Contrôles de sécurité recommandés pour la mise en œuvre des AWS capacités de sécurité des CAF

AWS Directives prescriptives

AWS Directives prescriptives: Contrôles de sécurité recommandés pour la mise en œuvre des AWS capacités de sécurité des CAF

Table of Contents

Contrôles de sécurité recommandés pour la mise en œuvre des AWS capacités de sécurité des CAF

Rishi Singla et Rovan Omar, Amazon Web Services ()AWS

Novembre 2023 (historique du document)

La sécurité est la priorité absolue de AWS. Pour alléger votre charge opérationnelle, vous partagez la responsabilité de la sécurité du cloud et de la conformité avec AWS. AWS est responsable de la sécurité du cloud, c'est-à-dire de la protection de l'infrastructure qui exécute les services proposés dans le AWS Cloud. Vous êtes responsable de la sécurité dans le cloud, notamment de vos données et de vos applications. Ce guide fournit des contrôles de sécurité qui peuvent vous aider à vous acquitter de vos responsabilités en matière de sécurité dans le AWS Cloud.

Le cadre d'adoption du AWS cloud (AWS CAF) fournit les meilleures pratiques conçues pour améliorer votre préparation au cloud. AWS La CAF classe ces meilleures pratiques en six points de vue : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Ce guide met l'accent sur les fonctionnalités suivantes du point de vue de la sécurité :

- Gestion des identités et des accès — Gérez les identités humaines et machines ainsi que leurs autorisations à grande échelle.
- Détection des menaces : configurez la journalisation et la surveillance pour détecter et étudier une éventuelle erreur de configuration de sécurité, une menace ou un comportement inattendu.
- Protection de l'infrastructure : protégez les systèmes et les services contre les accès involontaires ou non autorisés et les vulnérabilités potentielles.
- Protection des données : catégorisez les données en fonction de leur niveau de sensibilité. Maintenez la visibilité et le contrôle des données et de la manière dont elles sont consultées et utilisées dans votre organisation.
- Réponse aux incidents — Établissez des mécanismes pour répondre aux incidents de sécurité et atténuer leur impact potentiel.

Le fait de ne pas mettre en œuvre des contrôles de sécurité préventifs, détectifs et réactifs pour ces fonctionnalités de sécurité AWS CAF peut constituer un risque critique pour votre environnement cloud et perturber votre activité. La mise en œuvre des contrôles de sécurité décrits dans ce guide peut aider votre entreprise à protéger son environnement cloud.

> **Note**
>
> AWS fournit des services, des outils et des cadres qui peuvent vous aider à opérer en toute sécurité dans le AWS Cloud. Ce guide s'aligne sur le AWS Well-Architected Framework AWS , le Cloud Adoption Framework AWS (CAF), l'architecture de référence de sécuritéAWS (SRA) et AWS les autres recommandations de sécurité publiées par. AWS Les contrôles présentés dans ce guide ne tiennent pas compte de toutes les considérations relatives à la sécurité du cloud, et ce guide n'est pas destiné à remplacer ces frameworks.

Recommandations de contrôle de sécurité pour la gestion des identités et des accès

Vous pouvez créer des identités dans AWS ou vous connecter à une source d'identité externe. Grâce aux politiques AWS Identity and Access Management (IAM), vous accordez aux utilisateurs les autorisations nécessaires pour qu'ils puissent accéder aux AWS ressources et aux applications intégrées ou les gérer. Une gestion efficace des identités et des accès permet de s'assurer que les bonnes personnes et les bonnes machines ont accès aux bonnes ressources dans les bonnes conditions. Le AWS Well-Architected Framework fournit les meilleures pratiques pour gérer les identités et leurs autorisations. Parmi les meilleures pratiques, citons le recours à un fournisseur d'identité centralisé et l'utilisation de mécanismes de connexion robustes, tels que l'authentification multifactorielle (MFA). Les contrôles de sécurité présentés dans cette section peuvent vous aider à mettre en œuvre ces meilleures pratiques.

Contrôles de cette section :

- Surveiller et configurer les notifications relatives à l'activité de l'utilisateur root
- Ne créer aucune clé d'accès pour l'utilisateur root
- Activer le MFA pour l'utilisateur root
- Suivez les meilleures pratiques de sécurité pour IAM
- Accorder des autorisations de moindre privilège
- Définissez des barrières d'autorisation au niveau de la charge de travail
- Faites pivoter les clés d'accès IAM à intervalles réguliers
- Identifier les ressources partagées avec une entité externe

Surveiller et configurer les notifications relatives à l'activité de l'utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique appelée utilisateur root. Par défaut, l'utilisateur root dispose d'un accès complet à toutes Services AWS les ressources du compte. Vous devez contrôler et surveiller étroitement l'utilisateur root, et vous ne devez l'utiliser que pour les tâches qui nécessitent des informations d'identification de l'utilisateur root.

Pour plus d'informations, consultez les ressources suivantes :

- Accordez un accès avec le moindre privilège dans le Well-Architected AWS Framework
- Surveillez l'activité de l'utilisateur root IAM dans les directives AWS prescriptives

Ne créer aucune clé d'accès pour l'utilisateur root

L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La désactivation de l'accès programmatique à l'utilisateur root permet de réduire le risque d'exposition accidentelle des informations d'identification de l'utilisateur et de compromission ultérieure de l'environnement cloud. Nous vous recommandons de créer et d'utiliser des rôles IAM comme informations d'identification temporaires pour accéder à vos ressources Comptes AWS et à vos ressources.

Pour plus d'informations, consultez les ressources suivantes :

- La clé d'accès de l'utilisateur root IAM ne doit pas exister dans la documentation AWS Security Hub
- Suppression des clés d'accès pour l'utilisateur root dans la documentation IAM
- Rôles IAM dans la documentation IAM

Activer le MFA pour l'utilisateur root

Nous vous recommandons d'activer plusieurs dispositifs d'authentification multifactorielle (MFA) pour Compte AWS l'utilisateur root et les utilisateurs IAM. Cela augmente la barre de sécurité Comptes AWS et peut simplifier la gestion des accès. Étant donné qu'un utilisateur root est un utilisateur hautement privilégié qui peut effectuer des actions privilégiées, il est essentiel d'exiger l'authentification MFA pour l'utilisateur root. Vous pouvez utiliser un dispositif MFA matériel qui génère un code numérique basé sur l'algorithme TOTP (mot de passe à usage unique) basé sur le temps, une clé de sécurité matérielle FIDO ou une application d'authentification virtuelle.

En 2024, la MFA sera requise pour accéder à l'utilisateur root de n'importe quel utilisateur. Compte AWS Pour plus d'informations, consultez Secure by Design : AWS pour améliorer les exigences en matière de MFA en 2024 dans le blog sur la AWS sécurité. Nous vous encourageons vivement à étendre cette pratique de sécurité et à exiger l'authentification MFA pour tous les types d'utilisateurs de vos AWS environnements.

Dans la mesure du possible, nous vous recommandons d'utiliser un périphérique MFA matériel pour l'utilisateur root. Un appareil MFA virtuel peut ne pas fournir le même niveau de sécurité qu'un appareil MFA matériel. Vous pouvez utiliser le MFA virtuel en attendant l'approbation ou la livraison du matériel.

