Adopter la confiance zéro : une stratégie pour une transformation métier sécurisée et agile

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Adopter la confiance zéro : une stratégie pour une transformation métier sécurisée et agile

Table of Contents

Adopter la confiance zéro : une stratégie pour une transformation métier sécurisée et agile

Greg Gooden, Amazon Web Services (AWS)

Décembre 2023 (historique du document)

Aujourd'hui, plus que jamais, les entreprises placent la sécurité au centre de leurs priorités. Cela leur permet de bénéficier d'un large éventail d'avantages, tels que le maintien de la confiance de leurs clients, l'amélioration de la mobilité de leur main-d'œuvre ou la création d'opportunités commerciales numériques. Ce faisant, ils continuent de se poser la même question : quels sont les modèles optimaux pour garantir les niveaux de sécurité et de disponibilité adéquats pour mes systèmes et mes données ? Le terme Confiance zéro est de plus en plus utilisé pour décrire la réponse moderne à cette question.

L'architecture confiance zéro (ZTA) est un modèle conceptuel et un ensemble de mécanismes associés qui visent à fournir des contrôles de sécurité autour des ressources numériques qui ne dépendent pas uniquement ou fondamentalement des contrôles réseau traditionnels ou de l'environnement du réseau. Au lieu de cela, les contrôles réseau sont complétés par l'identité, l'appareil, le comportement et d'autres contextes et signaux riches afin de prendre des décisions d'accès plus précises, intelligentes, adaptatives et continues. En implémentant un modèle de ZTA, vous pouvez réaliser une prochaine itération significative dans une évolution continue de la cybersécurité et des concepts de défense en profondeur en particulier.

Processus de prise de décision

La mise en œuvre d'une stratégie ZTA nécessite une planification et une prise de décision minutieuses. Il s'agit d'évaluer divers facteurs et de les aligner sur les objectifs organisationnels. Les principaux processus de prise de décision pour entreprendre le parcours vers la ZTA sont les suivants :

1. Engagement des parties prenantes : il est essentiel d'impliquer d'autres CxO, VP et senior managers afin de comprendre leurs priorités, leurs préoccupations et leur vision du niveau de sécurité de votre organisation. En impliquant les principales parties prenantes dès le départ, vous pouvez aligner l'implémentation de la ZTA sur les objectifs stratégiques globaux et obtenir le soutien et les ressources nécessaires.

2. Évaluation des risques : la réalisation d'une évaluation complète des risques permet d'identifier les problèmes, la surface excessive et les ressources critiques afin de prendre des décisions éclairées en matière de contrôles de sécurité et d'investissement. Évaluez le niveau de sécurité actuel de votre organisation, identifiez les faiblesses potentielles et priorisez les domaines à améliorer en fonction du contexte des risques propre à votre secteur d'activité et à votre environnement opérationnel.
3. Évaluation de la technologie : l'évaluation du paysage technologique existant de l'organisation et l'identification des lacunes permettent de sélectionner des outils et des solutions appropriés conformes aux principes de la ZTA. Cette évaluation doit inclure une analyse approfondie des éléments suivants :
    - Architecture réseau
    - Systèmes de gestion des identités et des accès
    - Mécanismes d'authentification et d'autorisation
    - Gestion unifiée des points de terminaison
    - Outils et processus de propriété des ressources
    - Technologies de chiffrement
    - Fonctionnalités de surveillance et de journalisation
    - Le choix de la bonne pile technologique est crucial pour créer un modèle de ZTA robuste.
4. Gestion du changement : il est essentiel de reconnaître les impacts culturels et organisationnels liés à l'adoption d'un modèle de ZTA. La mise en œuvre de pratiques de gestion du changement contribue à garantir une transition et une acceptation harmonieuses à travers l'organisation. Cela implique de sensibiliser les employés aux principes et aux avantages de la ZTA, de dispenser une formation sur les nouvelles pratiques de sécurité et de promouvoir une culture soucieuse de la sécurité qui encourage la responsabilité et l'apprentissage continu.

Ces directives prescriptives visent à fournir aux CxO, aux VP et aux senior managers une stratégie complète pour l'implémentation de la ZTA. Elles couvriront les principaux aspects de la ZTA, dont les suivants :

- État de préparation organisationnelle
- Approches d'adoption progressive
- Collaboration des parties prenantes
- Bonnes pratiques pour réaliser une transformation métier sûre et agile

En suivant ces conseils, votre organisation peut se frayer un chemin dans le paysage de la ZTA et réussir sa transition vers la sécurité dans le Cloud Amazon Web Services (AWS). AWS propose une variété de services que vous pouvez utiliser pour implémenter une ZTA, tels que Accès vérifié par AWS, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway et Amazon GuardDuty. Ces services peuvent contribuer à protéger les ressources AWS contre tout accès non autorisé.

Résultats commerciaux ciblés

Cette section décrit les résultats attendus associés à la définition et à l'implémentation d'une architecture confiance zéro au sein de votre organisation.

Niveau de sécurité amélioré

En adoptant les principes de confiance zéro, votre entreprise peut renforcer son niveau de sécurité, atténuer les risques de sécurité, mais aussi protéger votre infrastructure et vos données cloud. Le principe fondamental de la confiance zéro qui consiste à accorder l'accès sur la base du besoin de savoir, associé à des contrôles stricts, réduit considérablement la surface et limite l'impact potentiel des événements de sécurité. Cette approche proactive permet aux organisations de garder une longueur d'avance sur les risques de sécurité émergents et de garantir la confidentialité, l'intégrité et la disponibilité des ressources.

Adoption transparente du cloud

L'élaboration d'un plan d'adoption d'une architecture confiance zéro (ZTA) bien défini peut contribuer à garantir une transition fluide et fructueuse vers l'environnement cloud. Les principes de la ZTA s'alignent étroitement sur les bonnes pratiques en matière de sécurité du cloud en fournissant aux organisations une base solide leur permettant de bénéficier en toute sécurité des avantages du cloud computing. L'intégration des principes de la ZTA dès le départ aide votre entreprise à concevoir son architecture cloud en plaçant la sécurité au cœur de ses préoccupations.

Conformité et alignement réglementaire

La mise en œuvre des pratiques de la ZTA peut aider votre organisation à répondre aux exigences et aux normes sectorielles et réglementaires. La ZTA promeut intrinsèquement le principe du moindre privilège et applique des contrôles d'accès stricts. Les contrôles d'accès sont souvent imposés par des réglementations telles que les suivantes :

- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)
- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS).

En adoptant la confiance zéro, votre entreprise peut contribuer à démontrer son engagement en matière de protection des données, de confidentialité et de conformité réglementaire, tout en minimisant les risques de pénalités ou d'atteinte à la réputation.

Protection des données améliorée

Les organisations peuvent protéger les données sensibles tout au long du processus d'adoption du cloud en mettant en œuvre le chiffrement des données, des contrôles d'accès et des évaluations de sécurité régulières. Votre organisation peut prendre les mesures spécifiques suivantes :

- Chiffrement des données : le chiffrement des données est le processus qui consiste à chiffrer des données en texte clair en texte chiffré de manière à ce qu'une clé soit nécessaire pour déchiffrer les données et les restituer sous leur forme d'origine en texte clair. Il est donc beaucoup plus difficile pour les personnes non autorisées d'accéder aux données sensibles, même si elles sont en mesure d'obtenir une copie des données.
- Contrôles d'accès : les contrôles d'accès limitent les personnes autorisées à accéder aux données sensibles et ce qu'elles peuvent en faire. Cela peut être fait en attribuant des rôles et des autorisations aux utilisateurs, et en utilisant l'authentification multifactorielle ou d'autres méthodes pour vérifier l'identité des utilisateurs.
- Évaluations de sécurité régulières : les évaluations de sécurité régulières peuvent aider les organisations à identifier et à résoudre les problèmes de sécurité et à y remédier de manière proactive. Ces évaluations peuvent être menées par des équipes de sécurité internes ou par des sociétés de sécurité externes.

