Adoption de la norme Matter pour les fabricants d'appareils IoT

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Adoption de la norme Matter pour les fabricants d'appareils IoT

Table of Contents

Adoption de la norme Matter pour les fabricants d'appareils IoT

Tushar Patel, Vijay Ujjain et David Walters, Amazon Web Services ()AWS

Février 2024 (historique du document)

Selon Statista, le nombre de foyers intelligents dans le monde devrait atteindre 780 millions d'ici 2028. Cette croissance rapide a entraîné des défis en termes d'exploitation et de gestion. Du point de vue du consommateur, chaque fournisseur d'appareils dispose d'une méthode différente pour intégrer l'appareil domotique à un réseau domestique via une application spécifique à ce fournisseur d'appareils. Il est donc difficile de gérer un éventail croissant de types d'appareils provenant de différents fournisseurs. De même, du point de vue d'un fabricant d'appareils, la certification de ses produits domotiques auprès de divers écosystèmes augmente le coût et la complexité de ses processus commerciaux. Par exemple, cela peut nécessiter des SKU différents pour le même modèle d'appareil. Maintenir une application d'expérience utilisateur convaincante et fournir des mises à jour périodiques représente une charge supplémentaire, ce qui détourne les ressources de l'accent mis sur le développement et la fourniture d'un meilleur produit. Les consommateurs et les fabricants d'appareils bénéficieraient d'une norme commune d'interopérabilité pour les maisons intelligentes. Cette norme permet aux appareils de plusieurs fournisseurs d'interagir les uns avec les autres de manière fluide, sécurisée et fiable.

La nouvelle norme Matter représente une opportunité intéressante pour les fabricants d'appareils Internet des objets (IoT) dans le domaine de la maison intelligente. Cette norme vise à améliorer la compatibilité et l'interopérabilité entre les appareils de différents fabricants. Matter est un protocole de connectivité domestique intelligent ouvert qui permet la communication entre les appareils IoT, les applications mobiles et les services cloud.

