Architecture de cloud computing sécurisée (SCCA) activée AWS pour le ministère américain de la Défense

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Architecture de cloud computing sécurisée (SCCA) activée AWS pour le ministère américain de la Défense

Table of Contents

Architecture de cloud computing sécurisée (SCCA) activée AWS pour le ministère américain de la Défense

Rob Higareda et Rughved Gadgil, Amazon Web Services ()AWS

Mars 2024 (historique du document)

Le département américain de la défense (DoD) segmente les informations du cloud en niveaux d'impact (IL). Le niveau d'impact est associé à la sensibilité des informations et au risque de perte de confidentialité, d'intégrité ou de disponibilité de ces informations. L'IL4 prend en charge les informations non classifiées contrôlées (CUI) contrôlées par le DoD, et l'IL5 prend en charge les informations CUI du DoD et les informations des systèmes de sécurité nationale (NSS). Ce guide est conçu pour vous aider à créer une zone d'atterrissage compatible avec les informations IL4 et IL5.

Pour créer une infrastructure cloud conforme aux normes IL4 ou IL5, vous devez créer des composants spécifiques. L'architecture de cloud computing sécurisée (SCCA) de la Defense Information Systems Agency (DISA) est une sélection de services de sécurité et de gestion du cloud. Il fournit une approche standardisée pour créer une limite de cloud. Le SCCA inclut également des composants de sécurité au niveau des applications pour les informations IL4 et IL5 hébergées dans le cloud.

Ce guide vous aide à répondre aux exigences du SCCA en utilisant l'accélérateur de zone d'atterrissage (LZA) activé. AWS La solution LZA déploie un ensemble de fonctionnalités de base conçues pour s'aligner sur les AWS meilleures pratiques et les multiples cadres de conformité mondiaux. Le LZA peut vous aider à créer de nombreux composants nécessaires pour adhérer au SCCA du DoD. Ce guide recommande également comment ajouter des composants supplémentaires pour garantir la conformité à la norme SCCA et établir une base sécurisée pour vos environnements cloud. AWS Bien que ce guide n'inclue pas toutes les situations potentielles, il fournit des conseils sur la façon de démarrer et sur ce qui Services AWS peut vous aider à répondre aux exigences de la SCCA.

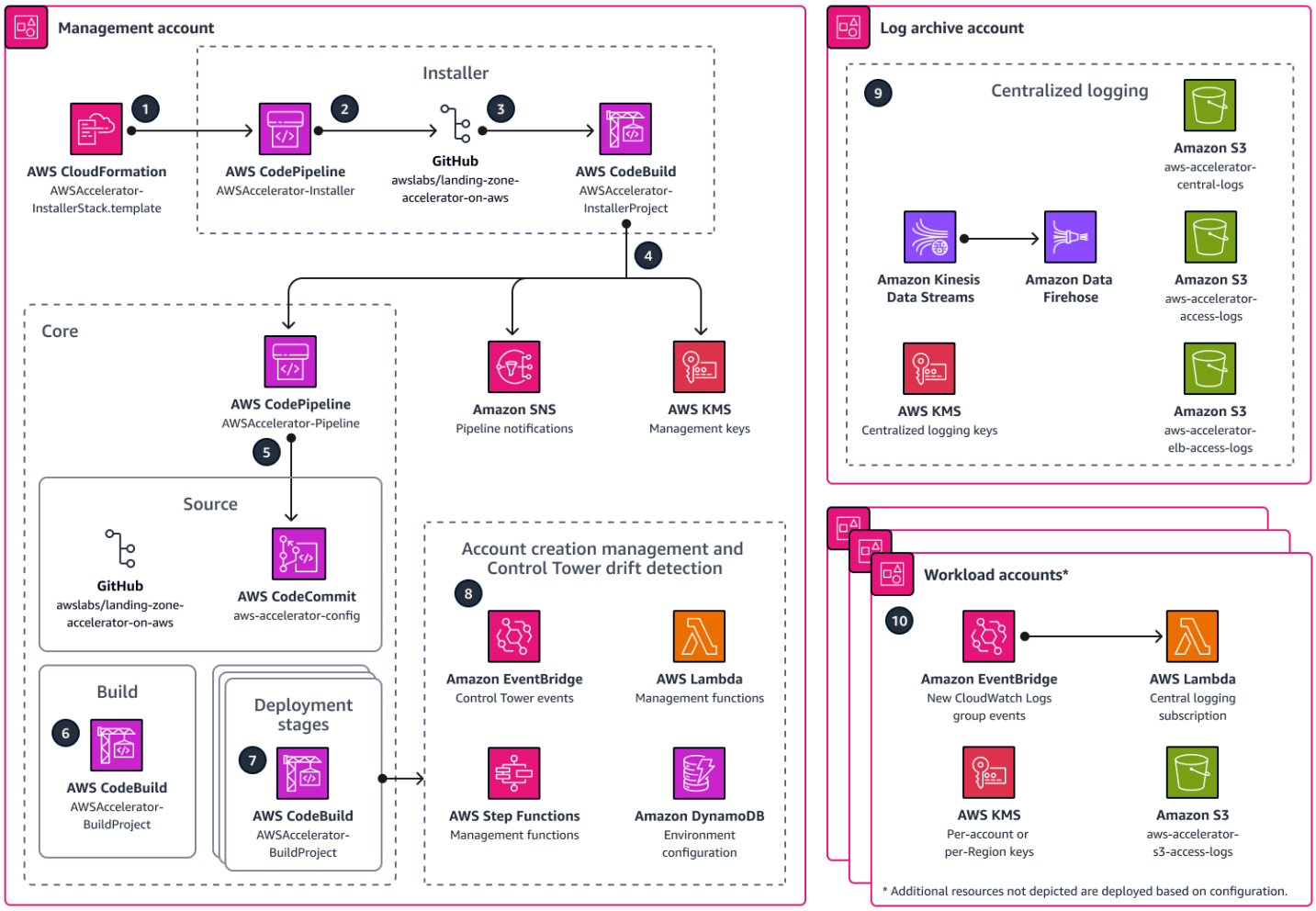
Public visé

Ce guide est destiné aux personnes qui doivent se conformer à l'architecture de cloud computing sécurisée du DoD afin de sécuriser les informations IL4 et IL5 dans le. AWS Cloud Si ce n'est pas déjà fait, consultez le guide des exigences de sécurité du cloud computing DISA avant de lire ce guide.

Présentation de l'accélérateur de zone d'atterrissage

Afin de créer une zone d'atterrissage conforme à l'architecture de cloud computing sécurisée (SCCA) de la Defense Information Systems Agency (DISA), vous devez disposer de certains éléments pour vous aider à répondre aux exigences minimales. AWS AWS a créé l'accélérateur de zone d'atterrissage (LZA) pour vous aider à déployer une zone d'atterrissage conforme aux exigences requises. À l'aide de la solution LZA, vous pouvez déployer l'environnement à l'aide d'un ensemble de fichiers de configuration. Ces fichiers de configuration vous aident à vous concentrer sur la fourniture d'un environnement au lieu d'apprendre à chaque individu Service AWS comment le déployer.