Dans les situations où vous gérez des centaines de comptes AWS Organizations, en fonction de la tolérance au risque de votre organisation, il se peut que l'utilisation d'une MFA matérielle pour l'utilisateur racine de chaque compte d'une unité organisationnelle (UO) ne soit pas évolutive. Dans ce cas, vous pouvez choisir un compte dans l'unité d'organisation qui fait office de compte de gestion de l'unité d'organisation, puis désactiver l'utilisateur root pour les autres comptes de cette unité d'organisation. Par défaut, le compte de gestion de l'unité d'organisation n'a pas accès aux autres comptes. En configurant à l'avance l'accès entre comptes, vous pouvez accéder aux autres comptes depuis le compte de gestion de l'unité d'organisation en cas d'urgence. Pour configurer l'accès entre comptes, vous créez un rôle IAM dans le compte membre et vous définissez des politiques afin que seul l'utilisateur root du compte de gestion de l'unité d'organisation puisse assumer ce rôle. Pour plus d'informations, voir Tutoriel : Déléguer l'accès à Comptes AWS l'aide de rôles IAM dans la documentation IAM.

Nous vous recommandons d'activer plusieurs dispositifs MFA pour vos informations d'identification d'utilisateur root. Vous pouvez enregistrer jusqu'à huit appareils MFA de n'importe quelle combinaison.

Pour plus d’informations, consultez les ressources suivantes :

- Activation d'un jeton TOTP matériel dans la documentation IAM
- Activation d'un dispositif d'authentification multifactorielle virtuelle (MFA) dans la documentation IAM
- Activation d'une clé de sécurité FIDO dans la documentation IAM
- Sécurisez la connexion de votre utilisateur root avec l'authentification multifactorielle (MFA) dans la documentation IAM

Suivez les meilleures pratiques de sécurité pour IAM

La documentation IAM inclut une liste des meilleures pratiques conçues pour vous aider à sécuriser vos ressources Comptes AWS et vos ressources. Il inclut des recommandations pour configurer l'accès et les autorisations selon le principe du moindre privilège. Parmi les meilleures pratiques en

matière de sécurité IAM, citons la configuration de la fédération des identités, l'exigence de la MFA et l'utilisation d'informations d'identification temporaires.

Pour plus d’informations, consultez les ressources suivantes :

- Bonnes pratiques de sécurité en matière d'IAM dans la documentation IAM
- Utilisation d'informations d'identification temporaires avec AWS les ressources de la documentation IAM

Accorder des autorisations de moindre privilège

Le moindre privilège est la pratique qui consiste à n'accorder que les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques.

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs, tels que leurs balises. Vous pouvez utiliser les attributs de groupe, d'identité et de ressource pour définir des autorisations de manière dynamique à grande échelle, plutôt que de définir des autorisations pour des utilisateurs individuels. Par exemple, vous pouvez utiliser ABAC pour autoriser un groupe de développeurs à accéder uniquement aux ressources associées à un tag spécifique à leur projet.

Pour plus d’informations, consultez les ressources suivantes :

- Appliquer les autorisations de moindre privilège dans la documentation IAM
- À quoi sert ABAC AWS dans la documentation IAM

Définissez des barrières d'autorisation au niveau de la charge de travail

Il est recommandé d'utiliser une stratégie multi-comptes, car elle offre la flexibilité nécessaire pour définir des garde-fous au niveau de la charge de travail. L'architecture AWS de référence de sécurité fournit des conseils prescriptifs sur la manière de structurer vos comptes. Ces comptes sont gérés en tant qu'organisation dans AWS Organizations, et ils sont regroupés en unités organisationnelles (OUs).

Services AWS, par exemple AWS Control Tower, peut vous aider à gérer de manière centralisée les contrôles au sein d'une organisation. Nous vous recommandons de définir un objectif clair pour chaque compte ou unité d'organisation au sein de l'organisation, et d'appliquer des contrôles en fonction de cet objectif. AWS Control Tower met en œuvre des contrôles préventifs, de détection et proactifs qui vous aident à gérer les ressources et à contrôler la conformité. Un contrôle préventif est conçu pour empêcher qu'un événement ne se produise. Un contrôle de détection est conçu pour détecter, enregistrer et alerter après la survenue d'un événement. Un contrôle proactif est conçu pour empêcher le déploiement de ressources non conformes en analysant les ressources avant qu'elles ne soient provisionnées.

Pour plus d’informations, consultez les ressources suivantes :

- Séparez les charges de travail à l'aide de comptes dans le AWS Well-Architected Framework
- AWS Architecture de référence de sécurité (AWS SRA) dans les directives AWS prescriptives
- À propos des contrôles AWS Control Tower dans la AWS Control Tower documentation
- Mise en œuvre de contrôles de sécurité AWS dans les directives AWS prescriptives
- Utilisez les politiques de contrôle des services pour définir des règles de protection des autorisations entre les comptes de votre AWS organisation dans le blog sur la AWS sécurité

Faites pivoter les clés d'accès IAM à intervalles réguliers

Il est recommandé de mettre à jour les clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme. Nous recommandons de faire pivoter les clés d'accès tous les 90 jours ou moins. La rotation des clés d'accès réduit le risque d'utilisation d'une clé d'accès associée à un compte compromis ou résilié. Il empêche également l'accès en utilisant une ancienne clé qui pourrait avoir été perdue, compromise ou volée. Mettez toujours à jour les applications après avoir fait pivoter les touches d'accès.

Pour plus d’informations, consultez les ressources suivantes :

- Mettez à jour les clés d'accès si nécessaire pour les cas d'utilisation nécessitant des informations d'identification à long terme dans la documentation IAM
- Faites pivoter automatiquement les clés d'accès utilisateur IAM à grande échelle avec AWS Organizations et AWS Secrets Manager dans les directives AWS prescriptives
- Mise à jour des clés d'accès dans la documentation IAM

Identifier les ressources partagées avec une entité externe

Une entité externe est une ressource, une application, un service ou un utilisateur extérieur à votre AWS organisation, tel qu'un autre Comptes AWS, un utilisateur root, un utilisateur ou un rôle IAM, un utilisateur fédéré Service AWS, un utilisateur anonyme (ou non authentifié). Il est recommandé d'utiliser IAM Access Analyzer pour identifier les ressources de votre organisation et de vos comptes, telles que les buckets Amazon Simple Storage Service (Amazon S3) ou les rôles IAM, partagées avec une entité externe. Cela vous permet d'identifier les accès involontaires aux ressources et aux données, qui constituent un risque pour la sécurité.

Pour plus d’informations, consultez les ressources suivantes :

- Vérifiez l'accès public et entre comptes aux ressources avec IAM Access Analyzer dans la documentation IAM
- Analysez l'accès public et entre comptes dans le AWS Well-Architected Framework
- Utilisation AWS Identity and Access Management Access Analyzer dans la documentation IAM

Recommandations de contrôle de sécurité pour la journalisation et la surveillance

La journalisation et la surveillance sont des aspects importants de la détection des menaces. La détection des menaces est l'une des fonctionnalités du AWS Cloud Adoption Framework (AWS CAF) du point de vue de la sécurité. En utilisant les données des journaux, votre entreprise peut surveiller votre environnement afin de comprendre et d'identifier les erreurs de configuration, les menaces et les comportements inattendus potentiels en matière de sécurité. Comprendre les menaces potentielles peut aider votre entreprise à hiérarchiser les contrôles de sécurité, et une détection efficace des menaces peut vous aider à y répondre plus rapidement.

Contrôles de cette section :

- Configurez au moins un sentier multirégional dans CloudTrail
- Configuration de la journalisation au niveau du service et de l'application
- Établissez un emplacement centralisé pour analyser les journaux et répondre aux événements de sécurité
- Empêchez l'accès non autorisé aux compartiments S3 contenant des fichiers CloudTrail journaux
- Configuration des alertes pour les modifications apportées aux groupes de sécurité ou au réseau ACLs
- Configurer les alertes pour les CloudWatch alarmes qui passent à l'état ALARM

Configurez au moins un sentier multirégional dans CloudTrail

AWS CloudTrailvous aide à auditer la gouvernance, la conformité et le risque opérationnel de votre Compte AWS Les actions entreprises par un utilisateur, un rôle ou un Service AWS sont enregistrées sous forme d'événements dans CloudTrail. Les événements incluent les mesures prises dans les AWS Management Console, AWS Command Line Interface (AWS CLI) AWS SDKs et APIs. Cet historique des événements vous permet d'analyser votre niveau de sécurité, de suivre l'évolution des ressources et d'auditer la conformité.