Les architectures confiance zéro adoptent une approche globale de la protection des données en mettant en œuvre un certain nombre de mesures de sécurité. Ces mesures incluent une authentification forte, le chiffrement des données et des contrôles d'accès précis. Cette approche minimise le risque d'événements de sécurité liés aux données et protège les informations sensibles contre tout accès non autorisé.

Réponse aux incidents efficace

Les organisations peuvent détecter les événements de sécurité et y répondre plus rapidement et plus efficacement en établissant des cadres de surveillance et de réponse aux incidents dans l'environnement cloud. Les architectures confiance zéro mettent l'accent sur la surveillance continue, l'intégration de renseignements sur les menaces et la visibilité en temps réel des activités des

utilisateurs, du trafic réseau et du comportement du système. Les équipes de sécurité peuvent ensuite identifier et atténuer de manière proactive les événements de sécurité. Cette approche réduit le temps nécessaire pour détecter les problèmes potentiels et y répondre, tout en minimisant l'impact sur les opérations métier. Les points clés sont les suivants :

- Tests : quel que soit le cadre ou la méthodologie de réponse aux incidents sur lesquels s'aligne votre organisation, vous devez tester régulièrement votre plan de réponse aux incidents. Les exercices de simulation, les simulations et les tests et équipe rouge (Red Teaming) permettent de s'entraîner à répondre aux incidents dans des contextes réalistes, de découvrir les lacunes en matière d'outillage et de capacités, mais aussi de renforcer l'expérience et la confiance des personnes chargées de répondre aux incidents.
- Surveillance : surveillez en permanence vos environnements cloud pour détecter tout signe d'activité anormale. Pour ce faire, vous pouvez utiliser divers outils et techniques, tels que l'analyse des journaux, la surveillance du réseau et l'analyse des vulnérabilités.
- Intégration des renseignements sur les menaces : intégrez les renseignements sur les menaces dans vos cadres de surveillance et de réponse aux incidents. Cela aidera votre entreprise à identifier les menaces et à y répondre plus rapidement et plus efficacement.
- Visibilité en temps réel : pour identifier les incidents de sécurité et y répondre rapidement, votre entreprise a besoin d'une visibilité en temps réel sur les activités des utilisateurs, le trafic réseau et le comportement du système.
- Identification et atténuation proactives : en identifiant et en atténuant de manière proactive les événements de sécurité, votre organisation peut réduire le temps nécessaire pour détecter les menaces potentielles et y répondre, et ainsi minimiser l'impact sur les opérations métier.

Amélioration de la productivité de la main-d'œuvre

La main-d'œuvre moderne a besoin de flexibilité pour travailler à partir d'un nombre croissant de lieux, d'appareils et d'horaires. En mettant en œuvre une ZTA, vous pouvez répondre à ces exigences et améliorer la mobilité, la productivité et la satisfaction du personnel, tout en maintenant ou en améliorant le niveau de sécurité de l'organisation.

Permettre la transformation numérique

Les organisations cherchent de plus en plus à interconnecter les appareils, les machines, les installations, les infrastructures et les processus en dehors du périmètre réseau traditionnel

dans le cadre de la transformation numérique. Les appareils liés à l'Internet des objets (IoT) et à la technologie opérationnelle (OT, également appelés Internet industriel des objets, ou IIoT) transmettent souvent des informations de télémétrie et de maintenance prédictive directement au cloud. La protection des charges de travail implique l'application de contrôles de sécurité qui vont au-delà de l'approche périmétrique traditionnelle.

Récapitulatif de la section

En se concentrant sur ces résultats commerciaux ciblés, votre entreprise peut exploiter tout le potentiel de la ZTA et renforcer son niveau de sécurité dans le cloud. Il est important d'aligner ces résultats sur les objectifs organisationnels spécifiques, de les adapter à vos exigences métier particulières et d'évaluer régulièrement leur efficacité afin d'assurer une amélioration continue.

Comprendre les principes de confiance zéro

L'architecture confiance zéro (ZTA) repose sur un ensemble de principes fondamentaux qui constituent la base de son modèle de sécurité. La compréhension de ces principes est essentielle pour les organisations qui cherchent à adopter efficacement une stratégie ZTA. Cette section couvre les principes fondamentaux de la ZTA.

Vérification et authentification

Le principe de vérification et d'authentification souligne l'importance d'une identification et d'une authentification solides pour les principaux de tous types, y compris les utilisateurs, les machines et les appareils. La ZTA exige une vérification continue des identités et de l'état d'authentification tout au long d'une session, idéalement à chaque demande. Elle ne repose pas uniquement sur les contrôles ou l'emplacement réseau traditionnels. Cela inclut l'implémentation d'une authentification multifactorielle (MFA) forte et moderne, ainsi que l'évaluation de signaux environnementaux et contextuels supplémentaires lors des processus d'authentification. En adoptant ce principe, les organisations peuvent contribuer à garantir que les décisions d'autorisation des ressources prennent en compte les meilleures données d'identité possibles.

Accès sur la base du moindre privilège

Le principe du moindre privilège implique d'accorder aux principaux le niveau d'accès minimum requis pour effectuer leurs tâches. En adoptant le principe d'accès sur la base du moindre privilège, les entreprises peuvent appliquer des contrôles d'accès précis, de sorte que les principaux n'aient accès qu'aux ressources nécessaires pour s'acquitter de leurs rôles et responsabilités. Il s'agit notamment d'implémenter une allocation d'accès juste-à-temps, des contrôles d'accès basés sur les rôles (RBAC) et des examens d'accès réguliers afin de minimiser la surface et le risque d'accès non autorisé.

Microsegmentation

La microsegmentation est une stratégie de sécurité réseau qui divise un réseau en segments isolés plus petits afin d'autoriser des flux de trafic spécifiques. Vous pouvez réaliser une microsegmentation en définissant des limites de charge de travail et en appliquant des contrôles d'accès stricts entre les différents segments.

La microsegmentation peut être mise en œuvre par le biais de la virtualisation du réseau, d'un réseau défini par logiciel (SDN), de pare-feux basés sur l'hôte, de listes de contrôle d'accès réseau (NACL) et des fonctionnalités spécifiques à AWS telles que les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) ou AWS PrivateLink. Les passerelles de segmentation contrôlent le trafic entre les segments pour autoriser explicitement l'accès. La microsegmentation et les passerelles de segmentation aident les entreprises à limiter les chemins inutiles à travers le réseau, en particulier celles qui mènent à des systèmes et à des données critiques.

Surveillance et analytique continues

La surveillance et l'analytique continues impliquent la collecte, l'analyse et la corrélation d'événements et de données liés à la sécurité à travers l'environnement de votre organisation. En mettant en œuvre des outils de surveillance et d'analytique robustes, votre entreprise peut évaluer les données de sécurité et la télémétrie de manière convergée.

Ce principe souligne l'importance de la visibilité sur le comportement des utilisateurs, le trafic réseau et les activités du système pour identifier les anomalies et les événements de sécurité potentiels. Les technologies avancées telles que la gestion des informations et des événements de sécurité (SIEM), l'analytique du comportement des utilisateurs et des entités (UEBA) et les plateformes de renseignement sur les menaces jouent un rôle essentiel dans la mise en place d'une surveillance continue et d'une détection proactive des menaces.

Automatisation et orchestration

L'automatisation et l'orchestration aident les entreprises à simplifier les processus de sécurité, à réduire les interventions manuelles et à améliorer les temps de réponse. En automatisant les tâches de sécurité routinières et en recourant à des fonctionnalités d'orchestration, votre organisation peut appliquer des politiques de sécurité cohérentes et réagir rapidement aux événements de sécurité. Ce principe inclut également l'automatisation des processus de provisionnement et de déprovisionnement des accès afin de garantir une gestion rapide et précise des autorisations des utilisateurs. En adoptant l'automatisation et l'orchestration, votre organisation peut améliorer son efficacité opérationnelle, réduire le nombre d'erreurs humaines et concentrer ses ressources sur des initiatives de sécurité plus stratégiques.