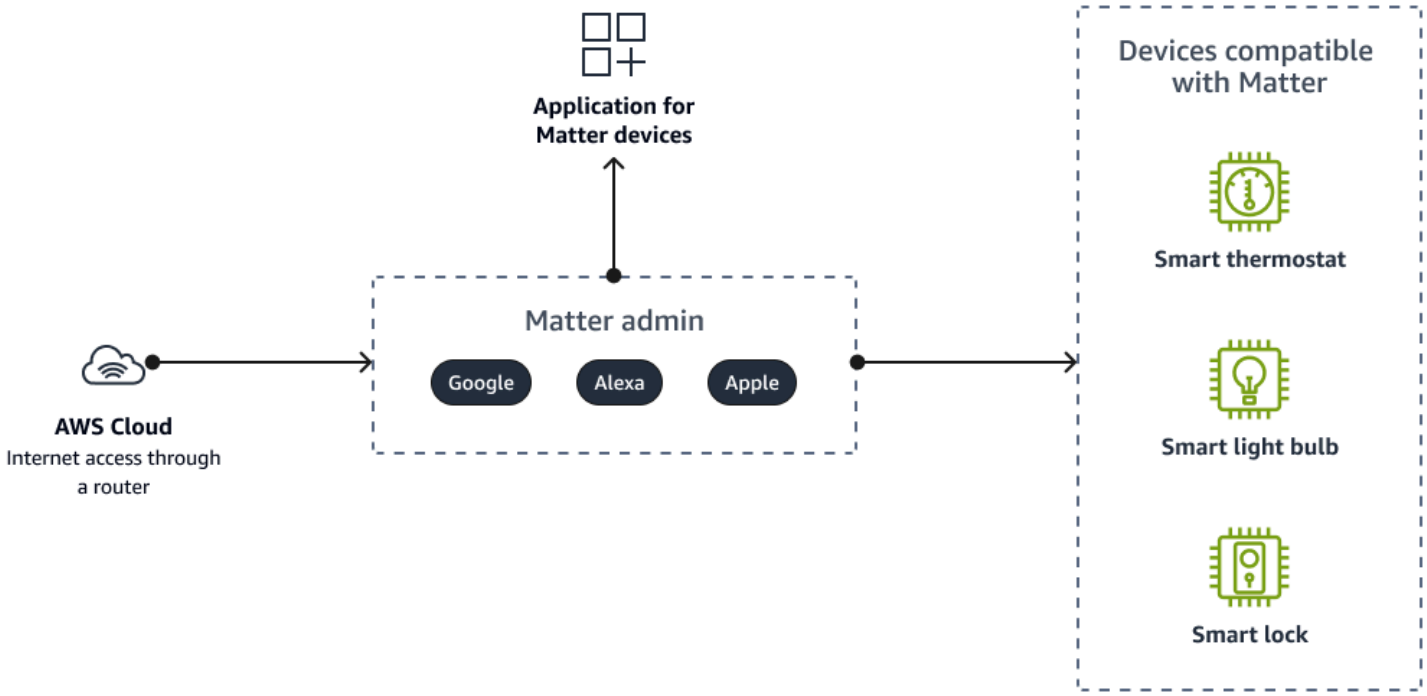
Objectifs

Lors de l'intégration de la norme Matter dans leurs produits, les fabricants d'appareils IoT doivent relever plusieurs défis avant de commencer le développement. Matter offre de nombreux avantages par rapport aux protocoles IoT propriétaires, notamment l'interopérabilité, la sécurité, la simplicité, la fiabilité et la pérennité des appareils. Cependant, l'intégration de Matter dans les déploiements IoT nouveaux et existants nécessite une planification et une stratégie minutieuses. Les fabricants souhaitent obtenir des conseils sur le processus de conformité Matter afin de tirer parti des avantages

tout en évitant les pièges. Ce guide fournit aux fabricants d'appareils IoT des conseils complets sur l'adoption de Matter. Il comprend une feuille de route claire, de la stratégie à la mise en œuvre. Ce guide facilite la transition vers Matter, en vous aidant à créer des produits sécurisés, interopérables et prêts pour l'avenir qui prospèrent dans l'écosystème de la maison intelligente. Avec la bonne approche stratégique, les entreprises peuvent surmonter les obstacles liés à l'adoption de Matter et développer des appareils IoT innovants qui respectent les normes ouvertes.

Ce guide fournit aux fabricants d'appareils un aperçu complet de Matter et des étapes nécessaires pour devenir conforme à Matter. Il décrit les avantages et les inconvénients de la planification d'une stratégie d'adoption de Matter. Le guide suggère également les meilleures pratiques pour tirer parti de Matter tout en continuant à prendre en charge les protocoles sans fil existants, de manière progressive. Pour les fabricants d'appareils IoT qui explorent des solutions domotiques, ce guide peut éclairer votre stratégie de connectivité.

Norme Understanding the Matter



Protocole Matter

Matter est un protocole de connectivité domestique intelligent ouvert qui permet la communication entre les appareils, les applications mobiles et les services cloud. Développé par la Connectivity Standards Alliance (CSA), Matter simplifie la connectivité et l'interopérabilité pour les consommateurs et les fabricants. Matter prend en charge un large éventail de catégories de maisons intelligentes. Pour les consommateurs, Matter assure l'intégration, la gestion unifiée et le contrôle des écosystèmes. Pour les fabricants, Matter réduit les coûts de développement et de support grâce à une certification unique et au développement d'applications. De nombreuses grandes entreprises, telles qu'Amazon, Apple et Google, promeuvent l'adoption de Matter. La CSA propose quatre niveaux d'adhésion en fonction de l'implication de l'organisation : promoteurs, participants, adoptants et associés. Grâce à un solide soutien du secteur, Matter vise à fournir une connectivité fluide entre les marques aux consommateurs et à rationaliser le développement pour les fabricants.

Vue d'ensemble du fonctionnement de Matter

Matter est un protocole IP au niveau des applications pour les appareils domotiques des écosystèmes de fournisseurs. Il fonctionne sur les appareils utilisant le protocole IPv6.