Pour un enregistrement continu des événements de votre site Compte AWS, vous devez créer un parcours. Chaque parcours doit être configuré pour enregistrer tous les événements Régions AWS. En enregistrant tous les événements Régions AWS, vous vous assurez que tous les événements qui

se produisent dans votre compte Compte AWS sont enregistrés, quel que soit l'endroit où Région AWS ils se sont produits. Un suivi multirégional garantit que les événements de service mondiaux sont enregistrés.

Pour plus d’informations, consultez les ressources suivantes :

- CloudTrail les meilleures pratiques en matière de sécurité dans la CloudTrail documentation
- Conversion d'un parcours qui s'applique à une région pour qu'il s'applique à toutes les régions de la CloudTrail documentation
- Activation et désactivation de la journalisation globale des événements de service dans la documentation CloudTrail

Configuration de la journalisation au niveau du service et de l'application

Le AWS Well-Architected Framework vous recommande de conserver les journaux des événements de sécurité des services et des applications. Il s'agit d'un principe fondamental de sécurité pour les audits, les enquêtes et les cas d'utilisation opérationnelle. La conservation des journaux des services et des applications est une exigence de sécurité courante qui repose sur les normes, politiques et procédures de gouvernance, de risque et de conformité (GRC).

Les équipes chargées des opérations de sécurité s'appuient sur les journaux et les outils de recherche pour découvrir des événements potentiellement intéressants susceptibles d'indiquer une activité non autorisée ou une modification involontaire. Vous pouvez activer la journalisation pour différents services, en fonction du cas d'utilisation. Par exemple, vous pouvez enregistrer l'accès au compartiment Amazon S3, le trafic ACL AWS WAF Web, le trafic Amazon API Gateway au niveau de la couche réseau ou les CloudFront distributions Amazon.

Pour plus d’informations, consultez les ressources suivantes :

- Diffusez Amazon CloudWatch Logs sur un compte centralisé à des fins d'audit et d'analyse sur le blog AWS d'architecture
- Configurer la journalisation des services et des applications dans le AWS Well-Architected Framework

Établissez un emplacement centralisé pour analyser les journaux et répondre aux événements de sécurité

L'analyse manuelle des journaux et le traitement des informations ne suffisent pas pour faire face au volume d'informations associé aux architectures complexes. L'analyse et les rapports à eux seuls ne facilitent pas l'affectation des événements à la bonne ressource en temps opportun. Le AWS Well-Architected Framework vous recommande d' AWS intégrer les événements et les résultats de sécurité dans un système de notification et de flux de travail, tel qu'un système de gestion des tickets, des bogues ou des informations et événements de sécurité (SIEM). Ces systèmes vous aident à attribuer, acheminer et gérer les événements de sécurité.

Pour plus d’informations, consultez les ressources suivantes :

- Analysez les journaux, les résultats et les métriques de manière centralisée dans le AWS Well-Architected Framework
- Analysez la sécurité, la conformité et l'activité opérationnelle à l'aide d' CloudTrail Amazon Athena dans le blog sur la AWS sécurité
- AWS Partenaires fournissant des services de détection et de réponse aux menaces dans le cadre du portefeuille de AWS partenaires

Empêchez l'accès non autorisé aux compartiments S3 contenant des fichiers CloudTrail journaux

Par défaut, les fichiers CloudTrail journaux sont stockés dans des compartiments Amazon S3. Une bonne pratique de sécurité consiste à empêcher tout accès non autorisé à tout compartiment Amazon S3 contenant des fichiers CloudTrail journaux. Cela vous permet de maintenir l'intégrité, l'exhaustivité et la disponibilité de ces journaux, ce qui est essentiel à des fins de criminalistique et d'audit. Si vous souhaitez enregistrer des événements de données pour des compartiments S3 contenant des fichiers CloudTrail journaux, vous pouvez créer un journal CloudTrail à cette fin.

Pour plus d’informations, consultez les ressources suivantes :

- Configuration des paramètres de blocage de l'accès public pour vos compartiments S3 dans la documentation Amazon S3
- CloudTrail meilleures pratiques de sécurité préventive dans la documentation CloudTrail

- Création d'un parcours dans la CloudTrail documentation

Configuration des alertes pour les modifications apportées aux groupes de sécurité ou au réseau ACLs

Un groupe de sécurité dans Amazon Virtual Private Cloud (Amazon VPC) contrôle le trafic autorisé à atteindre et à quitter les ressources auxquelles il est associé. Une liste de contrôle d'accès réseau (ACL) autorise ou refuse un trafic entrant ou sortant spécifique au niveau du sous-réseau du VPC. Ces ressources sont essentielles à la gestion des accès dans votre AWS environnement.

Créez et configurez une CloudWatch alarme Amazon qui vous avertit en cas de modification de la configuration d'un groupe de sécurité ou d'une ACL réseau. Configurez cette alarme pour qu'elle vous alerte chaque fois qu'un appel d' AWS API est effectué pour mettre à jour les groupes de sécurité. Vous pouvez également utiliser des services, tels qu'Amazon EventBridge AWS Config, pour répondre automatiquement à ce type d'événements de sécurité.

Pour plus d’informations, consultez les ressources suivantes :

- Annulez et recevez automatiquement des notifications concernant les modifications apportées à vos groupes de sécurité Amazon VPC sur le blog de AWS sécurité
- Utilisation des CloudWatch alarmes Amazon dans la CloudWatch documentation
- Implémentez des événements de sécurité exploitables dans le AWS Well-Architected Framework
- Automatisez la réponse aux événements dans le AWS Well-Architected Framework

Configurer les alertes pour les CloudWatch alarmes qui passent à l'état ALARM

Dans CloudWatch, vous pouvez spécifier les actions qu'une alarme effectue lorsqu'elle change d'état entre les `INSUFFICIENT_DATA` états `OKALARM`, et. Le type d'action d'alarme le plus courant consiste à avertir une ou plusieurs personnes en envoyant un message à une rubrique Amazon Simple Notification Service (Amazon SNS). Vous pouvez également configurer des alarmes à créer OpsItemsou des incidents AWS Systems Manager.

Nous vous recommandons d'activer les actions d'alarme pour être automatiquement alertée si une métrique surveillée dépasse le seuil défini. La surveillance des alarmes vous aide à identifier les activités inhabituelles et à répondre rapidement aux problèmes de sécurité et de fonctionnement.

Pour plus d’informations, consultez les ressources suivantes :

- Implémentez des événements de sécurité exploitables dans le AWS Well-Architected Framework
- Actions d'alarme dans la CloudWatch documentation

Recommandations en matière de contrôle de sécurité pour protéger l'infrastructure

La protection de l'infrastructure est un élément clé de tout programme de sécurité. Il inclut des méthodologies de contrôle qui vous aident à protéger vos réseaux et vos ressources informatiques. Les exemples de protection de l'infrastructure incluent les limites de confiance, une defense-in-depth approche, le renforcement de la sécurité, la gestion des correctifs, ainsi que l'authentification et l'autorisation du système d'exploitation. Pour plus d'informations, consultez la section Protection de l'infrastructure dans le AWS Well-Architected Framework. Les contrôles de sécurité présentés dans cette section peuvent vous aider à mettre en œuvre les meilleures pratiques en matière de protection de l'infrastructure.

