du processus de développement.

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 EC2 instance Amazon ou la rotation des informations d'identification.

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

Politique qui fournit un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPs définissez des garde-fous ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez les utiliser SCPs comme listes d'autorisation ou de refus pour spécifier les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

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

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors 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.

contrôle de supervision et acquisition de données (SCADA)

Dans le secteur manufacturier, un système qui utilise du matériel et des logiciels pour surveiller les actifs physiques et les opérations de production.

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.

invite du système

Technique permettant de fournir un contexte, des instructions ou des directives à un LLM afin d'orienter son comportement. Les instructions du système aident à définir le contexte et à établir des règles pour les interactions avec les utilisateurs.

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

Un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations, voir Qu'est-ce qu'une passerelle de transit dans la AWS Transit Gateway documentation.

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

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation 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, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

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

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des 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

Voir le cadre AWS de qualification de la charge de travail.

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.

invite Zero-Shot

Fournir à un LLM des instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. Le LLM doit utiliser ses connaissances pré-entraînées pour gérer la tâche. L'efficacité de l'invite zéro dépend de la complexité de la tâche et de la qualité de l'invite. Voir également les instructions en quelques clics.

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.