Conceptuellement, Matter est organisé comme un ensemble de nœuds de réseau, qui sont des points de terminaison de Matter. Voici un bref résumé de la terminologie du sujet :

- Les appareils Matter sont des produits domestiques intelligents, tels que des ampoules, des interrupteurs, des thermostats ou des serrures.
- Un Matter Fabric est le réseau virtuel sur lequel tous les appareils sont connectés. Tous les appareils partagent la même racine sécurisée. Le tissu forme une topologie de réseau en étoile.
- Un administrateur Matter crée, maintient et gère la sécurité et les privilèges pour tous les appareils de la structure. Un administrateur peut être un hub ou une application. Matter possède une fonctionnalité multi-administrateurs, grâce à laquelle un appareil Matter peut faire partie de plusieurs structures simultanément. Par exemple, un seul appareil Matter peut être géré à la fois par un appareil Amazon Alexa et un appareil Google Home, qui peuvent tous deux être des administrateurs Matter sur le même réseau physique.
- Un commissaire Matter est un appareil qui met en service (ou intègre) un nouvel appareil Matter dans le tissu. Il peut s'agir d'une application sur un téléphone, d'une passerelle domotique ou d'un administrateur Matter.
- Un pont Matter connecte des appareils utilisant un protocole non IP à une structure Matter.

Pour plus d'informations sur les différents rôles que le matériel et les logiciels peuvent assumer dans Matter, consultez Peeking Under the Hood of Your Matter Smart Home (billet de blog de la CSA).

Avantages de la certification avec Matter

L'introduction de Matter promet d'apporter des avantages significatifs à la fois aux consommateurs de maisons intelligentes et aux fabricants qui les servent. En établissant un langage commun pour les appareils intelligents, Matter vise à démêler le marché fragmenté actuel grâce à une configuration simplifiée, à une gestion unifiée entre les plateformes et à un choix et à une flexibilité accrus en matière de commande vocale.

Pour les consommateurs, cette expérience unifiée devrait rendre la construction et l'extension de leur maison intelligente nettement moins complexes et moins intimidantes. Les fabricants d'appareils obtiennent également des avantages significatifs grâce à la rationalisation de la certification, à la réduction des coûts de développement et à la simplification du support client. Les deux groupes en bénéficient, car Matter améliore l'interopérabilité et réduit les obstacles à l'adoption de la maison intelligente. Dans l'ensemble, la certification selon la norme Matter devrait accélérer la croissance du marché de la maison intelligente en résolvant les problèmes qui l'ont freiné jusqu'à présent.

Rubriques

Avantages de la certification Matter pour les consommateurs de maisons intelligentes

L'introduction de Matter promet d'apporter des avantages significatifs aux consommateurs. Matter fournit un langage commun permettant aux appareils domotiques de fonctionner ensemble de manière fluide sur les principales plateformes. En certifiant les appareils avec Matter, les consommateurs peuvent s'attendre à une configuration et à une gestion simplifiées de leur maison intelligente, ainsi qu'à une flexibilité et à un choix accrus dans la manière dont ils contrôlent leurs appareils.

Configuration simplifiée et gestion unifiée

L'une des plus grandes frustrations des consommateurs est la complexité des processus de configuration et d'intégration nécessaires pour faire fonctionner différents appareils domotiques et les faire fonctionner ensemble. Chaque appareil peut avoir besoin de sa propre application propriétaire

et d'un compte distinct. Pour résoudre ce problème, Matter active les plug-and-play fonctionnalités des appareils certifiés. L'intégration d'appareils certifiés Matter est aussi simple que de connecter l'appareil au réseau domestique local, puis d'utiliser l'administrateur Matter, telle que l'application Alexa, pour lire le code QR sur l'appareil.