Contrôles de cette section :

- Spécifier les objets racines par défaut pour les CloudFront distributions
- Scannez le code de l'application pour identifier les problèmes de sécurité courants
- Créez des couches réseau à l'aide de réseaux dédiés VPCs et de sous-réseaux
- Limitez le trafic entrant aux seuls ports autorisés
- Bloquer l'accès public aux documents de Systems Manager
- Bloquer l'accès public aux fonctions Lambda
- Restreindre le trafic entrant et sortant dans le groupe de sécurité par défaut
- Détectez les vulnérabilités logicielles et les risques d'exposition involontaire au réseau
- Configurez AWS WAF
- Configurer des protections avancées contre les attaques DDo S
- Utiliser une defense-in-depth approche pour contrôler le trafic réseau

Spécifier les objets racines par défaut pour les CloudFront distributions

Amazon CloudFront accélère la diffusion de votre contenu Web en le diffusant via un réseau mondial de centres de données, ce qui réduit le temps de latence et améliore les performances. Si vous ne définissez pas un objet racine par défaut, des demandes pour la racine de votre distribution sont

transmises à votre serveur d'origine. Si vous utilisez une origine Amazon Simple Storage Service (Amazon S3), la demande peut renvoyer une liste du contenu de votre compartiment S3 ou une liste des contenus privés de votre origine. La spécification d'un objet racine par défaut vous permet d'éviter d'exposer le contenu de votre distribution.

Pour plus d'informations, consultez les ressources suivantes :

- Spécifier un objet racine par défaut dans la CloudFront documentation

Scannez le code de l'application pour identifier les problèmes de sécurité courants

Le AWS Well-Architected Framework vous recommande de scanner les bibliothèques et les dépendances pour détecter les problèmes et les défauts. Il existe de nombreux outils d'analyse de code source que vous pouvez utiliser pour analyser le code source. Par exemple, Amazon CodeGuru peut rechercher les problèmes de sécurité courants dans Java or Python applications et fournir des recommandations pour les mesures correctives.

Pour plus d'informations, consultez les ressources suivantes :

- CodeGuru documentation
- Outils d'analyse du code source sur le OWASP Foundation website
- Gérez les vulnérabilités dans le AWS Well-Architected Framework

Créez des couches réseau à l'aide de réseaux dédiés VPCs et de sous-réseaux

Le AWS Well-Architected Framework vous recommande de regrouper les composants qui partagent des exigences de sensibilité en couches. Cela permet de minimiser l'impact potentiel d'un accès non autorisé. Par exemple, un cluster de base de données qui ne nécessite pas d'accès à Internet doit être placé dans un sous-réseau privé de son VPC pour s'assurer qu'il n'existe aucune route vers ou depuis Internet.

AWS propose de nombreux services qui peuvent vous aider à tester et à identifier l'accessibilité du public. Par exemple, Reachability Analyzer est un outil d'analyse de configuration qui vous permet de tester la connectivité entre une ressource source et une ressource de destination dans votre. VPCs

Network Access Analyzer peut également vous aider à identifier les accès réseau involontaires aux ressources.

Pour plus d'informations, consultez les ressources suivantes :

- Créez des couches réseau dans le AWS Well-Architected Framework
- Documentation sur l'analyseur de Reachability Analyzer
- Documentation relative à l'analyseur d'accès réseau
- Créez un sous-réseau dans la documentation Amazon Virtual Private Cloud (Amazon VPC)

Limitez le trafic entrant aux seuls ports autorisés

L'accès illimité, tel que le trafic provenant de l'adresse IP `0.0.0.0/0` source, augmente le risque d'activités malveillantes, telles que le piratage, les attaques denial-of-service (DoS) et la perte de données. Les groupes de sécurité fournissent un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Aucun groupe de sécurité ne doit autoriser un accès d'entrée illimité à des ports connus, tels que SSH et Windows protocole RDP (Remote Desktop Protocol). Pour le trafic entrant, dans vos groupes de sécurité, autorisez uniquement les connexions TCP ou UDP sur les ports autorisés. Pour vous connecter aux instances Amazon Elastic Compute Cloud (Amazon EC2), utilisez le gestionnaire de session ou Run Command au lieu d'un accès SSH ou RDP direct.

Pour plus d'informations, consultez les ressources suivantes :

- Travaillez avec des groupes de sécurité dans la EC2 documentation Amazon
- Contrôlez le trafic vers vos AWS ressources à l'aide des groupes de sécurité décrits dans la documentation Amazon VPC

Bloquer l'accès public aux documents de Systems Manager

À moins que votre cas d'utilisation ne nécessite l'activation du partage public, les AWS Systems Manager meilleures pratiques recommandent de bloquer le partage public des documents de Systems Manager. Le partage public peut fournir un accès involontaire à des documents. Un document public de Systems Manager peut exposer des informations précieuses et sensibles sur votre compte, vos ressources et vos processus internes.

Pour plus d'informations, consultez les ressources suivantes :

- Meilleures pratiques pour les documents partagés de Systems Manager dans la documentation de Systems Manager
- Modifier les autorisations pour un document Systems Manager partagé dans la documentation de Systems Manager

Bloquer l'accès public aux fonctions Lambda

AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Les fonctions Lambda ne doivent pas être accessibles au public car cela pourrait permettre un accès involontaire au code de la fonction.

Nous vous recommandons de configurer des politiques basées sur les ressources pour les fonctions Lambda afin de refuser l'accès depuis l'extérieur de votre compte. Vous pouvez y parvenir en supprimant les autorisations ou en ajoutant la `AWS:SourceAccount` condition à l'instruction autorisant l'accès. Vous pouvez mettre à jour les politiques basées sur les ressources pour les fonctions Lambda via l'API Lambda ou (). AWS Command Line Interface AWS CLI

Nous vous recommandons également d'activer la fonction [Lambda.1] Les politiques de la fonction Lambda devraient interdire le contrôle d'accès public dans. AWS Security Hub Ce contrôle confirme que les politiques basées sur les ressources pour les fonctions Lambda interdisent l'accès public.

Pour plus d’informations, consultez les ressources suivantes :

- AWS Lambda contrôles dans la documentation de Security Hub
- Utilisation de politiques basées sur les ressources pour Lambda dans la documentation Lambda
- Ressources et conditions relatives aux actions Lambda dans la documentation Lambda

Restreindre le trafic entrant et sortant dans le groupe de sécurité par défaut

Si vous n'associez pas de groupe de sécurité personnalisé lorsque vous AWS provisionnez une ressource, celle-ci est associée au groupe de sécurité par défaut du VPC. Les règles par défaut de ce groupe de sécurité autorisent tout le trafic entrant provenant de toutes les ressources attribuées à ce groupe de sécurité, ainsi que l'ensemble du trafic sortant et du trafic sortant IPv4 . IPv6 Cela peut permettre un trafic involontaire vers la ressource.

AWS recommande de ne pas utiliser le groupe de sécurité par défaut. Créez plutôt des groupes de sécurité personnalisés pour des ressources ou des groupes de ressources spécifiques.

Le groupe de sécurité par défaut ne pouvant pas être supprimé, nous vous recommandons de modifier les règles du groupe de sécurité par défaut afin de limiter le trafic entrant et sortant. Lorsque vous configurez les règles des groupes de sécurité, suivez le principe du moindre privilège.

Nous vous recommandons également d'activer le [EC2.2] Les groupes de sécurité VPC par défaut ne doivent pas autoriser le contrôle du trafic entrant ou sortant dans Security Hub. Ce contrôle confirme que le groupe de sécurité par défaut d'un VPC refuse le trafic entrant et sortant.