L'image suivante montre les services impliqués dans le déploiement du LZA. Les chiffres indiquent le flux de travail, de la modification des fichiers de configuration Services AWS à la configuration des comptes de charge de travail.



Cette solution est conçue pour s'aligner sur les AWS meilleures pratiques et se conformer à de multiples cadres de conformité mondiaux. Lorsqu'elle est utilisée en coordination avec des services tels que AWS Control Tower, cette solution fournit une solution complète à faible code couvrant plus de 35 Services AWS fonctionnalités. Plus précisément, cette solution vous aide à gérer et à gouverner un environnement multi-comptes conçu pour prendre en charge des charges de travail hautement réglementées et des exigences de conformité complexes. LZA vous aide à établir l'état de préparation de votre plateforme grâce à des fonctionnalités de sécurité, de conformité et opérationnelles. Ce guide inclut des notes spécifiques concernant l'utilisation de cette solution afin de faciliter l'alignement sur les directives du gouvernement fédéral et du ministère de la Défense (DoD) des États-Unis.

AWS fournit la solution LZA sous la forme d'un projet open source créé à l'aide du AWS Cloud Development Kit (AWS CDK). Vous pouvez l'installer directement dans votre environnement, ce qui vous donne un accès complet à la solution d'infrastructure en tant que code (IaC).

Grâce à un ensemble simplifié de fichiers de configuration, vous pouvez :

- Configurez des fonctionnalités, des garde-corps et des services de sécurité supplémentaires, tels que des règles AWS Configgérées et. AWS Security Hub
- Gérez votre topologie réseau de base via des services tels qu'Amazon Virtual Private Cloud (Amazon VPC), et. AWS Transit GatewayAWS Network Firewall
- Générez des comptes de charge de travail supplémentaires à l'aide de AWS Control Tower Account Factory.

Aucun frais supplémentaire ou engagement initial n'est requis pour utiliser Landing Zone Accelerator sur AWS. Vous ne payez que pour Services AWS ce que vous activez pour configurer votre plateforme et faire fonctionner vos garde-corps. Cette solution peut également prendre en charge AWS des partitions non standard AWS GovCloud (US), notamment les régions AWS Secret et AWS Top Secret.

> **Important**
>
> La solution LZA ne garantit pas à elle seule la conformité. Il fournit l'infrastructure de base à partir de laquelle vous pouvez intégrer des solutions complémentaires supplémentaires. Les informations contenues dans le guide de mise en œuvre de la LZA ne sont pas exhaustives. Vous devez examiner, évaluer, évaluer et approuver la solution conformément aux fonctionnalités, outils et configurations de sécurité propres à votre entreprise. Il

est de votre entière responsabilité et de celle de votre organisation de déterminer les exigences réglementaires applicables et de vous assurer que vous vous conformez à toutes les exigences. Bien que cette solution aborde à la fois les exigences techniques et administratives, elle ne vous aide pas à vous conformer aux exigences administratives non techniques.

Planification de votre déploiement LZA sur AWS

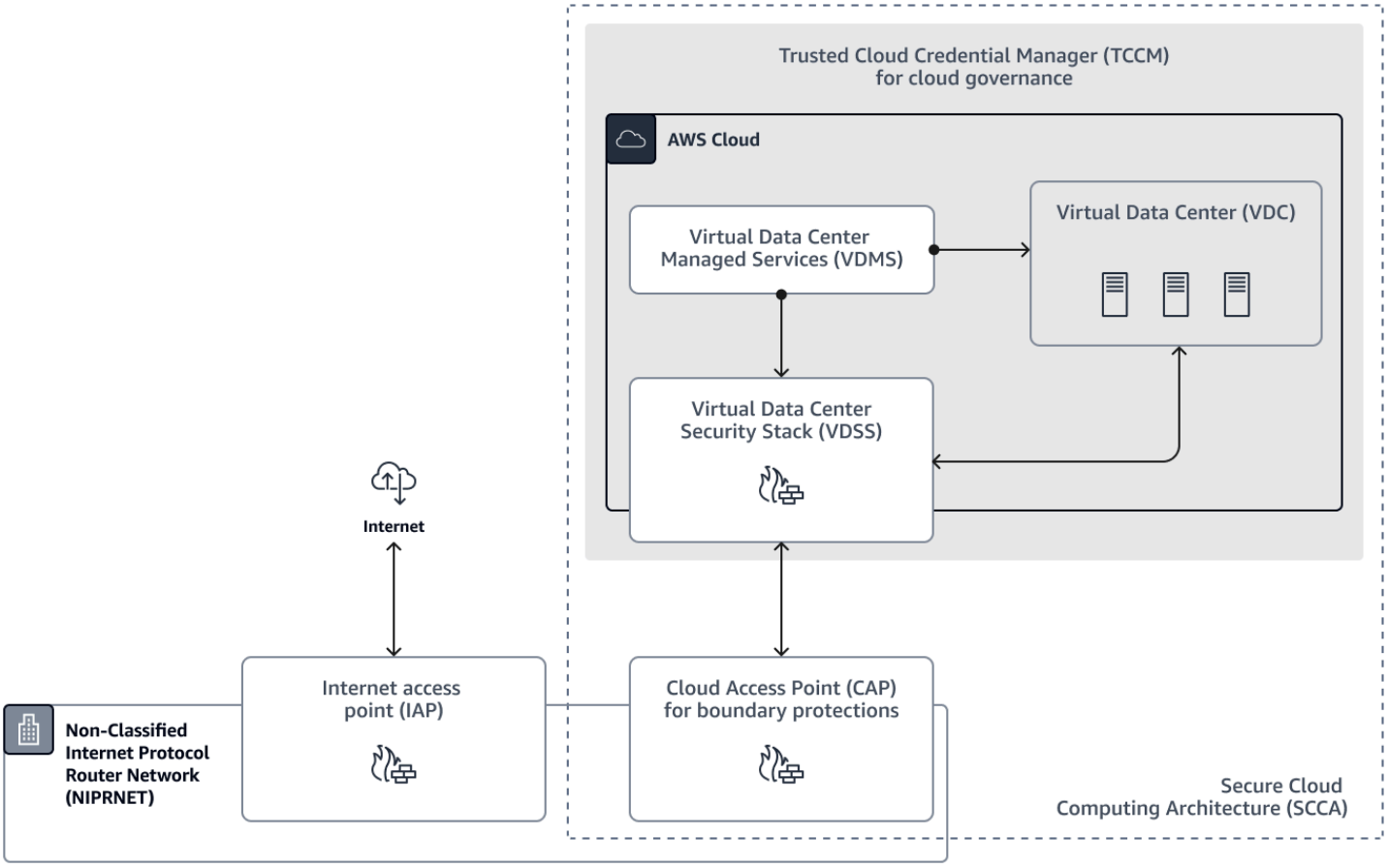
AWS a créé un guide de mise en œuvre détaillé pour déployer la solution Landing Zone Accelerator (LZA) sur AWS. Pour un schéma d'architecture et une vue d'ensemble des étapes de déploiement, voir le schéma d'architecture dans le guide d' AWS implémentation de l'accélérateur de zone d'atterrissage. Votre environnement doit répondre aux prérequis avant de déployer la solution. À l'aide des exigences décrites dans le chapitre sur les composants et les exigences du SCCA de ce guide, vous pouvez choisir entre les options de déploiement décrites dans le guide de mise en œuvre de la LZA.