Autorisation

Dans une ZTA, chaque demande d'accès à une ressource doit être explicitement autorisée par un point d'application de la consignation. Outre l'identité authentifiée, les politiques d'autorisation doivent prendre en compte un contexte supplémentaire, tel que l'état et la posture de l'appareil, les modèles de comportement, le classement des ressources et les facteurs liés au réseau. Le processus d'autorisation doit évaluer ce contexte convergent par rapport aux politiques d'accès correspondantes applicables à la ressource à laquelle on accède. De manière optimale, les modèles de machine learning peuvent fournir un complément dynamique aux politiques déclaratives. Lorsqu'ils sont utilisés, ces modèles doivent se concentrer uniquement sur des restrictions supplémentaires et ne pas accorder d'accès qui n'a pas été explicitement spécifié.

Récapitulatif de la section

En adhérant à ces principes fondamentaux de la ZTA, les entreprises peuvent établir un modèle de sécurité robuste adapté à la diversité de l'environnement d'entreprise moderne. L'implémentation de ces principes nécessite une approche globale qui combine la technologie, les processus et les personnes afin de parvenir à un état d'esprit de confiance zéro et de mettre en place un niveau de sécurité résilient.

Composants clés d’une architecture confiance zéro

Pour mettre en œuvre efficacement une stratégie d’architecture confiance zéro (ZTA), votre organisation doit comprendre les principaux éléments qui constituent une ZTA. Ces composants fonctionnent de concert pour améliorer en permanence un modèle de sécurité complet conforme aux principes de confiance zéro. Cette section aborde les éléments clés d’une ZTA.

Gestion des identités et des accès

La gestion des identités et des accès constitue la base d’une ZTA en fournissant une authentification utilisateur robuste et des mécanismes de contrôle d’accès à grain grossier. Elle inclut des technologies telles que l’authentification unique (SSO), l’authentification multifactorielle (MFA) et des solutions de gouvernance et de gestion des identités. La gestion des identités et des accès fournit un niveau élevé d’assurance de l’authentification et un contexte important qui font partie intégrante de la prise de décisions d’autorisation de confiance zéro. Dans le même temps, la ZTA est un modèle de sécurité dans lequel l’accès aux applications et aux ressources est accordé par utilisateur, par appareil et par session. Cela permet de protéger les organisations contre tout accès non autorisé, même si les informations d’identification d’un utilisateur sont compromises.

Secure Access Service Edge

Un Secure Access Service Edge (SASE) est une nouvelle approche de la sécurité réseau qui virtualise, combine et distribue les fonctions réseau et de sécurité au sein d’un seul service basé sur le cloud. Le SASE peut fournir un accès sécurisé aux applications et aux ressources, quel que soit l’emplacement de l’utilisateur.

Le SASE inclut diverses fonctionnalités de sécurité, telles que des passerelles Web sécurisées, un pare-feu en tant que service et un accès réseau de confiance zéro (ZTNA). Ces fonctionnalités fonctionnent de concert pour protéger les organisations contre les menaces les plus variées, notamment les logiciels malveillants, l’hameçonnage et les rançongiciels.

Prévention des pertes de données

Les technologies de prévention des pertes de données (DLP) peuvent aider les organisations à protéger les données sensibles contre toute divulgation non autorisée. Les solutions DLP surveillent et contrôlent les données en mouvement et au repos. Cela permet aux organisations de définir

et d'appliquer des politiques qui empêchent les événements de sécurité liés aux données, en garantissant ainsi la protection des informations sensibles sur l'ensemble du réseau.

Gestion des informations et des événements de sécurité

Les solutions de gestion des informations et des événements de sécurité (SIEM) collectent, regroupent et analysent les journaux des événements de sécurité provenant de diverses sources au sein de l'infrastructure d'une organisation. Vous pouvez utiliser ces données pour détecter les incidents de sécurité, faciliter la réponse aux incidents et fournir des informations sur les menaces et les vulnérabilités potentielles.

Pour la ZTA en particulier, la capacité d'une solution de SIEM à corréler et à comprendre la télémétrie associée à partir de différents systèmes de sécurité est essentielle pour améliorer la détection et la réponse aux modèles anormaux.

Catalogue de la propriété des ressources de l'entreprise

Pour accorder correctement l'accès aux ressources de l'entreprise, une organisation doit disposer d'un système fiable qui catalogue ces ressources et, surtout, qui en est le propriétaire. Cette source de vérité doit fournir des flux de travail qui facilitent les demandes d'accès, les décisions d'approbation associées et les attestations régulières. À terme, cette source de vérité contiendra les réponses à la question « qui peut accéder à quoi ? » au sein de l'organisation. Vous pouvez utiliser les réponses à la fois pour l'autorisation, l'audit et la conformité.

Gestion unifiée des points de terminaison

Outre l'authentification forte de l'utilisateur, une ZTA doit également tenir compte de la santé, de la posture et de l'état de l'appareil de l'utilisateur pour évaluer si l'accès aux données et aux ressources de l'entreprise est sécurisé. Une plateforme de gestion unifiée des points de terminaison (UEM) fournit les fonctionnalités suivantes :

- Mise en service des appareils
- Gestion continue de la configuration et des correctifs
- Référencement de sécurité
- Création de rapports de télémétrie
- Nettoyage et mise hors service des appareils

Points d’application basés sur des politiques

Dans une ZTA, l’accès à chaque ressource doit être explicitement autorisé par un point d’application de la consignation basé sur des politiques. Dans un premier temps, ces points d’application peuvent être basés sur les points d’application existants dans les réseaux et les systèmes d’identité existants. Les points d’application peuvent être progressivement renforcés en tenant compte de l’éventail plus large de contextes et de signaux fournis par la ZTA. À plus long terme, votre organisation doit mettre en œuvre des points d’application propres à la ZTA qui fonctionnent dans un contexte convergé, intègrent de manière cohérente les fournisseurs de signaux, maintiennent un ensemble de politiques complet et sont améliorés grâce aux informations recueillies grâce à la télémétrie combinée.

Récapitulatif de la section

La compréhension de ces éléments clés est essentielle pour les organisations qui envisagent d’adopter une ZTA. En mettant en œuvre ces composants et en les intégrant dans un modèle de sécurité cohérent, votre organisation peut établir un solide niveau de sécurité basé sur les principes de confiance zéro. Les sections suivantes explorent l’état de préparation organisationnelle, les approches d’adoption progressive et les bonnes pratiques pour vous aider à correctement mettre en œuvre la ZTA au sein de votre organisation.

Évaluation de l’état de préparation organisationnelle pour l’adoption de la confiance zéro

L’adoption d’une nouvelle stratégie d’architecture est une démarche importante qui nécessite une planification minutieuse et la prise en compte de facteurs organisationnels. Cette section se concentre sur les principales considérations relatives à l’état de préparation organisationnelle pour l’adoption de la confiance zéro à travers l’entreprise. En tenant compte de ces considérations, votre organisation peut jeter les bases d’un niveau de sécurité plus solide et plus efficace.

Alignement du leadership et communication

L’alignement du leadership et la communication sont essentiels à la réussite de l’implémentation de la confiance zéro. Les dirigeants doivent comprendre les avantages de la confiance zéro et savoir quelles ressources sont nécessaires. Ils doivent également être prêts à apporter des changements à la culture et aux processus de l’organisation. La communication avec les employés est nécessaire pour renforcer la confiance et l’adhésion. Les employés doivent comprendre pourquoi l’organisation met en œuvre la confiance zéro, ce que cela signifie pour eux et comment ils peuvent apporter leur aide. La communication doit être ouverte, transparente et constante.

Soutien et adhésion des dirigeants

Pour réussir l’implémentation de l’architecture confiance zéro (ZTA), il est essentiel d’aligner les principales parties prenantes et les dirigeants sur les objectifs, les avantages et les mesures de réussite de l’architecture. Partagez l’importance des principes de confiance zéro pour améliorer la sécurité et permettre l’agilité métier en délaissant la sécurité traditionnelle basée sur le périmètre au profit d’une approche plus précise et axée sur l’utilisateur. En optant pour cette approche, votre entreprise peut s’adapter plus rapidement aux changements et aux menaces. L’alignement de la direction donne le ton à l’organisation et aide à lever les réticences potentielles au changement.