Pour plus d’informations, consultez les ressources suivantes :

- Contrôlez le trafic vers vos AWS ressources à l'aide des groupes de sécurité décrits dans la documentation Amazon VPC
- Groupes de sécurité par défaut pour vous VPCs dans la documentation Amazon VPC
- EC2Contrôles Amazon dans la documentation du Security Hub

Détectez les vulnérabilités logicielles et les risques d'exposition involontaire au réseau

Nous vous recommandons d'activer Amazon Inspector dans tous vos comptes. Amazon Inspector est un service de gestion des vulnérabilités qui analyse en permanence vos EC2 instances Amazon, les images des conteneurs Amazon Elastic Container Registry (Amazon ECR) et les fonctions Lambda pour détecter les vulnérabilités logicielles et les expositions involontaires au réseau. Il prend également en charge l'inspection approfondie des EC2 instances Amazon. Lorsqu'Amazon Inspector identifie une vulnérabilité ou un chemin réseau ouvert, il produit un résultat que vous pouvez examiner. Si Amazon Inspector et Security Hub sont tous deux configurés dans votre compte, Amazon Inspector envoie automatiquement les résultats de sécurité à Security Hub pour une gestion centralisée.

Pour plus d’informations, consultez les ressources suivantes :

- Numérisation des ressources avec Amazon Inspector dans la documentation Amazon Inspector
- Amazon Inspector Inspection approfondie pour Amazon EC2 dans la documentation Amazon Inspector
- Scannez EC2 AMIs à l'aide d'Amazon Inspector dans le blog sur AWS la sécurité

- Création d'un programme de gestion des vulnérabilités évolutif sur la base AWS des directives AWS prescriptives
- Automatisez la protection du réseau dans le AWS Well-Architected Framework
- Automatisez la protection informatique dans le AWS Well-Architected Framework

Configurez AWS WAF

AWS WAFest un pare-feu d'applications Web qui vous permet de surveiller et de bloquer les requêtes HTTP ou HTTPS transmises aux ressources protégées de votre application Web, telles qu'Amazon API Gateway APIs, les CloudFront distributions Amazon ou les équilibreurs de charge d'application. Selon les critères que vous spécifiez, le service répond aux demandes soit avec le contenu demandé, soit avec un code d'état HTTP 403 (Interdit), soit avec une réponse personnalisée. AWS WAF peuvent aider à protéger les applications Web ou APIs contre les exploits Web courants susceptibles d'affecter la disponibilité, de compromettre la sécurité ou de consommer des ressources excessives. Envisagez de configurer AWS WAF Comptes AWS et d'utiliser une combinaison de règles AWS gérées, de règles personnalisées et d'intégrations de partenaires pour protéger vos applications contre les attaques de la couche application (couche 7).

Pour plus d’informations, consultez les ressources suivantes :

- Commencer AWS WAF dans la AWS WAF documentation
- AWS WAF partenaires de livraison sur le AWS site
- Automatisations de sécurité pour AWS WAF la bibliothèque de AWS solutions
- Mettre en œuvre l'inspection et la protection dans le cadre AWS Well-Architected

Configurer des protections avancées contre les attaques DDo S

AWS Shieldfournit des protections contre les attaques par déni de service (DDoS) distribué visant les AWS ressources au niveau des couches réseau et transport (couches 3 et 4) et de la couche application (couche 7). Ce service est disponible en deux options : AWS Shield Standard et AWS Shield Advanced. Shield Standard protège automatiquement les AWS ressources prises en charge, sans frais supplémentaires.

Nous vous recommandons de vous abonner à Shield Advanced, qui fournit une protection étendue contre les attaques DDo S pour les ressources protégées. Les protections que vous offre Shield

Advanced varient en fonction de votre architecture et de vos choix de configuration. Envisagez de mettre en œuvre les protections Shield Advanced pour les applications où vous avez besoin de l'un des éléments suivants :

- Disponibilité garantie pour les utilisateurs de l'application.
- Accès rapide à des experts en mitigation DDo S si l'application est affectée par une attaque DDo S.
- Prise de conscience par AWS du fait que l'application peut être affectée par une attaque DDo S, notification des attaques émanant d'AWS et remontée à vos équipes chargées de la sécurité ou des opérations.
- La prévisibilité des coûts de votre cloud, y compris lorsqu'une attaque DDo S affecte votre utilisation de Services AWS.

Pour plus d’informations, consultez les ressources suivantes :

- AWS Shield Advanced présentation dans la documentation du Shield
- AWS Shield Advanced ressources protégées dans la documentation du Shield
- AWS Shield Advanced fonctionnalités et options de la documentation Shield
- Réagir aux événements DDo S dans la documentation Shield
- Mettre en œuvre l'inspection et la protection dans le cadre AWS Well-Architected

Utiliser une defense-in-depth approche pour contrôler le trafic réseau

AWS Network Firewall est un pare-feu réseau géré et dynamique ainsi qu'un service de détection et de prévention des intrusions pour les clouds privés virtuels (VPCs) dans le AWS Cloud. Il vous aide à déployer des protections réseau essentielles sur le périmètre du VPC. Cela inclut le filtrage du trafic à destination et en provenance d'une passerelle Internet, d'une passerelle NAT ou via un VPN ou AWS Direct Connect. Network Firewall inclut des fonctionnalités qui contribuent à la protection contre les menaces réseau les plus courantes. Le pare-feu dynamique de Network Firewall peut intégrer le contexte des flux de trafic, tels que les connexions et les protocoles, pour appliquer les politiques.

Pour plus d’informations, consultez les ressources suivantes :

- AWS Network Firewall documentation
- Contrôlez le trafic à tous les niveaux dans le AWS Well-Architected Framework

Recommandations en matière de contrôle de sécurité pour protéger les données

Le AWS Well-Architected Framework regroupe les meilleures pratiques en matière de protection des données en trois catégories : classification des données, protection des données au repos et protection des données en transit. Les contrôles de sécurité présentés dans cette section peuvent vous aider à mettre en œuvre les meilleures pratiques en matière de protection des données. Ces meilleures pratiques fondamentales doivent être mises en place avant de concevoir des charges de travail dans le cloud. Ils empêchent la mauvaise gestion des données et vous aident à respecter les obligations organisationnelles, réglementaires et de conformité. Utilisez les contrôles de sécurité décrits dans cette section pour mettre en œuvre les meilleures pratiques en matière de protection des données.

Contrôles de cette section :

- Identifier et classer les données au niveau de la charge de travail
- Établissez des contrôles pour chaque niveau de classification des données
- Chiffrer les données au repos
- Chiffrer les données en transit
- Bloquer l'accès public aux instantanés Amazon EBS
- Bloquer l'accès public aux instantanés Amazon RDS
- Bloquez l'accès public à Amazon RDS, Amazon Redshift et aux ressources AWS DMS
- Bloquer l'accès public aux compartiments Amazon S3
- Exiger la MFA pour supprimer les données dans les compartiments Amazon S3 critiques
- Configuration des domaines Amazon OpenSearch Service dans un VPC
- Configurer les alertes de AWS KMS key suppression
- Bloquer l'accès public à AWS KMS keys
- Configurer les écouteurs de l'équilibreur de charge pour utiliser des protocoles sécurisés

Identifier et classer les données au niveau de la charge de travail

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 réduit souvent la fréquence de duplication des données. Cela permet de réduire les coûts de stockage et de sauvegarde et d'accélérer les recherches.

Nous vous recommandons de comprendre le type et la classification des données traitées par votre charge de travail, les processus métier associés, l'endroit où les données sont stockées et le propriétaire des données. La classification des données aide les responsables de la charge de travail à identifier les emplacements qui stockent des données sensibles et à déterminer comment ces données doivent être consultées et partagées. Les balises sont des paires clé-valeur qui servent de métadonnées pour organiser les AWS ressources. Les balises peuvent aider à gérer, identifier, organiser, rechercher et filtrer les ressources.