Composants et exigences du SCCA

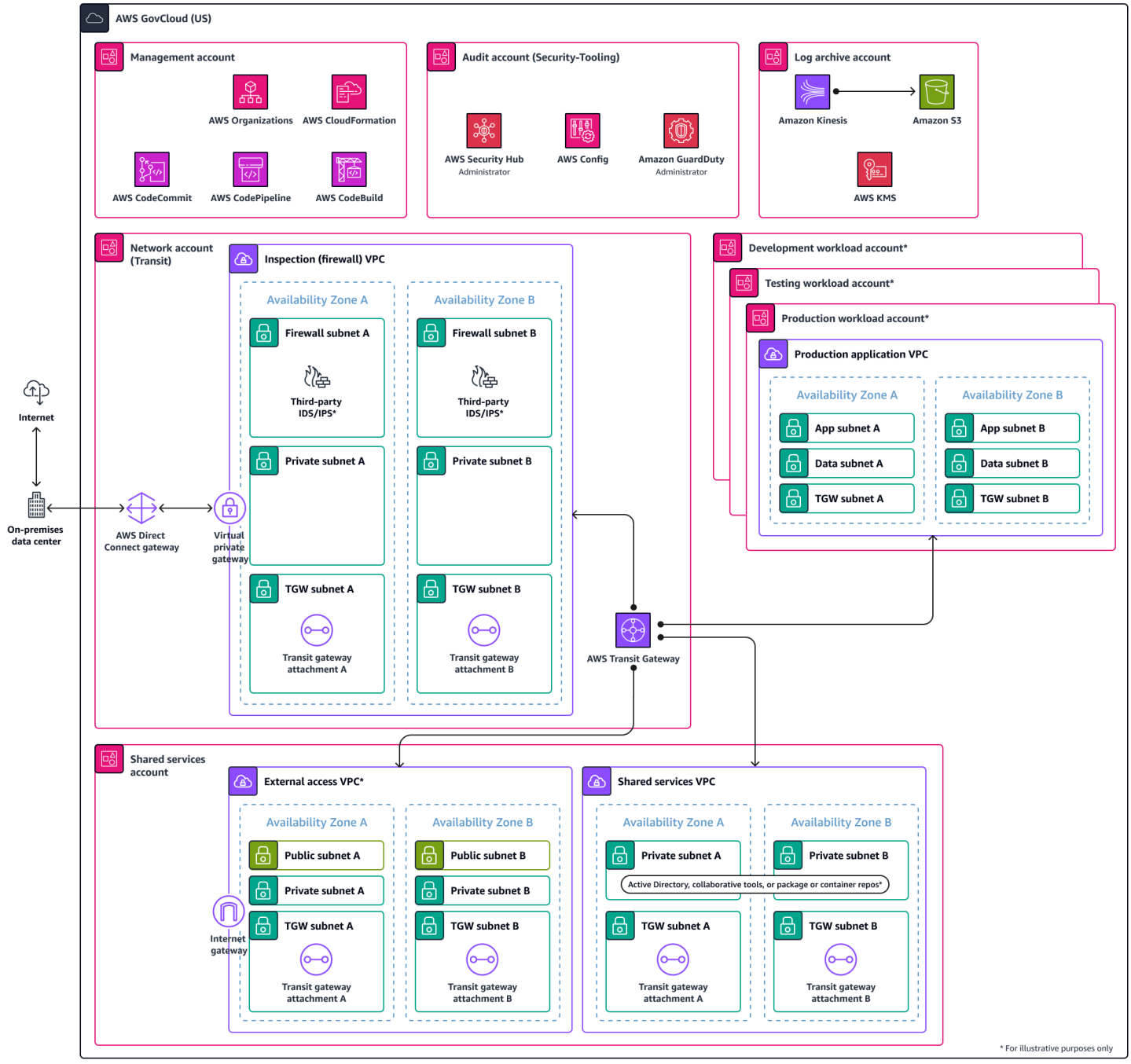
L'architecture de cloud computing sécurisée (SCCA) de la Defense Information Systems Agency (DISA), adoptée par le ministère américain de la Défense (DoD), se veut une approche évolutive et rentable pour sécuriser les applications basées sur le cloud dans le cadre d'une architecture de sécurité commune. Il fournit une approche standard pour sécuriser les données IL4 et IL5 dans les environnements cloud. Comme décrit dans la fiche d'information de la DISA SCCA, les principaux éléments de la SCCA sont les suivants :

- Point d'accès au cloud (CAP) : fournit un accès au cloud et protège les réseaux du DoD depuis le cloud. Protections rationalisées axées sur la protection des limites du réseau.
- Virtual Data Center Security Stack (VDSS) : sécurité de l'enclave du réseau virtuel pour protéger les applications et les données dans les offres cloud commerciales.
- Virtual Data Center Managed Services (VDMS) : sécurité de l'hôte des applications pour un accès privilégié des utilisateurs dans les environnements commerciaux.
- Trusted Cloud Credential Manager (TCCM) : gestionnaire d'identifiants cloud pour appliquer le contrôle d'accès basé sur les rôles (RBAC) et les accès les moins privilégiés.

L'image suivante montre ces composants du SCCA.



Cette section décrit en détail chaque composant et les composants correspondants du LZA qui peuvent vous aider à respecter la norme DISA (Defense Information Systems Agency). L'image suivante montre la structure multi-comptes LZA qui construit les composants du SCCA dans le. AWS Cloud Cette structure multi-comptes LZA est une base qui vous aide à obtenir une architecture entièrement conforme aux exigences de la DISA SCCA. Pour un exemple d'architecture qui vous aide à répondre pleinement aux exigences de conformité, consultez le SCCA sur le schéma AWS GovCloud d'architecture.