Communication transparente

Maintenez une communication ouverte et transparente avec les employés tout au long du processus d’implémentation de la confiance zéro. Expliquez les raisons, les avantages et les résultats escomptés de l’adoption et répondez rapidement aux préoccupations. Faites régulièrement le point sur l’état d’avancement de l’implémentation. Cela permettra d’accroître l’adhésion, de réduire la résistance et d’établir la confiance.

Développement des compétences et formation

Une fois que l'alignement de direction est acquis et que la communication est ouverte, il est important de développer les compétences et les connaissances des employés qui se chargeront de l'implémentation de la confiance zéro. Cela inclut la compréhension des principes de confiance zéro, ainsi que la manière de les implémenter dans leur travail et de réagir face aux événements de sécurité. Proposez des possibilités de formation et de développement pour aider les employés à acquérir ces compétences.

Connaissances et compétences en matière de cloud

Évaluez les compétences et les lacunes de l'organisation en matière de connaissances sur les technologies cloud et les principes de la confiance zéro. Proposez des programmes de formation et de développement pour améliorer les compétences des employés et les doter de l'expertise nécessaire pour travailler efficacement dans un environnement axé sur le cloud et la confiance zéro. Pour suivre le rythme de l'évolution des technologies et des pratiques de sécurité, encouragez une culture d'apprentissage continu.

Culture de la sécurité et sensibilisation

Évaluez la culture de la sécurité de l'organisation. Évaluez le niveau de sensibilisation des employés à la sécurité, leur compréhension des bonnes pratiques en la matière et leur adhésion aux politiques et procédures. Identifiez les lacunes au niveau des connaissances en matière de sécurité. Envisagez d'organiser des programmes de formation à la sécurité pour sensibiliser les employés à l'importance du principe de confiance zéro et à leur rôle de garant de la sécurité de l'environnement.

Structure organisationnelle et rôles

Pour réussir l'implémentation de la confiance zéro, établissez une structure organisationnelle et des rôles efficaces. Cela passe par la création d'un Centre d'excellence cloud (CCoE), l'examen et la modification des opérations de sécurité, ainsi que l'attribution des rôles et des responsabilités en matière de gestion des vulnérabilités, de réponse aux incidents et de surveillance de la sécurité.

Centre d'excellence cloud

Établissez un CCoE pour partager des conseils, des bonnes pratiques et assurer une supervision des opérations dans le cloud. Un CCoE se compose d'une équipe ou d'un groupe de personnes chargé

de créer et de mettre en œuvre les bonnes pratiques, les directives et les politiques de gouvernance liées au cloud. Le CCoE doit inclure des représentants des différentes unités commerciales et équipes informatiques afin de garantir la collaboration et l'alignement. Le CCoE joue un rôle primordial dans l'adoption des principes de confiance zéro dans les charges de travail hébergées dans le cloud. Le CCoE facilite également le partage des connaissances au sein de l'organisation.

Opérations de sécurité

Pour répondre aux besoins d'un environnement de confiance zéro, examinez et modifiez l'organisation actuelle des opérations de sécurité. Pour améliorer les capacités de surveillance, de réponse aux incidents et de renseignement sur les menaces, envisagez de mettre en place des centres des opérations de sécurité (SOC) ou des fournisseurs de services de sécurité gérés (MSSP). Définissez les rôles et les responsabilités en matière de gestion des vulnérabilités, de réponse aux incidents et de surveillance de la sécurité. Un processus de réponse aux incidents efficace est essentiel pour garantir que les événements de sécurité mineurs peuvent être détectés et corrigés rapidement afin de perturber la séquence des événements. Cela permet d'éviter qu'un événement mineur ne se transforme en un événement de plus grande ampleur.

Infrastructure et architecture informatiques

Examinez l'architecture et l'infrastructure informatiques de votre entreprise pour identifier les contraintes ou les dépendances susceptibles d'affecter l'adoption d'une approche de confiance zéro. Déterminez si les applications et systèmes actuels sont compatibles avec les composants architecturaux de confiance zéro requis. Analysez si des améliorations ou des ajustements de l'infrastructure sont nécessaires pour soutenir le succès du déploiement des principes de confiance zéro. Pour chaque application ou système, déterminez s'il est préférable d'implémenter la confiance zéro sur place ou dans le cadre d'un plus vaste effort de modernisation.

Gestion des risques, gouvernance et contrôle du changement

Pour réussir l'implémentation de la confiance zéro, mettez en place des processus efficaces de gestion des risques, de gouvernance et de contrôle du changement. Cela inclut l'alignement de la gestion des risques sur les principes de confiance zéro, l'élaboration d'un plan de réponse aux incidents, la collaboration avec les services juridiques et de conformité, ainsi que la mise en place d'un processus de contrôle du changement.

Gestion des risques

Examinez la stratégie de gestion des risques instaurée dans votre entreprise et déterminez dans quelle mesure elle adhère aux principes de confiance zéro. Analysez l'efficacité des systèmes actuels de réponse aux incidents, des mesures de sécurité et des procédures d'évaluation des risques. Déterminez les domaines qui doivent être améliorés pour se conformer à la stratégie de confiance zéro. Commencez à développer un système de réponse automatique aux incidents ou un cadre de surveillance et d'analytique continus pour accélérer la résolution des incidents.

Processus de contrôle du changement

Pour garantir que toutes les modifications liées au cloud respectent les exigences de sécurité et de conformité, établissez des méthodes efficaces de contrôle du changement. Établissez une procédure systématique de gestion du changement qui inclut l'analyse de la configuration de sécurité, les évaluations des risques, les approbations et la documentation. Examinez et vérifiez fréquemment les mises à jour afin de préserver l'intégrité de l'architecture confiance zéro.

Surveillance et évaluation

Pour réussir l'implémentation de la confiance zéro, votre organisation doit surveiller et évaluer en permanence son niveau de sécurité. Cela comprend l'établissement d'indicateurs de performance clés (KPI), la surveillance et l'évaluation des KPI, ainsi que la promotion d'une culture d'amélioration continue. En suivant ces étapes, les organisations peuvent s'assurer que leur mise en œuvre de la confiance zéro est réussie et qu'elles œuvrent toujours à l'amélioration de leur sécurité.

Indicateurs de performance clés

Établissez des indicateurs de performance clés (KPI) pertinents pour évaluer le succès et l'efficacité du déploiement de la confiance zéro. Ces KPI peuvent mesurer la satisfaction des utilisateurs, la progression de l'équipement et du déploiement, la réduction des coûts, le respect de la conformité et le nombre d'incidents de sécurité. Pour suivre le développement global et identifier les possibilités d'amélioration, surveillez et évaluez régulièrement ces KPI.

Amélioration continue

La mise en place de systèmes permettant de recueillir les opinions et les points de vue des parties prenantes contribuera à encourager une culture d'amélioration continue. Encouragez les membres du personnel à faire part de leurs réflexions et propositions pour améliorer la sécurité, l'efficacité et l'expérience utilisateur de l'environnement cloud. Utilisez ces informations pour simplifier les procédures, améliorer les mesures de sécurité et stimuler l'innovation.

Récapitulatif de la section

En tenant compte de ces considérations organisationnelles et culturelles, votre organisation peut créer un environnement favorable à l'adoption d'un modèle de sécurité de confiance zéro dans le cloud. La section suivante aborde les approches d'adoption progressive et fournit des conseils sur la manière d'implémenter progressivement les principes de confiance zéro de façon pratique et gérable.

Cultiver un état d'esprit Zero Trust

La mise en œuvre du Zero Trust va au-delà des implémentations techniques. Cela nécessite un changement culturel au sein de votre organisation. Favoriser un état d'esprit Zero Trust implique de mettre l'accent sur les aspects clés suivants.

Éducation et formation Zero Trust

Renseignez les employés sur les valeurs et les avantages de l'architecture Zero Trust (ZTA). Fournissez des explications techniques et non techniques des concepts et des approches de la ZTA par le biais de sessions de formation, d'ateliers et d'autres ressources. Encouragez les membres du personnel à prendre conscience de leurs responsabilités dans l'établissement et le maintien d'un paradigme de sécurité Zero Trust.