Pour plus d’informations, consultez les ressources suivantes :

- Classification des données dans les livres AWS blancs
- Identifiez les données incluses dans votre charge de travail dans le AWS Well-Architected Framework

Établissez des contrôles pour chaque niveau de classification des données

Définissez les contrôles de protection des données pour chaque niveau de classification. Par exemple, utilisez les contrôles recommandés pour sécuriser les données classées comme publiques et protégez les données sensibles à l'aide de contrôles supplémentaires. Utilisez des mécanismes et des outils qui réduisent ou éliminent le besoin d'accéder directement aux données ou de les traiter manuellement. L'automatisation de l'identification et de la classification des données réduit le risque d'erreur de classification, de mauvaise manipulation, de modification ou d'erreur humaine.

Par exemple, pensez à utiliser Amazon Macie pour scanner les compartiments Amazon Simple Storage Service (Amazon S3) afin de détecter des données sensibles, telles que des informations personnelles identifiables (PII). Vous pouvez également automatiser la détection des accès involontaires aux données en utilisant les journaux de flux VPC dans Amazon Virtual Private Cloud (Amazon VPC).

Pour plus d’informations, consultez les ressources suivantes :

- Définissez les contrôles de protection des données dans le AWS Well-Architected Framework

- Automatisez l'identification et la classification dans le AWS Well-Architected Framework
- AWS Architecture de référence en matière de confidentialité (AWS PRA) dans les directives AWS prescriptives
- Découvrir des données sensibles avec Amazon Macie dans la documentation Macie
- Journalisation du trafic IP à l'aide des journaux de flux VPC dans la documentation Amazon VPC
- Techniques courantes pour détecter les données PHI et PII Services AWSà l'aide du AWS blog for Industries

Chiffrer les données au repos

Les données au repos sont des données stationnaires sur votre réseau, telles que les données stockées. La mise en œuvre du chiffrement et de contrôles d'accès appropriés pour les données inactives contribue à réduire le risque d'accès non autorisé. Le chiffrement est un processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré. Vous avez besoin d'une clé de chiffrement pour rechiffrer le contenu en texte brut afin de pouvoir l'utiliser. Dans le AWS Cloud, vous pouvez utiliser AWS Key Management Service (AWS KMS) pour créer et contrôler des clés cryptographiques qui aident à protéger vos données.

Comme indiqué dansÉtablissez des contrôles pour chaque niveau de classification des données, nous vous recommandons de créer une politique qui précise le type de données à chiffrer. Incluez des critères permettant de déterminer quelles données doivent être cryptées et quelles données doivent être protégées par une autre technique, telle que la tokenisation ou le hachage.

Pour plus d’informations, consultez les ressources suivantes :

- Configuration du chiffrement par défaut dans la documentation Amazon S3
- Chiffrement par défaut pour les nouveaux volumes EBS et les copies instantanées dans la documentation Amazon EC2
- Chiffrement des ressources Amazon Aurora dans la documentation Amazon Aurora
- Présentation des détails cryptographiques de AWS KMS la documentation AWS KMS
- Création d'une stratégie de chiffrement d'entreprise pour les données inactives dans les directives AWS prescriptives
- Appliquez le chiffrement au repos dans le AWS Well-Architected Framework
- Pour plus d'informations sur le chiffrement en particulier Services AWS, consultez la AWS documentation de ce service

Chiffrer les données en transit

Les données en transit sont les données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau. Chiffrez toutes les données en transit à l'aide de protocoles TLS sécurisés et de suites de chiffrement. Le trafic réseau entre les ressources et Internet doit être crypté afin d'empêcher tout accès non autorisé aux données. Dans la mesure du possible, utilisez le protocole TLS pour chiffrer le trafic réseau au sein de votre environnement interne AWS .

Pour plus d’informations, consultez les ressources suivantes :

- Exiger le protocole HTTPS pour la communication entre les utilisateurs et CloudFront dans la CloudFront documentation Amazon
- Documentation AWS PrivateLink
- Appliquez le chiffrement en transit dans le AWS Well-Architected Framework
- Pour plus d'informations sur le chiffrement en particulier Services AWS, consultez la AWS documentation de ce service

Bloquer l'accès public aux instantanés Amazon EBS

Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon). EC2 Vous pouvez sauvegarder les données de vos volumes Amazon EBS sur Amazon S3 en prenant des point-in-time instantanés. Vous pouvez partager des instantanés publiquement avec d'autres personnes Comptes AWS, ou vous pouvez les partager en privé avec la personne Comptes AWS que vous spécifiez.

Nous vous recommandons de ne pas partager publiquement les instantanés Amazon EBS. Cela peut exposer des données sensibles par inadvertance. Lorsque vous partagez un instantané, vous permettez à d'autres personnes d'accéder aux données qu'il contient. Partagez des instantanés uniquement avec des personnes en qui vous avez confiance et qui disposent de toutes ces données.

Pour plus d’informations, consultez les ressources suivantes :

- Partagez un instantané dans la EC2 documentation Amazon
- Les instantanés Amazon EBS ne doivent pas être restaurables publiquement dans la documentation AWS Security Hub
- ebs-snapshot-public-restorable-consultez la documentation AWS Config

Bloquer l'accès public aux instantanés Amazon RDS

Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le. AWS Cloud Amazon RDS crée et enregistre des sauvegardes automatisées de votre instance de base de données (DB) ou de votre cluster de base de données multi-AZ pendant la fenêtre de sauvegarde de votre instance de base de données. Amazon RDS crée un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière et pas seulement les bases de données. Vous pouvez partager un instantané manuel dans le but de le copier ou de restaurer une instance de base de données à partir de celui-ci.

Si vous partagez un instantané en tant que public, assurez-vous qu'aucune des données qu'il contient n'est privée ou sensible. Lorsqu'un instantané est partagé publiquement, il donne à tous Comptes AWS les droits d'accès aux données. Cela peut entraîner une exposition involontaire des données de votre instance Amazon RDS.

Pour plus d’informations, consultez les ressources suivantes :

- Partage d'un instantané de base de données dans la documentation Amazon RDS
- rds-snapshots-public-prohibiteddans la AWS Config documentation
- L'instantané RDS doit être privé dans la documentation du Security Hub

Bloquez l'accès public à Amazon RDS, Amazon Redshift et aux ressources AWS DMS

Vous pouvez configurer les instances de base de données Amazon RDS, les clusters Amazon Redshift AWS Database Migration Service et AWS DMS() les instances de réplication pour qu'elles soient accessibles au public. Si la valeur du `publiclyAccessible` champ est`true`, ces ressources sont accessibles au public. Autoriser l'accès du public peut entraîner un trafic, une exposition ou des fuites de données inutiles. Nous vous recommandons de ne pas autoriser l'accès public à ces ressources.

Nous vous recommandons d'activer AWS Config les règles ou les contrôles Security Hub pour détecter si les instances de base de données Amazon RDS, les instances de AWS DMS réplication ou les clusters Amazon Redshift autorisent l'accès public.

> **Note**
>
> Les paramètres d'accès public pour les instances de AWS DMS réplication ne peuvent pas être modifiés une fois que l'instance a été provisionnée. Pour modifier le paramètre d'accès public, supprimez l'instance actuelle, puis recréez-la. Lorsque vous le recréez, ne sélectionnez pas l'option Accessible au public.