Point d'accès au cloud

Le point d'accès au cloud Boundary (BCAP) ou le point d'accès au cloud (CAP) est prédéterminé par votre organisation. Cela n'entre donc pas dans le champ d'application de ce guide. Le CAP permet d'accéder aux environnements cloud commerciaux à partir du Defense Information Systems Network (DISN). Le CAP fournit également une protection des limites du DISN depuis le cloud. À la limite du DISN, il inclut des capacités de cyberdéfense, telles que le pare-feu, les systèmes de détection

d'intrusion (IDS) et les systèmes de prévention des intrusions (IPS). Il est courant que les entreprises utilisent le modèle de référence de point d'accès natif du cloud du DoD pour y accéder. AWS

Stack de sécurité pour centres de données virtuels

L'objectif du Virtual Data Center Security Stack (VDSS) est de protéger les applications propriétaires de missions du DOD qui sont hébergées dans. AWS Le VDSS fournit une enclave pour les services de sécurité. Le VDSS effectue la majeure partie des opérations de sécurité dans le SCCA. Ce composant contient des services de sécurité et de réseau, tels que les contrôles d'accès à la connectivité entrante et les services de protection périmétrique, notamment les pare-feux d'applications Web, la protection DDOS, les équilibreurs de charge et les ressources de routage réseau. Le VDSS peut résider dans l'infrastructure cloud ou sur site, dans votre centre de données. AWS ou des fournisseurs tiers peuvent fournir des fonctionnalités VDSS via une infrastructure en tant que service (IaaS), ou AWS peuvent proposer ces fonctionnalités via des solutions logicielles en tant que service (SaaS). Pour plus d'informations sur le VDSS, consultez le guide des exigences de sécurité du DoD pour le cloud computing.

Le tableau suivant contient les exigences minimales pour le VDSS. Il explique si le LZA répond à chaque exigence et lequel Services AWS vous pouvez utiliser pour répondre à ces exigences.

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.2.1	Le VDSS doit maintenir une séparation virtuelle de tout le trafic de gestion, d'utilisateurs et de données.	AWS Network Firewall Liste de contrôle d'accès réseau (ACL) Groupes de sécurité pour interfaces réseau élastiques	Isolez les VPC	Couvert
2.1.2.2	Le VDSS doit autoriser l'utilisation du chiffreme	Amazon VPC (Chiffrer le	Bonnes pratiques de	Couvert

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
	nt pour la segmentation du trafic de gestion.	trafic entre les instances)	chiffrement pour Amazon VPC	
2.1.2.3	Le VDSS doit fournir une capacité de proxy inverse pour traiter les demandes d'accès provenant des systèmes clients.	N/A	Diffusion de contenu à l'aide d'un proxy inverse entièrement géré	Non couvert
2.1.2.4	Le VDSS doit fournir la capacité d'inspecter et de filtrer les conversations au niveau de l'application sur la base d'un ensemble de règles prédéfinies (y compris HTTP) afin d'identifier et de bloquer les contenus malveillants.	AWS WAF Network Firewall	Inspection du corps de la demande Web Inspection du trafic TLS avec Network Firewall	Partiellement couvert

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.2.5	Le VDSS doit fournir une capacité capable de distinguer et de bloquer le trafic non autorisé de la couche application.	AWS WAF	Comment utiliser Amazon GuardDuty et AWS WAF bloquer automatiquement les hôtes suspects	Non couvert
2.1.2.6	Le VDSS doit fournir une capacité permettant de surveiller les activités du réseau et du système afin de détecter et de signaler les activités malveillantes concernant le trafic entrant et sortant des réseaux/enclaves privés virtuels du propriétaire de la mission.	Journaux de flux VPC Amazon GuardDuty AWS Enclaves Nitro	AWS Atelier Nitro Enclaves	Partiellement couvert

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.2.7	Le VDSS doit fournir une capacité qui surveille les activités du réseau et du système afin d'arrêter ou de bloquer les activités malveillantes détectées.	Network Firewall AWS WAF	N/A	Partiellement couvert
2.1.2.8	Le VDSS inspectera et filtrera le trafic transitant entre les réseaux/enclaves privés virtuels du propriétaire de la mission.	Network Firewall	Déployez un filtrage centralisé du trafic	Couvert

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.2.9	Le VDSS doit interrompre et inspecter le trafic de communication SSL/TLS en prenant en charge l'authentification simple et double pour le trafic destiné aux systèmes hébergés au sein du CSE.	Network Firewall	Modèles de déploiement pour Network Firewall	Couvert
2.1.2.10	Le VDSS doit fournir une interface pour mener les activités de gestion des ports, des protocoles et des services (PPSM) afin de fournir un contrôle aux opérateurs MCD.	Network Firewall	Modèles de déploiement pour Network Firewall	Couvert

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.2.11	Le VDSS doit fournir une capacité de surveillance qui capture les fichiers journaux et les données d'événements à des fins d'analyse de cybersécurité.	Amazon CloudWatch AWS CloudTrail	Journalisation pour la réponse aux incidents de sécurité	Couvert
2.1.2.12	Le VDSS doit fournir ou transmettre des informations de sécurité et des données d'événements à un système d'archivage attribué pour la collecte, le stockage et l'accès communs aux journaux d'événements par les utilisateurs privilégiés effectuant des activités Boundary et Mission CND.	Amazon CloudWatch Logs	Sécurité dans les CloudWatch journaux	Couvert

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.2.13	Le VDSS fournira un système de gestion des clés de chiffrement conforme à la norme FIPS-140-2 pour le stockage des informations d'identification des clés de chiffrement privées du serveur générées et attribuées par le DoD pour l'accès et l'utilisation par le Web Application Firewall (WAF) lors de l'exécution de la rupture SSL/TLS et de l'inspection des sessions de communication cryptées.	AWS Secrets Manager AWS Key Management Service(AWS KMS)	Améliorez la sécurité des CloudFront origines d'Amazon grâce AWS WAF à Secrets Manager AWS KMS gestion des clés avec FIPS 140-2	Non couvert

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.2.14	Le VDSS doit fournir la capacité de détecter et d'identifier le détournement de session d'application.	N/A	N/A	Non couvert
2.1.2.15	Le VDSS fournira une extension DMZ du DoD à prendre en charge les applications Internet (IFA).	N/A	N/A	Non couvert
2.1.2.16	Le VDSS doit fournir une capture complète des paquets (FPC) ou une capacité FPC équivalente au service cloud pour l'enregistrement et l'interprétation des communications transitoires.	Network Firewall Journaux de flux VPC	N/A	Couvert

ID	Exigence de sécurité VDSS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.2.17	Le VDSS fournira des mesures et des statistiques du flux de paquets réseau pour toutes les communications transitoires.	CloudWatch	Surveillez le débit réseau des points de terminaison VPC d'interface à l'aide de CloudWatch	Couvert
2.1.2.18	Le VDSS prévoit l'inspection du trafic entrant et sortant du réseau privé virtuel de chaque propriétaire de mission.	Network Firewall	Déployez un filtrage centralisé du trafic	Couvert

Certaines composantes du CAP que vous définissez ne sont pas abordées dans ce guide car chaque agence possède son propre lien avec le CAP AWS. Vous pouvez compléter les composants du VDSS avec le LZA afin de faciliter l'inspection du trafic entrant. AWS Les services utilisés dans le LZA fournissent une analyse des limites et du trafic interne afin de sécuriser votre environnement. Afin de continuer à construire un VDSS, certains composants d'infrastructure supplémentaires ne sont pas inclus dans le LZA.