Collaboration et communication

Favorisez la collaboration et la transparence entre toutes les équipes et tous les services impliqués dans la mise en œuvre de la ZTA. Pour que tout le monde comprenne parfaitement le plan, favorisez la communication interfonctionnelle, le partage des connaissances et l'échange d'informations. Créez une culture de responsabilité partagée où chacun reconnaît l'importance de sa contribution à la sécurité globale de l'entreprise.

Apprentissage et amélioration continus

Donnez la priorité à l'apprentissage et à l'amélioration continus dans le contexte du Zero Trust. Encouragez les employés à se tenir au courant des dernières tendances, technologies et meilleures pratiques en matière de sécurité. Favorisez une culture d'innovation et d'expérimentation dans laquelle les employés sont encouragés à explorer de nouvelles solutions et approches pour renforcer la posture de sécurité de l'organisation.

Métriques et responsabilité

Établissez des indicateurs et des mécanismes de responsabilité clairs pour mesurer l'efficacité de la stratégie Zero Trust. Définissez des indicateurs de performance clés (KPI) qui correspondent aux objectifs de sécurité de l'organisation et suivez régulièrement les progrès. Tenez les individus et les

équipes responsables de leur contribution à la mise en œuvre et au maintien des principes Zero Trust.

Résumé de la section

En abordant ces aspects et en cultivant un état d'esprit Zero Trust, les organisations peuvent créer une base solide pour une adoption et une mise en œuvre réussies du Zero Trust. Ce changement culturel est essentiel pour aider tous les membres de l'organisation à comprendre l'importance du Zero Trust et à contribuer activement à son succès.

La section suivante explore les approches d'adoption par étapes et fournit des conseils sur la manière de mettre en œuvre progressivement les principes du Zero Trust de manière pratique et gérable.

Approche progressive de la confiance zéro

L'adoption d'une architecture confiance zéro (ZTA) nécessite une planification et une implémentation minutieuses. Nous recommandons une approche d'adoption progressive pour que la transition se fasse en douceur et pour minimiser les perturbations dans les activités de l'entreprise. Cette section fournit des conseils sur les principales phases de l'adoption d'une ZTA.

Phase 1 : évaluation et planification

La première phase de l'implémentation de la confiance zéro est l'évaluation et la planification. Cette phase est essentielle au succès de l'implémentation globale, car elle implique d'identifier et de corriger les éventuelles lacunes en ce qui concerne le niveau de sécurité actuel de votre organisation. En prenant le temps d'évaluer votre situation actuelle et de définir vos objectifs de sécurité, vous pouvez jeter les bases d'une implémentation réussie de la confiance zéro.

Dans le même temps, une évaluation parfaitement complète et précise n'est pas toujours réaliste. Pour éviter la paralysie de l'analyse qui vous empêche de passer à d'autres phases, préparez-vous à compartimenter ou à accepter un certain niveau d'imperfection.

1. Évaluation de la situation actuelle : effectuez une évaluation de votre infrastructure, de vos politiques et de vos contrôles de sécurité existants. Identifiez les vulnérabilités potentielles, les failles de sécurité et les domaines dans lesquels l'implémentation des principes de confiance zéro peut apporter des améliorations.
2. Définition des objectifs de sécurité : sur la base des résultats de l'évaluation de la situation actuelle, définissez des objectifs de sécurité qui adhèrent aux principes de confiance zéro. Ces objectifs de sécurité doivent également s'aligner sur la stratégie de sécurité globale de votre entreprise et remédier aux vulnérabilités et aux lacunes identifiées.
3. Conception de l'architecture : développez une ZTA qui soutient les objectifs de sécurité de votre entreprise. Cette architecture doit inclure les composants nécessaires, tels que des solutions de gestion des identités et des accès, des mécanismes de segmentation du réseau et des systèmes de surveillance continue. L'architecture doit également être évolutive, adaptable et capable de faire face à la croissance et aux progrès technologiques de demain. Idéalement, cette architecture devrait être représentée dans un format facile à utiliser par les équipes chargées de l'implémenter, comme un modèle AWS CloudFormation, et pas simplement sous forme de document ou de diagramme.

4. Impliquer les parties prenantes : impliquez toutes les parties prenantes, y compris les unités commerciales, les équipes informatiques et les équipes de sécurité, pour obtenir des informations et aligner leurs objectifs sur le plan d'implémentation de la ZTA. Encouragez la collaboration et la communication pour établir une compréhension commune des avantages et des exigences de l'approche de confiance zéro.

Phase 2 : Pilotage et implémentation

La deuxième phase de l'implémentation de la confiance zéro est le pilotage et l'implémentation. Cette phase consiste à tester la ZTA dans un environnement contrôlé à petite échelle, puis à la déployer de manière itérative au sein de votre organisation. Il est important de sensibiliser les employés aux nouvelles mesures de sécurité et à leur rôle dans le maintien d'un environnement de confiance zéro.

1. Piloter le déploiement : testez la ZTA dans un environnement contrôlé à petite échelle. Mettez en œuvre les composants et les contrôles de sécurité nécessaires définis lors de la phase de conception de l'architecture. Surveillez de près le déploiement du pilote, recueillez des commentaires et apportez les ajustements nécessaires. Soyez prêt à faire preuve de flexibilité dès le début du processus, lorsque la confiance zéro passe d'un exercice hypothétique à un exercice permettant d'acquérir une réelle expérience.
2. Déploiement itératif : sur la base des leçons tirées du déploiement pilote, commencez le déploiement itératif de confiance zéro au sein de l'organisation. Créez une dynamique grâce à un effet de volant d'inertie qui ne nécessite pas de campagne de grande envergure pour atteindre une masse de déploiement critique. Réserver les mandats de la direction ou les escalades pour la partie la plus longue du déploiement où ils pourraient s'avérer nécessaires.
3. Formation et sensibilisation des utilisateurs : sensibilisez les employés aux nouvelles mesures de sécurité et à leurs rôles dans le maintien d'un environnement de confiance zéro. Soulignez l'importance des pratiques sécurisées, telles que les mots de passe forts, l'authentification multifactorielle et les mises à jour de sécurité régulières.
4. Gestion du changement : créez un plan complet de gestion du changement pour faire face aux changements organisationnels et culturels associés à l'adoption de la confiance zéro. Présentez aux employés les avantages et les raisons de l'adoption, et répondez à leurs préoccupations ou à leurs réticences. Apportez un soutien et des conseils continus pour permettre une transition harmonieuse.

Phase 3 : Surveillance et amélioration continue

La troisième et dernière phase de l'implémentation de la confiance zéro est le suivi et l'amélioration continue. Cette phase consiste à établir un programme complet de surveillance et d'analytique, à créer un plan complet de réponse aux incidents et à solliciter régulièrement les commentaires des parties prenantes et des utilisateurs.

1. Surveillance continue : établissez un programme complet de surveillance et d'analytique pour évaluer en permanence le niveau de sécurité et détecter toute anomalie potentielle. Utilisez des outils et des technologies de sécurité avancés pour surveiller le comportement des utilisateurs, le trafic réseau et les activités du système.
2. Planification de la réponse aux incidents et de leur résolution : réez un plan complet de réponse aux incidents conforme aux principes de confiance zéro. Établissez des processus d'escalade clairs, définissez les rôles et les responsabilités et mettez en œuvre des mécanismes automatisés de réponse aux incidents dans la mesure du possible. Testez et mettez à jour régulièrement le plan de réponse aux incidents.
3. Obtention de commentaires et d'évaluations : sollicitez régulièrement les commentaires des parties prenantes et des utilisateurs afin de recueillir des informations sur l'efficacité de l'architecture confiance zéro (ZTA). Réalisez des évaluations périodiques pour mesurer l'impact sur le niveau de sécurité, l'efficacité opérationnelle et l'expérience utilisateur. Utilisez les commentaires et les résultats des évaluations pour identifier les domaines à améliorer. Attendez-vous à ce que vos ZTA changent au fil du temps et réfléchissez à la manière dont les équipes de développement mettront en œuvre ces mises à jour avec un minimum d'efforts ou de perturbations.