Pour plus d’informations, consultez les ressources suivantes :

- AWS DMS les instances de réplication ne doivent pas être publiques dans la documentation du Security Hub
- Les instances de base de données RDS doivent interdire l'accès public dans la documentation du Security Hub
- Les clusters Amazon Redshift devraient interdire l'accès public dans la documentation du Security Hub
- rds-instance-public-access-consultez la documentation AWS Config
- dms-replication-not-publicdans la AWS Config documentation
- redshift-cluster-public-access-consultez la documentation AWS Config
- Modification d'une instance de base de données Amazon RDS dans la documentation Amazon RDS
- Modification d'un cluster dans la documentation Amazon Redshift

Bloquer l'accès public aux compartiments Amazon S3

C'est une bonne pratique de sécurité d'Amazon S3 pour garantir que vos buckets ne sont pas accessibles au public. À moins que vous ne demandiez explicitement à quiconque sur Internet de lire ou d'écrire dans votre compartiment, assurez-vous que celui-ci n'est pas public. Cela permet de protéger l'intégrité et la sécurité des données. Vous pouvez utiliser AWS Config les règles et les contrôles du Security Hub pour vérifier que vos compartiments Amazon S3 sont conformes à ces bonnes pratiques.

Pour plus d’informations, consultez les ressources suivantes :

- Les meilleures pratiques de sécurité d'Amazon S3 dans la documentation Amazon S3

- Le paramètre S3 Block Public Access doit être activé dans la documentation du Security Hub
- Les compartiments S3 doivent interdire l'accès public en lecture dans la documentation du Security Hub
- Les compartiments S3 doivent interdire l'accès public en écriture dans la documentation du Security Hub
- bucket-public-read-prohibited règle s3- dans la AWS Config documentation
- s3- bucket-public-write-prohibited dans la AWS Config documentation

Exiger la MFA pour supprimer les données dans les compartiments Amazon S3 critiques

Lorsque vous travaillez avec la gestion des versions S3 dans des compartiments Simple Storage Service (Amazon S3), vous pouvez ajouter une couche de sécurité en activant la fonction MFA delete (Suppression de l'authentification multifacteur). Quand vous procédez ainsi, le propriétaire du compartiment doit inclure deux formes d'authentification dans toute demande pour supprimer une version ou modifier l'état de la gestion des versions du compartiment. Nous vous recommandons d'activer cette fonctionnalité pour les compartiments contenant des données essentielles pour votre organisation. Cela permet d'éviter les suppressions accidentelles de compartiments et de données.

Pour plus d'informations, consultez les ressources suivantes :

- Configuration de la suppression MFA dans la documentation Amazon S3

Configuration des domaines Amazon OpenSearch Service dans un VPC

Amazon OpenSearch Service est un service géré qui vous aide à déployer, à exploiter et à faire évoluer OpenSearch clusters dans le AWS Cloud. Amazon OpenSearch Service prend en charge OpenSearch et héritage Elasticsearch logiciel open source (OSS). Les domaines Amazon OpenSearch Service déployés au sein d'un VPC peuvent communiquer avec les ressources du VPC via le AWS réseau privé, sans qu'il soit nécessaire de passer par l'Internet public. Cette configuration améliore votre niveau de sécurité en limitant l'accès aux données en transit. Nous vous recommandons de ne pas associer de domaines Amazon OpenSearch Service à des sous-réseaux publics et de configurer le VPC conformément aux meilleures pratiques.

Pour plus d'informations, consultez les ressources suivantes :

- Lancement de vos domaines Amazon OpenSearch Service au sein d'un VPC dans la documentation Amazon OpenSearch Service
- opensearch-in-vpc-onlydans la AWS Config documentation
- OpenSearch les domaines doivent se trouver dans un VPC dans la documentation du Security Hub

Configurer les alertes de AWS KMS key suppression

AWS Key Management Service (AWS KMS) les clés ne peuvent pas être récupérées après leur suppression. Si une clé KMS est supprimée, les données toujours chiffrées sous cette clé sont définitivement irrécupérables. Si vous devez conserver l'accès aux données, avant de supprimer la clé, vous devez les déchiffrer ou les rechiffrer avec une nouvelle clé KMS. Vous devez supprimer une clé KMS seulement lorsque vous êtes sûr de ne plus avoir besoin de l'utiliser.

Nous vous recommandons de configurer une CloudWatch alarme Amazon qui vous avertira si quelqu'un initie la suppression d'une clé KMS. Comme il est destructeur et potentiellement dangereux de supprimer une clé KMS, AWS KMS vous devez définir une période d'attente et planifier la suppression dans un délai de 7 à 30 jours. Cela permet de revoir la suppression planifiée et de l'annuler, si nécessaire.

Pour plus d'informations, consultez les ressources suivantes :

- Planification et annulation de la suppression de clés dans la documentation AWS KMS
- Création d'une alarme qui détecte l'utilisation d'une clé KMS en attente de suppression dans la AWS KMS documentation
- AWS KMS keys ne doit pas être supprimé par inadvertance dans la documentation du Security Hub

Bloquer l'accès public à AWS KMS keys

Les politiques clés constituent le principal moyen de contrôler l'accès à AWS KMS keys. Chaque clé KMS a exactement une politique de clé. L'autorisation d'un accès anonyme aux clés KMS peut entraîner une fuite de données sensibles. Nous vous recommandons d'identifier toutes les clés KMS

accessibles au public et de mettre à jour leurs politiques d'accès afin d'empêcher les demandes non signées adressées à ces ressources.

Pour plus d’informations, consultez les ressources suivantes :

- Bonnes pratiques de sécurité AWS Key Management Service décrites dans la AWS KMS documentation
- Modification d'une politique clé dans la AWS KMS documentation
- Déterminer l'accès à AWS KMS keys dans la AWS KMS documentation

Configurer les écouteurs de l'équilibreur de charge pour utiliser des protocoles sécurisés

Elastic Load Balancing répartit automatiquement le trafic applicatif entrant sur plusieurs cibles. Vous configurez votre équilibreur de charge pour qu'il accepte le trafic entrant en spécifiant un ou plusieurs écouteurs. Un écouteur est un processus qui vérifie les demandes de connexion, en utilisant le protocole et le port que vous avez configurés. Chaque type d'équilibreur de charge prend en charge différents protocoles et ports :

- Les équilibreurs de charge d'application prennent les décisions de routage au niveau de la couche application et utilisent les protocoles HTTP ou HTTPS.
- Les équilibreurs de charge réseau prennent les décisions de routage au niveau de la couche transport et utilisent les protocoles TCP, TLS, UDP ou TCP_UDP.
- Les équilibreurs de charge classiques prennent les décisions de routage au niveau de la couche transport (en utilisant les protocoles TCP ou SSL) ou de la couche application (en utilisant les protocoles HTTP ou HTTPS).

Nous vous recommandons de toujours utiliser les protocoles HTTPS ou TLS. Ces protocoles garantissent que l'équilibreur de charge est responsable du chiffrement et du déchiffrement du trafic entre le client et la cible.

Pour plus d’informations, consultez les ressources suivantes :

- Écouteurs pour les équilibreurs de charge de vos applications dans la documentation Elastic Load Balancing
- Des écouteurs pour votre Classic Load Balancer dans la documentation d'Elastic Load Balancing

- Écouteurs pour vos équilibreurs de charge réseau dans la documentation Elastic Load Balancing
- Assurez-vous que les équilibreurs de AWS charge utilisent des protocoles d'écoute sécurisés dans AWS les directives prescriptives
- elb-tls-https-listeners-uniquement dans la documentation AWS Config
- Les écouteurs Classic Load Balancer doivent être configurés avec une terminaison HTTPS ou TLS dans la documentation du Security Hub
- Application Load Balancer doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS dans la documentation Security Hub

Recommandations de sécurité pour répondre aux incidents

Lorsqu'un événement de sécurité survient dans votre organisation, vos utilisateurs doivent être prêts à y répondre. Tous les utilisateurs doivent avoir une connaissance de base des processus de réponse en matière de sécurité de votre organisation. La planification, la formation et l'expérience sont essentielles à la réussite d'un programme de réponse aux incidents. Dans l'idéal, vous devez préparer votre organisation avant qu'un événement de sécurité potentiel ne se produise. Le AWS Well-Architected Framework identifie trois fondements nécessaires à la réussite d'un programme de réponse aux incidents dans le cloud : la préparation, les opérations et les activités post-incident. Pour plus d'informations, consultez la section Aspects de la réponse aux AWS incidents dans le AWS Well-Architected Framework.