En utilisant le cloud privé virtuel (VPC), vous pouvez définir des limites dans chacun d'entre eux Compte AWS afin de respecter les normes SCCA. Cela n'est pas configuré dans le cadre du LZA car les VPC, l'adressage IP et le routage sont des composants que vous devez configurer en fonction des besoins de votre infrastructure. Vous pouvez implémenter des composants tels que les extensions de sécurité du système de noms de domaine (DNSSEC) dans Amazon Route 53. Vous pouvez également ajouter des WAF commerciaux AWS WAF ou tiers pour vous aider à atteindre les normes nécessaires.

En outre, pour répondre à l'exigence 2.1.2.7 du DISA SCCA, vous pouvez utiliser un Network GuardDutyFirewall pour sécuriser et surveiller l'environnement afin de détecter tout trafic malveillant.

Virtual Data Center Managed Services

L'objectif des Virtual Data Center Managed Services (VDMS) est de fournir des services de sécurité des hôtes et de centres de données partagés. Les fonctions du VDMS peuvent soit s'exécuter dans le hub de votre SCCA, soit le responsable de la mission peut en déployer certaines parties lui-même. Comptes AWS Ce composant peut être fourni dans votre AWS environnement. Pour plus d'informations sur le VDMS, consultez le guide des exigences de sécurité du DoD pour le cloud computing.

Le tableau suivant contient les exigences minimales pour le VDMS. Il explique si le LZA répond à chaque exigence et lequel Services AWS vous pouvez utiliser pour répondre à ces exigences.

ID	Exigence de sécurité VDMS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.3.1	Le VDMS doit fournir une solution d'évaluation de la conformité assurée (ACAS), ou un équivalent approuvé, pour effectuer une surveillance continue de toutes les enclaves du CSE.	AWS Config AWS Security Hub AWS Audit Manager Amazon Inspector	Analyse des vulnérabilités avec Amazon Inspector	Partiellement couvert
2.1.3.2	Le VDMS doit fournir un système de sécurité basé sur	N/A	N/A	Non couvert

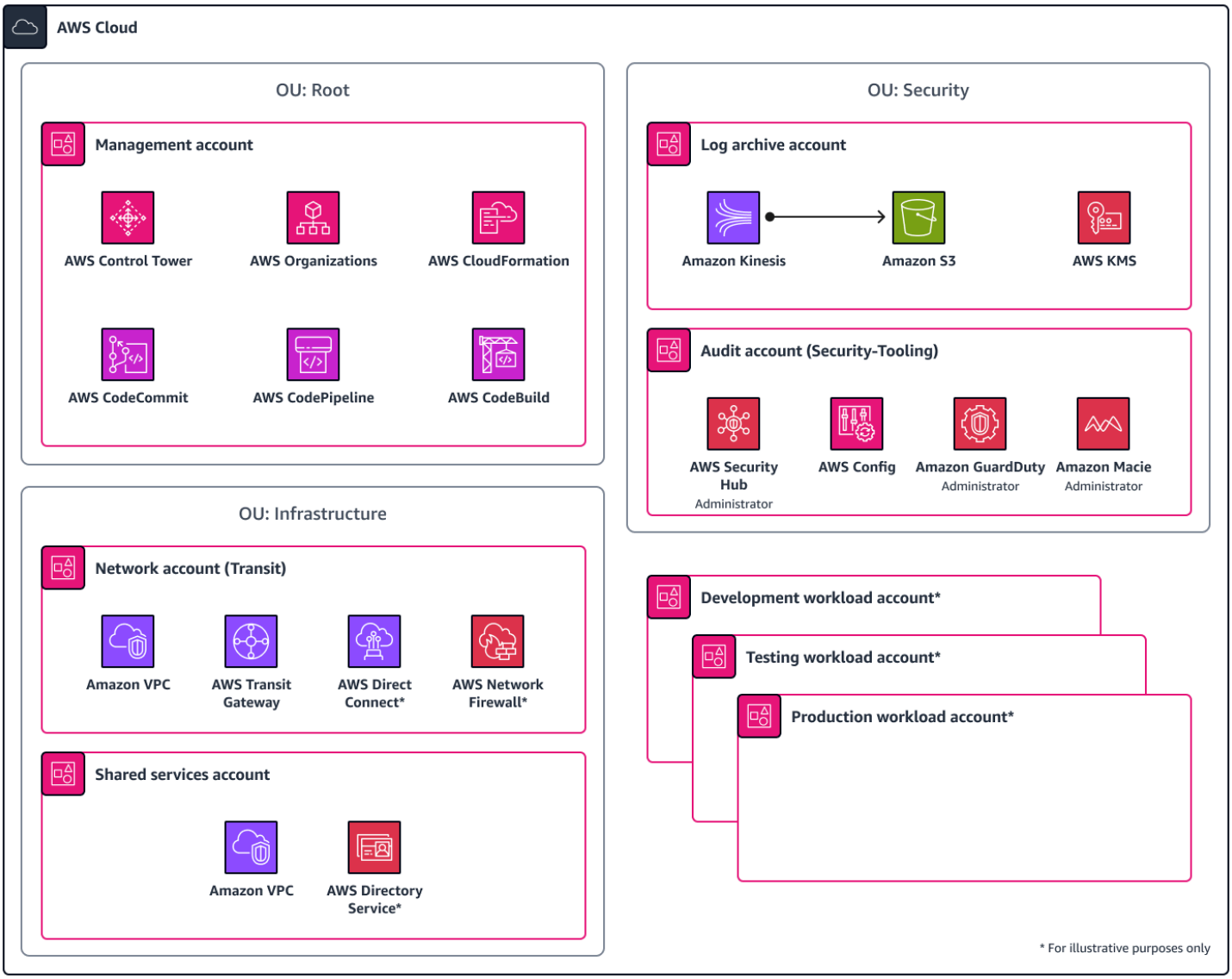
ID	Exigence de sécurité VDMS	AWS technologies	Ressources supplémentaires	Couvert par LZA
	l'hôte (HBSS), ou un équivalent approuvé, pour gérer la sécurité des terminaux de toutes les enclaves du CSE.			
2.1.3.3	Le VDMS fournira des services d'identité, notamment un répondeur du protocole d'état des certificats en ligne (oCloud Workload Security) pour l'authentification à deux facteurs par carte d'accès commun (CAC) du DoD à distance des utilisateurs privilégiés du DoD auprès des systèmes instanciés au sein du CSE.	Authentification multifactorielle (MFA) disponible via : AWS Identity and Access Management (IAM) AWS IAM Identity Center AWS Directory Service for Microsoft Active Directory AWS Private Certificate Authority	Configurer une carte CAC pour Amazon WorkSpaces	Partiellement couvert