Récapitulatif de la section

En suivant cette approche d'adoption progressive, les entreprises peuvent effectuer une transition efficace vers une ZTA tout en minimisant les risques et les perturbations. La section suivante décrit les bonnes pratiques pour réussir l'implémentation de la confiance zéro, en abordant les principales considérations et recommandations pour les CxO, les vice-présidents et les cadres supérieurs.

Bonnes pratiques pour réussir avec la confiance zéro

L'adoption réussie de l'architecture confiance zéro (ZTA) nécessite une approche stratégique et le respect des bonnes pratiques. Cette section présente un ensemble de bonnes pratiques pour aider les CXO, les VP et les senior managers à réussir leur adoption de la confiance zéro. En suivant ces recommandations, votre organisation peut établir une base de sécurité solide et profiter des avantages d'une approche de confiance zéro :

- Définir des objectifs et des résultats métier clairs : définissez clairement les objectifs et les résultats métier souhaités des opérations cloud. Alignez ces objectifs sur les principes de la confiance zéro afin de créer une base de sécurité solide tout en favorisant la croissance de l'activité et l'innovation.
- Réaliser une évaluation complète : effectuez une évaluation complète de l'infrastructure informatique, des applications et des ressources de données actuelles. Identifiez les dépendances, les dettes techniques et les problèmes de compatibilité potentiels. Cette évaluation éclairera le plan d'adoption et contribuera à prioriser les charges de travail en fonction de leur gravité, de leur complexité et de leur impact métier.
- Élaborer un plan d'adoption : intégrez un plan d'adoption détaillé qui décrit l'approche étape par étape pour transférer les charges de travail, les applications et les données vers le cloud. Définissez les phases d'adoption, les délais et les dépendances. Impliquez les principales parties prenantes et allouez les ressources en conséquence.
- Commencer à créer tôt : votre capacité à représenter de manière authentique ce à quoi ressemblera la confiance zéro au sein de votre organisation s'améliorera considérablement une fois que vous aurez commencé à le créer et à le déployer (plutôt que de l'analyser et d'en parler).
- Obtenir le parrainage de la direction : obtenez le parrainage de la direction et le soutien nécessaires à l'implémentation de la confiance zéro. Mobilisez d'autres cadres supérieurs pour qu'ils défendent l'initiative et allouent les ressources nécessaires. L'engagement de la direction est essentiel pour apporter les changements culturels et organisationnels nécessaires à une implémentation réussie.
- Mettre en œuvre un cadre de gouvernance : créez un cadre de gouvernance qui définit les rôles, les responsabilités et les processus décisionnels pour l'implémentation de la confiance zéro. Définissez clairement la responsabilité et la propriété des contrôles de sécurité, de la gestion des risques et de la conformité. Examinez et mettez à jour régulièrement le cadre de gouvernance afin de l'adapter à l'évolution des exigences de sécurité.
- Favoriser la collaboration interfonctionnelle : encouragez la collaboration et la communication entre les différentes unités commerciales, équipes informatiques et équipes de sécurité. Créez

une culture de responsabilité partagée afin de favoriser l'alignement et la coordination tout au long de l'implémentation de la confiance zéro. Encouragez des interactions, des partages de connaissances et des résolutions conjointes de problèmes réguliers.

- Sécuriser vos données et vos applications : la confiance zéro ne concerne pas uniquement l'accès des utilisateurs finaux aux ressources et aux applications. Les principes de confiance zéro doivent également être implémentés au sein des charges de travail et entre celles-ci. Appliquer les mêmes principes techniques (identité forte, microsegmentation et autorisation) en utilisant également l'intégralité du contexte disponible au sein du centre de données.
- Proposer une défense en profondeur : mettez en œuvre une stratégie de défense en profondeur en utilisant plusieurs niveaux de contrôles de sécurité. Combinez différentes technologies de sécurité, telles que l'authentification multifactorielle (MFA), la segmentation du réseau, le chiffrement et la détection des anomalies, pour fournir une protection complète. Assurez-vous que chaque couche vient compléter les autres pour créer un système de défense solide.
- Exiger une authentification renforcée : appliquez des mécanismes d'authentification forts, tels que la MFA, pour tous les utilisateurs accédant à toutes les ressources. Idéalement, considérez la MFA moderne, comme les clés de sécurité matérielles FIDO2, qui fournit un haut niveau de garantie d'authentification pour la confiance zéro et qui présente de nombreux avantages en matière de sécurité (par exemple, une protection contre l'hameçonnage).
- Centraliser et améliorer les autorisations : autorisez spécifiquement chaque tentative d'accès. En fonction des spécificités du protocole, cette opération doit être effectuée par connexion ou par demande. La méthode par demande est recommandée. Utilisez tous les contextes disponibles, notamment les informations relatives à l'identité, à l'appareil, au comportement et au réseau, pour prendre des décisions d'autorisation plus précises, adaptatives et sophistiquées.
- Utiliser le principe du moindre privilège : mettez en œuvre le principe du moindre privilège pour accorder aux utilisateurs les droits d'accès minimum requis pour mener leurs tâches à bien. Examinez et mettez à jour régulièrement les autorisations d'accès en fonction des rôles, des responsabilités et des besoins métier. Implémentez une allocation d'accès juste-à-temps.
- Utiliser la gestion des accès privilégiés : implémentez une solution de gestion des accès privilégiés (PAM) pour sécuriser les comptes privilégiés et réduire le risque d'accès non autorisé aux systèmes critiques. Les solutions de PAM peuvent fournir des contrôles d'accès privilégiés, ainsi que des fonctionnalités d'enregistrement de session et d'audit pour aider votre entreprise à protéger ses données et ses systèmes les plus sensibles.
- Utiliser la microsegmentation : divisez votre réseau en segments plus petits et plus isolés. Utilisez la microsegmentation pour appliquer des contrôles d'accès stricts entre les segments en fonction

des rôles des utilisateurs, des applications ou de la sensibilité des données. Efforcez-vous d'éliminer tous les chemins d'accès réseau inutiles, en particulier ceux qui mènent aux données.

- Surveiller les alertes de sécurité et y répondre : mettez en œuvre un programme complet de surveillance de la sécurité et de réponse aux incidents dans l'environnement cloud. Utilisez des outils et des services de sécurité natifs cloud pour détecter les menaces en temps réel, analyser les journaux et automatiser la réponse aux incidents. Établissez des procédures claires de réponse aux incidents, effectuez des évaluations de sécurité régulières et surveillez en permanence les anomalies ou les activités suspectes.
- Utiliser la surveillance continue : pour détecter les incidents de sécurité et y répondre rapidement et efficacement, mettez en œuvre une surveillance continue. Utilisez des outils d'analytique de sécurité avancés pour surveiller le comportement des utilisateurs, le trafic réseau et les activités du système. Automatisez les alertes et les notifications pour garantir une réponse rapide aux incidents.
- Promouvoir une culture de sécurité et de conformité : encouragez une culture de sécurité et de conformité à travers l'organisation. Sensibilisez les employés aux bonnes pratiques en matière de sécurité, à l'importance de respecter les principes de confiance zéro et au rôle des employés dans le maintien d'un environnement cloud sécurisé. Organisez régulièrement des formations de sensibilisation à la sécurité pour vous assurer que les employés sont vigilants face à l'ingénierie sociale et qu'ils comprennent leurs responsabilités en matière de protection des données et de confidentialité.
- Utiliser des simulations d'ingénierie sociale : réalisez des simulations d'ingénierie sociale pour évaluer la vulnérabilité des utilisateurs aux attaques de ce type. Utilisez les résultats des simulations pour adapter les programmes de formation afin d'améliorer la sensibilisation des utilisateurs et leur réponse aux menaces potentielles.
- Promouvoir la formation continue : instaurez une culture de formation et d'apprentissage continus en fournissant une formation et des ressources continues en matière de sécurité. Tenez les utilisateurs informés de l'évolution des bonnes pratiques en matière de sécurité. Encouragez les utilisateurs à rester vigilants et à signaler rapidement toute activité suspecte.
- Évaluer et optimiser en permanence : évaluez régulièrement l'environnement cloud pour détecter les domaines à améliorer. Utilisez des outils natifs cloud pour surveiller l'utilisation des ressources et les performances, et effectuez des évaluations des vulnérabilités et des tests de pénétration en vue d'identifier et de corriger les éventuelles faiblesses.
- Établir un cadre de gouvernance et de conformité : développez un cadre de gouvernance et de conformité pour garantir que votre organisation est conforme aux normes du secteur et aux exigences réglementaires. Dans le cadre, définissez des politiques, des procédures et des

contrôles pour protéger les données et les systèmes contre tout accès, utilisation, divulgation, interruption, modification ou destruction non autorisés. Mettez en œuvre des mécanismes de suivi et de création de rapports sur les métriques de conformité, en réalisant des audits réguliers et en traitant rapidement tout problème de non-conformité.