À l'exception des contrôles de sécurité qui vous informent des événements ou y répondent automatiquement, il existe un nombre limité de contrôles que vous pouvez établir pour répondre aux incidents. Une solide posture de réponse aux incidents est principalement établie par le biais des plans, des processus, des manuels, des manuels et des programmes de formation que vous utilisez dans votre organisation. Vous pouvez utiliser les contrôles et les recommandations de cette section pour mettre en œuvre les meilleures pratiques pour votre programme de réponse aux incidents. Pour plus d'informations sur les meilleures pratiques en matière de réponse aux incidents et les conseils de mise en œuvre, consultez la section Réponse aux incidents dans le AWS Well-Architected Framework.

Les recommandations de cette section sont les suivantes :

- Définir un plan de réponse aux incidents
- Créez et gérez des livrets et des playbooks de réponse aux incidents
- Mettre en œuvre une automatisation de la sécurité axée sur les événements
- Documenter la manière dont les équipes opérationnelles doivent interagir avec Support
- Configuration des alertes pour les événements de sécurité

Définir un plan de réponse aux incidents

Établissez un plan de réponse aux incidents (IRP) bien défini. Le plan de réponse aux incidents est conçu pour constituer la base de votre programme de réponse aux incidents. Ce plan doit être personnalisé pour répondre aux besoins de chaque organisation.

Pour plus d'informations, consultez les ressources suivantes :

- Développez et testez un plan de réponse aux incidents dans le Guide de réponse aux incidents de AWS sécurité
- Développez des plans de gestion des incidents dans le cadre AWS Well-Architected
- Identifier le personnel clé et les ressources externes dans le AWS Well-Architected Framework

Créez et gérez des livrets et des playbooks de réponse aux incidents

L'élaboration de playbooks est un élément clé de la préparation aux processus de réponse à un incident. Les manuels de réponse aux incidents fournissent une série d'étapes recommandées que les utilisateurs doivent suivre lorsqu'un événement de sécurité se produit. Le fait de disposer d'une structure et d'étapes claires simplifie la réponse et réduit le risque d'erreur humaine.

Pour plus d'informations, consultez les ressources suivantes :

- Pourquoi créer des playbooks dans le Guide de réponse aux incidents AWS de sécurité
- AWS exemples de playbooks de réponse aux incidents sur GitHub
- Développez et testez des manuels de réponse aux incidents de sécurité dans le cadre AWS Well-Architected

Mettre en œuvre une automatisation de la sécurité axée sur les événements

L'automatisation des réponses de sécurité est une 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.

Beaucoup Services AWS soutiennent les réponses automatisées. Par exemple, vous pouvez configurer une CloudWatch alarme Amazon pour des métriques spécifiques, et l'alarme peut déclencher une action lorsqu'elle change d'état. Par le biais d'Amazon EventBridge, vous pouvez

également configurer une réponse et une correction automatisées en fonction des résultats dans AWS Security Hub Amazon Inspector.

Pour plus d'informations, veuillez consulter les ressources ci-dessous :

- Corrigez automatiquement les résultats de sécurité d'Amazon Inspector dans le blog sur la AWS sécurité
- Commencez à automatiser les réponses de sécurité sur AWS le blog sur la AWS sécurité
- Réponse de sécurité automatisée activée AWS dans la bibliothèque de AWS solutions
- Utilisation des CloudWatch alarmes Amazon dans la CloudWatch documentation
- Réponse et correction automatisées dans la documentation du Security Hub
- Création de réponses personnalisées aux conclusions d'Amazon Inspector avec Amazon EventBridge dans la documentation Amazon Inspector

Documenter la manière dont les équipes opérationnelles doivent interagir avec Support

Pour vous Compte AWS, vous pouvez définir un contact principal et trois contacts alternatifs. Nous vous recommandons de fournir un contact de sécurité pour chacun Compte AWS ou pour votre organisation.

AWS Support propose une gamme de plans qui donnent accès à des outils et à une expertise susceptibles de contribuer au succès et à la santé opérationnelle des AWS solutions. Déterminez également si votre organisation bénéficierait de l'utilisation d'un plan AWS Managed Services plutôt que d'un Support plan. AWS Managed Services (AMS) vous aide à fonctionner de manière plus efficace et plus sûre en fournissant une gestion continue de votre AWS infrastructure, y compris la surveillance, la gestion des incidents, les conseils de sécurité, le support des correctifs et la sauvegarde des AWS charges de travail. Le modèle de support AMS peut être mieux adapté aux organisations dont les équipes chargées des opérations cloud disposent de ressources limitées. Nous vous recommandons de comparer ces modèles et ces plans afin de choisir celui qui convient le mieux au cas d'utilisation de votre entreprise et au niveau de maturité du cloud.

Pour plus d’informations, consultez les ressources suivantes :

- Découvrez les équipes d' AWS intervention et le support dans le guide de réponse aux incidents de AWS sécurité

- Mettez à jour les contacts alternatifs pour vous Compte AWS dans le guide de gestion de AWS compte
- Comparez les Support forfaits sur le AWS site Web
- Stratégie AWS Managed Services à utiliser pour atteindre les résultats commerciaux cibles dans les directives AWS prescriptives

Configuration des alertes pour les événements de sécurité

La détection d'une anomalie est aussi importante que les mesures mises en œuvre pour contrôler cette anomalie. L'alerte est l'élément principal de la phase de détection. Il génère une notification pour lancer le processus de réponse aux incidents en fonction de Compte AWS l'activité qui vous intéresse. Assurez-vous que les alertes contiennent des informations pertinentes permettant à l'équipe de prendre des mesures.

Pour plus d’informations, consultez les ressources suivantes :

- Détection dans le guide de réponse aux incidents de AWS sécurité
- Préparez les capacités de criminalistique dans le AWS Well-Architected Framework
- Implémentez des événements de sécurité exploitables dans le AWS Well-Architected Framework

Étapes suivantes

Au fur et à mesure que vous poursuivez votre transition vers le cloud, il est important d'appliquer ces contrôles documentés, ces conseils et ces options de correction. Ces recommandations vous aident à améliorer votre posture de sécurité dans le cloud et à vous acquitter de vos responsabilités en matière de sécurité AWS Cloud, telles que définies dans le modèle de responsabilité AWS partagée.

Pour les prochaines étapes, nous recommandons ce qui suit :

- Pour plus d'informations sur les meilleures pratiques et les conseils de mise en œuvre, consultez les six piliers du AWS Well-Architected Framework.
- Pour Services AWS ce qui est des contrôles utilisés par votre organisation, consultez la liste des AWS Security Hub contrôles disponibles et déterminez si vous devez activer l'un de ces contrôles dans votre environnement.
- Pour Services AWS ce qui est de celles que votre organisation utilise, consultez la liste des règles AWS Config gérées disponibles et déterminez si vous devez activer l'une de ces règles dans votre environnement.

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
MFA pour l'utilisateur root	Nous avons mis à jour les recommandations et fourni plus d'informations dans la section MFA pour l'utilisateur root.	9 novembre 2023
Publication initiale	—	27 octobre 2023

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.

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les 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.