ID	Exigence de sécurité VDMS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.3.4	Le VDMS doit fournir un système de gestion de configuration et de mise à jour pour servir les systèmes et les applications de toutes les enclaves du CSE.	AWS Systems Manager Gestionnaire de correctifs AWS Config	Automatiser la gestion des correctifs avec AWS Systems Manager (YouTube vidéo)	Partiellement couvert
2.1.3.5	Le VDMS doit fournir des services de domaine logiques comprenant l'accès aux annuaires, la fédération d'annuaires, le protocole DHCP (Dynamic Host Configuration Protocol) et le système de noms de domaine (DNS) pour toutes les enclaves du CSE.	AWS Managed Microsoft AD Amazon Virtual Private Cloud (Amazon VPC) Amazon Route 53	Configuration des attributs DNS pour votre VPC	Partiellement couvert

ID	Exigence de sécurité VDMS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.3.6	Le VDMS doit fournir un réseau de gestion des systèmes et des applications au sein du CSE qui est logiquement séparé des réseaux d'utilisateurs et de données.	Amazon VPC Sous-réseaux Amazon VPC	N/A	Couvert
2.1.3.7	Le VDMS doit fournir un système de journalisation et d'archivage des événements liés au système, à la sécurité, aux applications et aux activités des utilisateurs pour la collecte, le stockage et l'accès communs aux journaux d'événements par les utilisateurs privilégiés effectuant des activités BCP et MCP.	AWS Security Hub AWS CloudTrail Amazon CloudWatch Logs Amazon Simple Storage Service (Amazon S3)	Journalisation centralisée avec OpenSearch	Couvert

ID	Exigence de sécurité VDMS	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.3.8	Le VDMS doit permettre l'échange d'attributs d'authentification et d'autorisation des utilisateurs privilégiés du DoD avec le système de gestion des identités et des accès du CSP afin de permettre le provisionnement, le déploiement et la configuration du système cloud.	AWS Managed Microsoft AD	Améliorez votre configuration AWS Managed Microsoft AD de sécurité	Non couvert
2.1.3.9	Le VDMS doit mettre en œuvre les capacités techniques nécessaires pour exécuter la mission et les objectifs du rôle de TCCM.	AWS Managed Microsoft AD IAM IAM Identity Center	N/A	Partiellement couvert

Comme le montre l'image suivante, le LZA pose les composants de base pour répondre aux exigences de base du VDMS. Vous devez configurer certains composants supplémentaires après le déploiement du LZA pour vous aider à respecter les normes VDMS. Dans le tableau précédent, assurez-vous de consulter les liens de la colonne Ressources supplémentaires. Ces liens vous aident soit à configurer ces éléments supplémentaires, soit à apporter des améliorations supplémentaires en matière de sécurité.



Intégration de services supplémentaires

La colonne Ressources supplémentaires du tableau précédent répertorie les ressources qui vous aideront à développer le LZA afin de répondre aux exigences du VDMS. AWS propose également des supports d'atelier pour vous aider à configurer une architecture cloud sécurisée.

Sans modification, le LZA répond aux exigences IL4/IL5, mais vous pouvez déployer des services supplémentaires pour améliorer la sécurité de votre environnement. AWS

Par exemple, Amazon Inspector est un service de gestion des vulnérabilités qui analyse en permanence vos AWS charges de travail pour détecter les vulnérabilités logicielles et les risques d'exposition involontaire au réseau. Vous pouvez l'utiliser pour identifier et étudier les vulnérabilités des systèmes d'exploitation hôtes, tels que Windows et Linux. Même si Amazon Inspector n'intègre pas toutes les exigences nécessaires pour un système de sécurité basé sur l'hôte (HBSS), il fournit au moins une évaluation de base des vulnérabilités des instances.

Application de correctifs au système d'exploitation

L'application de correctifs au système d'exploitation est un élément essentiel du fonctionnement d'un environnement sécurisé. AWS propose et recommande d'utiliser le gestionnaire de correctifs, une fonctionnalité permettant de AWS Systems Manager maintenir des bases de correctifs cohérentes et d'automatiser le déploiement des correctifs. Patch Manager automatise le processus d'application des correctifs aux nœuds gérés à la fois avec des mises à jour liées à la sécurité et d'autres types de mises à jour.

Vous pouvez utiliser le Gestionnaire de correctifs pour appliquer des correctifs pour les systèmes d'exploitation et les applications. (Sur Windows Server, le support des applications est limité aux mises à jour des applications publiées par Microsoft.) Pour plus d'informations, consultez la section Orchestration de processus de correctifs personnalisés en plusieurs étapes à l'aide du gestionnaire de AWS Systems Manager correctifs sur le blog sur les opérations et les migrations AWS dans le cloud.

Pour step-by-step obtenir des instructions sur l'utilisation du gestionnaire de correctifs, consultez l'atelier sur les outils de AWS gestion et de gouvernance.

Pour plus d'informations sur la sécurisation des charges de travail Microsoft Windows sur AWS, consultez l'atelier sur la sécurisation des charges de travail Windows sur AWS.

Gestionnaire d'informations d'identification cloud fiable

Le Trusted Cloud Credential Manager (TCCM) est un composant du SCCA. Il est responsable de la gestion des accréditations. Lors de la mise en place du TCCM, il est important d'autoriser l'accès au SCCA avec le moindre privilège. Cela peut être réalisé en utilisant des services de gestion des AWS identités et des accès. Un composant supplémentaire du TCCM est une connexion aux Virtual Data

Center Managed Services (VDMS). Vous pouvez utiliser cette connexion selon vos besoins pour accéder au TCCM AWS Management Console afin de gérer le TCCM.

Le TCCM est une combinaison de technologies et de normes qui régissent l'accès à AWS. Le TCCM est considéré comme essentiel pour la plupart des implémentations car il contrôle les autorisations d'accès. La fonction TCCM n'est pas destinée à imposer des exigences uniques en matière de gestion des identités au fournisseur de services cloud (CSP) commercial. Le TCCM n'interdit pas non plus l'utilisation de la fédération CSP du DoD ou de solutions de courtage d'identité tierces pour fournir le contrôle d'identité prévu.

Les composants de la politique TCCM sont basés sur une compréhension générale du fait que les CSP proposent un système de gestion des identités et des accès qui permet de contrôler l'accès aux systèmes cloud. Ces systèmes peuvent inclure la console d'accès, l'API et les composants de service de l'interface de ligne de commande (CLI) du CSP. Au niveau de base, le TCCM doit verrouiller les informations d'identification qui peuvent être utilisées pour créer des réseaux et d'autres ressources non autorisés. Le TCCM est nommé par le responsable autorisé (AO) chargé de superviser les systèmes informatiques. Les politiques du TCCM établissent la nécessité d'un modèle d'accès avec le moindre privilège. Ces politiques sont responsables de la fourniture et du contrôle des informations d'identification des utilisateurs privilégiés dans le cloud commercial. Ceci afin de rester en conformité avec le guide des exigences de sécurité du DoD en matière de cloud computing, qui traite de la mise en œuvre de politiques, de plans et de procédures pour gérer les informations d'identification de votre compte de portail. Avant la connexion au Defense Information Systems Network (DISN), DISA valide l'existence du Cloud Credential Management Plan (CCMP) dans le cadre du processus d'approbation de connexion défini dans le Guide du processus de connexion.