- Encourager la collaboration et le partage des connaissances : encouragez la collaboration et le partage des connaissances entre les équipes qui prennent par à l'adoption de la ZTA. Vous pouvez le faire en favorisant la communication interfonctionnelle et la collaboration entre les unités informatiques, de sécurité et commerciales. Votre organisation peut également mettre en place des forums, des ateliers et des sessions de partage des connaissances pour promouvoir la compréhension, relever les défis et partager les enseignements tirés tout au long du processus d'adoption.

Principaux points à retenir

Ce guide a exploré les aspects essentiels du développement d'une stratégie d'architecture confiance zéro (ZTA) réussie. Cette section résume les principaux points à retenir des recommandations présentées :

- Comprendre les principes de confiance zéro : la confiance zéro est un modèle conceptuel et un ensemble de mécanismes associés qui visent à fournir des contrôles de sécurité autour des ressources numériques qui ne dépendent pas uniquement ou fondamentalement des contrôles réseau traditionnels ou de l'environnement du réseau. Au lieu de cela, les contrôles réseau sont complétés par l'identité, l'appareil, le comportement et d'autres contextes et signaux riches afin de prendre des décisions d'accès plus précises, intelligentes, adaptatives et continues. Familiarisez-vous avec les principes fondamentaux de la confiance zéro, tels que le moindre privilège, la microsegmentation, l'authentification continue et l'autorisation adaptative.
- Définir des objectifs clairs : définissez clairement les objectifs et les résultats métier souhaités de l'adoption de la ZTA. Alignez ces objectifs sur les principes de la confiance zéro pour contribuer à garantir une base de sécurité solide tout en favorisant la croissance de l'activité et l'innovation.
- Réaliser des évaluations complètes : effectuez une évaluation approfondie de votre infrastructure informatique, de vos applications et de vos ressources de données existantes. Identifiez les dépendances, les dettes techniques et les problèmes de compatibilité pour orienter votre stratégie d'adoption.
- Élaborer un plan d'adoption de la ZTA : créez un plan détaillé qui décrit l'approche étape par étape pour déplacer les charges de travail, les applications et les données vers le cloud. Tenez compte de facteurs tels que les exigences de conformité et la modernisation des applications.
- Mettre en œuvre une ZTA robuste : concevez et implémentez une ZTA qui applique des contrôles d'accès précis, des mécanismes d'authentification forts et une surveillance continue. Pour une adoption plus efficace de la ZTA, utilisez des services confiance zéro natifs cloud, comme Accès vérifié par AWS et Amazon VPC Lattice.
- Prioriser la sécurité des données et des applications : appliquez les principes de confiance zéro (identité forte, microsegmentation et autorisation) pour fournir tout le contexte disponible. Utilisez ce contexte pour les utilisateurs qui accèdent aux systèmes et aux ressources, ainsi que pour le flux de communications et de données au sein des composants du serveur principal et entre eux.
- Établir des cadres de surveillance et de réponse aux incidents : mettez en œuvre de solides fonctionnalités de surveillance de la sécurité et de réponse aux incidents dans l'environnement cloud. Utilisez des outils de sécurité natifs cloud pour la détection des menaces en temps réel,

l'analyse des journaux et l'automatisation de la réponse aux incidents, tels qu'Amazon Inspector, AWS Security Hub et Amazon GuardDuty.

- Promouvoir une culture de sécurité et de conformité : encouragez une culture de sensibilisation à la sécurité et de conformité à travers l'organisation. Sensibilisez les employés aux bonnes pratiques en matière de sécurité et à leur rôle dans le maintien d'un environnement cloud sécurisé.
- Évaluer et optimiser en permanence : évaluez régulièrement l'environnement cloud, les contrôles de sécurité et les processus opérationnels. Pour recueillir des informations et optimiser l'utilisation des ressources, la gestion des coûts et les performances, utilisez des outils d'analytique et de surveillance natifs cloud tels qu'Amazon CloudWatch et AWS Security Hub.
- Établir des cadres de gouvernance et de conformité : développez des cadres de gouvernance et de conformité conformes aux normes du secteur et aux exigences réglementaires. Définissez des politiques, des procédures et des contrôles visant à garantir le respect des normes de sécurité, de confidentialité et de conformité.

Étapes suivantes

L'adoption d'une architecture confiance zéro (ZTA) est l'un des moyens les plus sûrs d'améliorer la posture de votre organisation et de réduire les risques. Ces recommandations vous ont fourni une feuille de route complète pour l'implémentation de la confiance zéro, en commençant par la compréhension des principes jusqu'à l'évaluation de votre niveau de préparation, en passant par l'implémentation des composants requis.

Les prochaines étapes de ce flux de travail ou de ce domaine sont les suivantes :

- Implémentation du plan d'adoption
- Implémentation de la ZTA
- Réalisation régulière d'évaluations de sécurité
- Optimisation continue de l'environnement cloud et des contrôles de sécurité

La ZTA est un processus continu qui nécessite une surveillance, une évaluation et une adaptation constantes afin de garantir une base de sécurité solide. En suivant les bonnes pratiques décrites dans ces conseils, votre organisation peut améliorer son niveau de sécurité, garantir le respect des réglementations et protéger les données sensibles.

FAQ

Cette section fournit des réponses aux questions fréquemment posées concernant la conception et l'implémentation d'une architecture confiance zéro (ZTA).

Qu'est-ce que la confiance zéro ?

La confiance zéro est un modèle conceptuel et un ensemble de mécanismes associés qui visent à fournir des contrôles de sécurité autour des ressources numériques qui ne dépendent pas uniquement ou fondamentalement des contrôles réseau traditionnels ou de l'environnement du réseau. Au lieu de cela, les contrôles réseau sont complétés par l'identité, l'appareil, le comportement et d'autres contextes et signaux riches afin de prendre des décisions d'accès plus précises, intelligentes, adaptatives et continues.

Quels sont les Services AWS qui peuvent m'aider à implémenter une architecture confiance zéro ?

AWS propose plusieurs services qui peuvent aider à mettre en œuvre la confiance zéro, tels que Accès vérifié par AWS, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway et Amazon GuardDuty.

Comment puis-je garantir la sécurité des données avec AWS ?

AWS propose des services tels que AWS Key Management Service (AWS KMS) pour le chiffrement des données au repos et en transit, Amazon Virtual Private Cloud (Amazon VPC) pour l'isolation du réseau, et AWS Secrets Manager pour le stockage et la récupération sécurisés des informations d'identification.

Est-ce qu'AWS peut contribuer à répondre aux exigences de conformité dans un environnement de confiance zéro ?

Oui, AWS dispose de services et de programmes de conformité pour répondre aux diverses exigences réglementaires. AWS Artifact donne accès aux rapports de conformité AWS et AWS Config prend en charge le suivi et l'évaluation continus de la conformité.

Existe-t-il des outils ou des services AWS permettant d’automatiser la sécurité dans un environnement de confiance zéro ?

AWS fournit des services tels que AWS Security Hub qui centralisent et automatisent les résultats de sécurité, ainsi que des règles AWS Config pour définir et appliquer les politiques de sécurité.

Comment puis-je garantir une surveillance continue et une réponse aux incidents dans un environnement cloud de confiance zéro avec AWS ?

AWS propose des services tels qu’Amazon CloudWatch pour la surveillance en temps réel, ainsi que AWS CloudTrail pour la journalisation et l’analyse. Pour les bonnes pratiques en matière de réponse aux incidents, vous pouvez utiliser le Guide de réponse aux incidents de sécurité AWS.