Le tableau suivant contient les exigences minimales pour le TCCM. Il explique si le LZA répond à chaque exigence et lequel Services AWS vous pouvez utiliser pour répondre à ces exigences.

ID	Exigences de sécurité du TCCM	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.4.1	Le TCCM élaborera et tiendra à jour un plan de gestion des informations d'identification	N/A	N/A	Non couvert

ID	Exigences de sécurité du TCCM	AWS technologies	Ressources supplémentaires	Couvert par LZA
	dans le cloud (CCMP) pour aborder la mise en œuvre des politiques, des plans et des procédures qui seront appliqués à la gestion des informations d'identification des comptes du portail client du propriétaire de la mission.			
2.1.4.2	Le TCCM collectera, auditera et archivera tous les journaux d'activité et alertes du portail client.	AWS CloudTrail Amazon CloudWatch Logs	N/A	Couvert

ID	Exigences de sécurité du TCCM	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.4.3	Le TCCM doit s'assurer que les alertes du journal d'activité sont partagées avec, transmises ou récupérables par les utilisateurs privilégiés du DoD engagés dans des activités MCP et BCP.	AWS CloudTrail CloudWatch Journaux Amazon Simple Notification Service (Amazon SNS) CloudWatch Informations sur les journaux	N/A	Couvert
2.1.4.4	Le TCCM doit, si nécessaire pour le partage d'informations, créer des comptes d'accès au référentiel de journaux pour l'accès aux données du journal d'activité par les utilisateurs privilégiés effectuant à la fois des activités MCP et BCP.	AWS CloudTrail CloudWatch Journaux Amazon SNS CloudWatch Informations sur les journaux	N/A	Couvert

ID	Exigences de sécurité du TCCM	AWS technologies	Ressources supplémentaires	Couvert par LZA
2.1.4.5	Le TCCM doit récupérer et contrôler de manière sécurisée les informations d'identification du compte du portail client avant la connectivité de l'application de mission au DISN.	AWS IAM Identity Center	N/A	Couvert
2.1.4.6	Le TCCM créera, délivrera et révoquera, si nécessaire, les informations d'identification du portail client le moins privilégié basées sur les rôles aux administrateurs des applications et du système du propriétaire de la mission (c'est-à-dire les utilisateurs privilégiés du DoD).	AWS Identity and Access Management (IAM) AWS Directory Service for Microsoft Active Directory	N/A	Couvert

Afin de permettre au TCCM de répondre aux exigences, le LZA utilise le contrôle programmatique des ressources via le service IAM. Vous pouvez également associer IAM à IAM AWS Managed Microsoft AD pour implémenter l'authentification unique dans un autre annuaire. Cela lie votre AWS environnement à votre infrastructure sur site avec des approbations Active Directory. Dans le LZA, l'implémentation est déployée avec des rôles IAM pour un accès temporaire basé sur les sessions. Les rôles IAM sont des informations d'identification de courte durée qui aident votre organisation à répondre aux exigences TCCM nécessaires.

Bien que la LZA mette en œuvre l'accès à moindre privilège et un accès programmatique à court terme aux AWS ressources, passez en revue les meilleures pratiques en matière d'IAM pour vous assurer que vous suivez les directives de sécurité recommandées.

Pour plus d'informations sur la mise en œuvre AWS Managed Microsoft AD, consultez la AWS Managed Microsoft ADsection de l'atelier Active Directory on AWS Immersion Day.

Le modèle de responsabilitéAWS partagée s'applique au TCCM et au LZA. La LZA définit les aspects fondamentaux du contrôle d'accès, mais chaque organisation est responsable de la configuration de ses contrôles de sécurité.

Conclusion

Pour le ministère américain de la Défense (DoD), ce guide explique quelles sont les exigences de la Defense Information Systems Agency (DISA) pour déployer une architecture de cloud computing sécurisée (SCCA). En utilisant l'accélérateur de zone d'atterrissage (LZA) activé AWS, vous pouvez mettre en œuvre AWS des offres et éliminer le fait de soulever des objets lourds et indifférenciés. Cela vous permet de vous concentrer sur votre mission qui consiste à créer une infrastructure cloud conforme aux normes IL4 ou IL5.

Ressources

AWS documentation

- AWS Services concernés par programme de conformité (AWS conformité)
- Guide des exigences de sécurité en matière de cloud computing du ministère de la Défense (AWS conformité)
- Accélérateur de zone d'atterrissage activé AWS (bibliothèque de AWS solutions)
- Guide de mise en AWS œuvre de l'accélérateur de zone d'atterrissage
- SCCA sur le schéma AWS GovCloud d'architecture

Autres ressources

- Guide des exigences de sécurité du cloud computing (site Web de la DISA)
- Conception de référence du point d'accès cloud natif (CNAP) du ministère de la Défense (DoD) (site Web du DoD)
- Fiche d'information sur l'architecture sécurisée du cloud computing du DoD (site Web de la DISA)

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
Publication initiale	—	12 mars 2024

AWS Glossaire des recommandations

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

Nombres

7 R

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

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers Amazon Aurora Édition compatible avec PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (RDSAmazon) for 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 sur site vers Oracle sur une EC2 instance dans le AWS Cloud.
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : Migrer une Microsoft Hyper-V application 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 Utilisation du contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACID

Voir atomicité, cohérence, isolement, 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 que la migration active-passif.

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-modèle

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité () ACID

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

contrôle d'accès 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

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

l'organisation à une adoption réussie du cloud. Pour plus d'informations, consultez le AWS CAFsite Web et le AWS CAFlivre blanc.

AWS Workload Qualification Framework (AWS WQF)

Outil qui évalue les charges de travail de migration de base de données, recommande des politiques de migration et fournit des estimations de travail. AWS 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

robot malveillant

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'indexation 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.

réseau d'ordinateurs zombies

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 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 Centre d'excellence cloud.

CDC

Consultez la section Capture des données de modification.

capture de données modifiées (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

Voir Intégration continue et livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence cloud (CCoE)

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

cloud computing

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

modèle d'exploitation cloud

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

étapes d'adoption du cloud

Les quatre phases que les organisations traversent généralement lorsqu'elles migrent vers 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 mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant unCCoE, en établissant un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

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

CMDB

Consultez la base de données de gestion des configurations.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (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 des configurations (CMDB)

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

pack de conformité

Une collection de AWS Config règles et d'actions correctives que vous pouvez mettre en place pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans un Compte AWS et une région, ou au sein d'une organisation, à l'aide d'un YAML modèle. Pour plus d'informations, consultez Conformance packs 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 est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

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 Cadre AWS Well-Architected. Pour plus d'informations, veuillez consulter Classification des données.

dérive des données

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

données en transit

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

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 de 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 sur AWS, vous ajoutez plusieurs contrôles à différentes couches de

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

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte 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, veuillez consulter Reprise après sinistre des charges de travail sur AWS : restauration dans le cloud dans le cadre AWS Well-Architected Framework.