Ressources

Références

- What is a cloud center of excellence and why should your organization create one? – Ce billet de blog donne un aperçu du CCoE, des bonnes pratiques pour créer un CCoE efficace, et bien plus encore.
- Zero Trust on AWS : cette page fournit un aperçu des principes de sécurité de confiance zéro et des bonnes pratiques dans l'environnement AWS.
- Zero Trust architecture: An AWS perspective : ce billet de blog partage une définition et des principes directeurs de la manière dont la confiance zéro est implémenté chez AWS.
- Guide de l'utilisateur AWS Identity and Access Management (IAM) : ce guide propose une documentation complète sur la gestion de l'accès et des autorisations des utilisateurs dans IAM, un élément essentiel de l'architecture confiance zéro.
- AWS Security Hub : découvrez Security Hub, un service qui offre une vue complète des alertes de sécurité et de l'état de conformité sur vos Comptes AWS.
- Cadre AWS Well-Architected : découvrez le cadre Well-Architected, qui fournit des conseils sur la création d'architectures sécurisées, hautement performantes, résilientes et efficaces sur AWS.
- AWS Security Incident Response Guide : ce guide présente un aperçu des principes fondamentaux de la réponse aux incidents de sécurité au sein de l'environnement AWS Cloud de votre organisation. Il fournit une vue d'ensemble des concepts de sécurité du cloud et de réponse aux incidents, et il identifie les fonctionnalités, les services et les mécanismes du cloud mis à la disposition des clients qui répondent à des problèmes de sécurité.

Outils

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty

- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- Accès vérifié par AWS

Historique du document

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

Modification	Description	Date
Mises à jour ajoutées	Des informations ont été ajoutées à la section Composants clés d'une architecture confiance zéro, des modifications ont été apportées à la section Évaluation de l'état de préparation organisationnelle pour l'adoption de la confiance zéro, des informations ont été ajoutées à la section Bonnes pratiques et des modifications ont été apportées à la FAQ.	4 décembre 2023
Publication initiale	—	19 juin 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 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 (RDSAmazon) 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 un Microsoft Hyper-V application à 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.

ACID

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

SQLFonction 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, consistance, isolation, 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 basé sur les 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 AWS 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 CAForganise les directives 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, 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, consultez le AWS CAFsite Web et le AWS CAFlivre blanc.

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 WQFest 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 API appels 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.

CCoE

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

modifier la capture de données (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 l'utiliser à diverses CDC 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 CCoEarticles 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 uneCCoE, établir un modèle d'exploitation)
- 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

Consultez la base de données de gestion des configurations.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub or Bitbucket 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, AWS Panorama propose des appareils qui ajoutent des CV aux réseaux de caméras locaux, et Amazon SageMaker 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 de configuration (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 issues de la phase CMDB de découverte et d'analyse du portefeuille lors 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 YAML modèle. 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 source, de génération, de test, intermédiaire 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. DVSMétend 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 la façon dont vous pouvez utiliser le design piloté par domaine avec le motif Strangler Fig, voir Modernisation de l'ancienne version de Microsoft. ASP NET(ASMX) des services Web de manière incrémentielle à l'aide de conteneurs et d'Amazon API Gateway.

DR

Consultez la section 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 dans 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 VPC terminaison d'interface. Pour plus d'informations, consultez la section Créer un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (AmazonVPC).

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section Chiffrement des enveloppes dans la documentation AWS Key Management Service (AWS KMS).

environment

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

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

environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

époppée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les grands enjeux en matière de AWS CAF 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. EDAest 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. Ceci est généralement exprimé sous la forme d'un score numérique qui peut être calculé à l'aide de diverses techniques, telles que les explications additives de Shapley (SHAP) et les dégradés 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 un LLMpetit 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 étapes 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. FMssont 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. Ils sont mis en œuvre à l'aide de politiques de contrôle des services et de limites IAM d'autorisations. 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 IAM principaux qui définit leurs autorisations au sein de l' AWS Cloud environnement.

application inactive

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

IIoT

Voir Internet industriel des objets.

infrastructure immuable

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

entrant (entrée) VPC

Dans une architecture AWS multi-comptes, une architecture 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 Élaborer une stratégie de transformation numérique industrielle pour l'Internet des objets (IIoT).

inspection VPC

Dans une architecture AWS multi-comptes, système centralisé VPC qui gère les inspections du trafic réseau entre VPCs (identiques ou différents Régions AWS), 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. ITILconstitue la base deITSM.

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 ITSM outils, consultez 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. An 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, consultez la section Appliquer les autorisations du moindre privilège dans la IAM documentation.

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.

MES

Voir le système d'exécution de la fabrication.

Transport de télémétrie 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.

Migration Acceleration Program (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. MAPinclut une méthodologie de migration pour exécuter les migrations existantes de manière méthodique et un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

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

usine de migration

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

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le 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 MPAfournit une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, TCO comparaisons, analyse des coûts de migration) ainsi que la planification de la migration (analyse et collecte des données des applications, regroupement des applications, hiérarchisation des migrations et planification des vagues). L'MPAoutil (nécessite une connexion) est disponible gratuitement pour tous les AWS consultants et consultants APN partenaires.

Évaluation de l'état de préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une entreprise 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. MRAest la première phase de la stratégie de AWS migration.

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

Consultez la section 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-États-Unis

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. OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

accord au niveau opérationnel () OLA

Un accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de soutenir un accord de niveau de service (). SLA

examen de l'état de préparation opérationnelle (ORR)

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

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. OCMaide les organisations à se préparer et à passer à de nouveaux systèmes et stratégies en accélérant l'adoption des changements, en résolvant les problèmes de transition et en suscitant 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, consultez le OCMguide.

contrôle d'accès à l'origine (OAC)

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

identité d'accès à l'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisezOAI, 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 granulaire et amélioré.

ORR

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

DE

Voir technologie opérationnelle.

sortant (sortie) VPC

Dans une architecture AWS multi-comptes, 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

Une politique de IAM gestion attachée IAM aux principaux pour définir les autorisations maximales que l'utilisateur ou le rôle peut avoir. Pour plus d'informations, consultez la section Limites des autorisations dans la IAM documentation.

informations personnellement 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. PIILes exemples incluent les noms, les adresses et les coordonnées.

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, un IAM rôle ou un utilisateur. Pour plus d'informations, consultez les termes et concepts de Principal in Roles dans la IAM documentation.

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 DNS requêtes relatives à un domaine et à 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 LLMinvite 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 environnement basé sur des microservices MES, 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 SQL relationnelle.

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

RACImatrice

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

RAG

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.

RASCImatrice

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 du 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, responsable, consultée, informée (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 RASCImatrice, et si vous l'excluez, elle est appelée RACImatrice.

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'intelligence artificielle générative dans laquelle un système LLMfait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données d'entraînement avant de générer une réponse. Par exemple, un RAG modèle peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, reportez-vous à la section Qu'est-ce que c'est 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)

L'utilisation d'SQLexpressions simples et flexibles qui ont défini des règles d'accès. RCACconsiste en des autorisations de ligne et des masques de colonnes.

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de 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

SAML2,0

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 AWS API opérations sans que vous ayez à créer un compte utilisateur IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML basée sur la version 2.0, consultez la section À propos de la fédération SAML basée sur la version 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 combinent des systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un SIEM système 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 et 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 VPC de sécurité, 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 propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPsdéfinissez 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

Le URL point d'entrée d'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.

accord 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 un exemple de la façon d'appliquer ce modèle, voir Modernisation de l'ancienne version de MicrosoftASP.NET(ASMX) des services Web de manière incrémentielle à l'aide de conteneurs et d'Amazon API Gateway.

sous-réseau

Une série d'adresses IP dans votreVPC. 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 LLMhomme pour 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.

VPCpeering

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des adresses IP privées. Pour plus d'informations, consultez What is VPC peering dans la VPC documentation Amazon.

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

SQLFonction 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.

WORM

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 de type « 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 LLMdes instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. LLMIl doit utiliser ses connaissances pré-entraînées pour effectuer 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 de CPU 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.