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

informatique de périphérie

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou 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, veuillez consulter Creating an endpoint service 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, veuillez consulter la rubrique Envelope encryption dans la documentation AWS Key Management Service (AWS KMS).

environment

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

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

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les épopées en matière de AWS CAF sécurité comprennent la gestion des identités et des accès, les contrôles de détection, la sécurité de l'infrastructure, la

protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le guide d'implémentation du programme.

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 d'informations

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 AWS Bordures d'isolation des défauts.

branche de fonctionnalités

Voir la succursale.

fonctionnalités

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

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, veuillez consulter Machine learning model interpretability with :AWS.

transformation de fonctionnalité

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

FGAC

Voir le contrôle d'accès affiné.

contrôle précis des accès () 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 via la capture des données de modification afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

G

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Dans Amazon CloudFront, option permettant d'empêcher les utilisateurs de pays spécifiques 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, veuillez consulter

la rubrique Restriction de 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 l'approche héritée, tandis que le flux de travail basé sur les liaisons est l'approche moderne préférée.

stratégie inédite

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

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités d'organisation (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des IAM 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 de l'historien

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

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

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

correctif

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

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 Cadre AWS Well-Architected.

entrant (d'entrée) VPC

Dans une architecture à AWS comptes multiples, 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 entrées, les sorties et l'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un

premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

Un 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, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

inspection VPC

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

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir Internet des objets.

bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. 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, veuillez consulter le guide d'intégration des opérations.

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur les étiquettes () LBAC

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

zone de destination

Une zone de destination est un AWS environnement à comptes multiples Well-Architected évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement

de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

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 la 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. Les logiciels malveillants comprennent notamment 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 lorsqu'il fonctionne. Pour plus d'informations, veuillez consulter Building mechanisms in the AWS Well-Architected Framework.

compte membre

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

MES

Voir le système d'exécution de la fabrication.

Transport de télémétrie par 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

Petit service indépendant qui communique via des informations bien définies 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, veuillez consulter Integrating microservices by using AWS serverless services.

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie à l'aide de la légèreté. 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 de plus amples informations, veuillez consulter Implémentation de microservices sur AWS.

Migration Acceleration Program (MAP)

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

migration à grande échelle

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

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de l'usine de migration comprennent généralement des responsables des opérations, des analystes métier et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des professionnels travaillant dans des 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 : réhéberger la migration vers Amazon EC2 avec AWS Application Migration Service.

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

Approche utilisée pour migrer une charge de travail vers AWS Cloud. Pour plus d'informations, veuillez consulter l'entrée dans ce glossaire et Mobilize your organization to accelerate large-scale migrations.

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, veuillez consulter Strategy for modernizing 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, veuillez consulter Evaluating modernizing readiness for applications in the AWS Cloud.

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Transport de télémétrie par file d'attente de messages.

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 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

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

examen de l'état de préparation opérationnelle (ORR)

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

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

Journal de suivi créé par AWS CloudTrail qui journalise tous les événements pour tous les Comptes AWS dans une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, veuillez consulter la rubrique Creating a trail for an organization 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 effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant l'adoption des

changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre s'appelle accélération des personnes, 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 d'origine (OAC)

Dans CloudFront, option améliorée qui permet de restreindre l'accès à 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 d'origine (OAI)

Dans CloudFront, option qui permet de restreindre l'accès à votre contenu Amazon S3. Lorsque vous utilisezOAI, CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés peuvent accéder au contenu dans un compartiment S3 uniquement via une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

ORR

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

DE

Voir technologie opérationnelle.

sortant (de sortie) VPC

Dans une architecture à AWS comptes multiples, 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 entrées, les sorties et l'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

P

limite des autorisations

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

données d'identification personnelle (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 qui permet de définir des autorisations (voir Politique basée sur l'identité), de spécifier les conditions d'accès (voir Politique de contrôle de service), ou de définir les autorisations maximales pour tous les comptes d'une organisation dans AWS Organizations (voir Politique de contrôle de service).

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.

poussée de predicate

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela permet de réduire la quantité de données devant être extraites et traitées à partir de la base de données relationnelle, et d'améliorer les performances des requêtes.

contrôle préventif

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

principal

Une entité d' AWS qui peut exécuter des actions et accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS, un IAM rôle ou un utilisateur. Pour plus d'informations, consultez les termes et concepts de Principal in Roles dans la IAM documentation.

Protection de la confidentialité dès la conception

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

zones hébergées privées

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

contrôle proactif

Utilisation d'un 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.

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.

publier/souscrire (pub/sub)

Modèle qui permet les 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, redevable, consulté, informé (RACI).

rançongiciel

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

RASCImatrice

Voir responsable, redevable, 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.

réarchitecture

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise et l’interruption du service.

objectif de temps de récupération (RTO)

Délai maximal acceptable entre l'interruption du service et son rétablissement.

refactoriser

Voir 7 Rs.

Région

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

réhébergement

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 AWS Cloud Résilience.

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

rotation

Processus où vous mettez à jour le secret périodiquement pour rendre l'accès au informations d'identification plus difficile pour un pirate informatique.

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

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

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un 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, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs qui vous aident à mettre en œuvre les meilleures pratiques en matière 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 le Service AWS qui les reçoit.

politique de contrôle des services (SCP)

Politique qui propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPsdéfinissez des barrières de protection ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser SCPs comme listes d'autorisation ou de refus, pour indiquer les services ou les actions autorisés ou interdits. Pour plus d'informations, veuillez consulter la rubrique Stratégies de contrôle de service 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.

contrat de niveau de service () SLA

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

indicateur de niveau de service () SLI

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

objectif de niveau de service () SLO

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

modèle de responsabilité partagée

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

SIEM

Voir 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 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, veuillez consulter Phased approach to modernizing applications dans le. AWS Cloud

SPOF

Voir point de défaillance unique.

schéma d'étoiles

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus

petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un entrepôt de données ou à des fins de business intelligence.

modèle de figuier étrangleur

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

sous-réseau

Plage 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.

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

Hub de transit de réseau que vous pouvez utiliser pour relier votre réseau VPCs et vos réseaux sur site. Pour plus d'informations, veuillez consulter la rubrique 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

Octroi d'autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation dans AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des

tâches de gestion à votre place. Pour plus d'informations, 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.

tasks indifférenciés

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

Connexion entre deux VPCs qui vous permet d'acheminer le trafic à l'aide d'adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'VPCappairage ? 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 fenêtrage

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 zéro 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.

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.