Cette expérience de configuration unifiée via une seule application signifie que les consommateurs n'ont plus besoin de jongler entre plusieurs applications distinctes pour gérer différentes marques d'appareils. Ils peuvent visualiser et contrôler l'ensemble de leurs lampes, serrures, capteurs, etc. certifiés MATTER, à partir d'une seule interface. Les utilisateurs d'Apple HomeKit, d'Amazon Alexa et de Google Assistant bénéficient tous de la possibilité de découvrir et de contrôler les appareils Matter sans avoir à télécharger des applications d'un fabricant distinct. La gestion simplifiée des appareils domotiques par le biais d'un système unifié réduit la complexité pour les consommateurs et simplifie considérablement le développement et l'extension de leur configuration.

Choix et flexibilité améliorés en matière de commande vocale

La commande vocale est devenue un moyen populaire pour les consommateurs d'interagir avec leurs appareils domotiques. Cependant, aujourd'hui, le choix de l'assistant vocal dicte souvent les marques d'appareils que vous pouvez contrôler avec votre voix. La matière change cela en permettant le contrôle vocal dans les écosystèmes.

Les consommateurs peuvent désormais choisir l'écosystème d'assistants vocaux le mieux adapté à leurs besoins, sans avoir à se soucier de la compatibilité des appareils. Un utilisateur à l'aise avec l'Assistant Google peut contrôler ses appareils certifiés Matter avec sa voix, même s'ils ont été initialement fabriqués pour Alexa ou HomeKit pour les marchés.

Cette compatibilité croisée des commandes vocales crée un environnement plus ouvert qui offre aux utilisateurs un plus grand choix. Ils peuvent choisir des appareils en fonction de leurs fonctionnalités et de leurs prix plutôt que de leur compatibilité avec un écosystème unique. Si un utilisateur souhaite changer d'assistant vocal à l'avenir, sa configuration domotique existante peut facilement évoluer avec lui, car tous les appareils parlent le langage Matter commun.

Avantages de la certification Matter pour les fabricants d'appareils

En plus d'aider les consommateurs, la certification Matter apporte également des avantages significatifs aux fabricants d'appareils intelligents. En adoptant la norme Matter, les entreprises peuvent obtenir des avantages qui réduisent les coûts et élargissent leur clientèle.

Certification unique pour tous les écosystèmes

Actuellement, pour garantir la compatibilité entre les écosystèmes tels qu'Alexa HomeKit et Google Home, les fabricants doivent passer par plusieurs processus de certification longs et coûteux avec chaque organisation. La matière change cela en établissant une certification commune unique.

Les fabricants d'appareils ne doivent certifier leurs produits qu'une seule fois selon la norme Matter afin qu'ils soient compatibles avec tous les principaux écosystèmes domotiques et assistants vocaux. Cela rationalise le développement et réduit les coûts de certification de manière significative par rapport au statu quo. Il n'est plus nécessaire de consacrer des ressources au maintien de certifications distinctes au fur et à mesure que les produits sont mis à jour. Une certification Single Matter garantit également la pérennité des produits et garantit leur compatibilité même lorsque de nouveaux écosystèmes apparaissent.

Coûts de développement réduits

Matter contribue également à réduire les coûts de développement pour les fabricants. En adoptant une norme de connectivité et de sécurité commune, les entreprises bénéficient de composants d'infrastructure partagés qui contribuent à l'ensemble du projet Matter.

Par exemple, les fabricants n'ont plus besoin d'inclure leurs propres routeurs Thread border propriétaires dans leurs produits, déléguant cette responsabilité aux fabricants de hubs. Les bibliothèques et les pilotes open source partagés réduisent encore les tâches d'ingénierie redondantes. Grâce aux mécanismes communs de découverte des services et de configuration des appareils, il est moins nécessaire de développer des applications sur mesure. Ces réductions des coûts d'infrastructure et de développement d'applications peuvent être répercutées sur les consommateurs sous la forme d'appareils domotiques plus abordables.

Support client simplifié

La fragmentation actuelle du marché de la maison intelligente entraîne de lourdes charges de support client pour les fabricants. Les consommateurs rencontrent fréquemment des problèmes de connectivité, de configuration et de compatibilité qui nécessitent un dépannage. Matter vise à réduire ces problèmes en normalisant les fonctions de base.

Lorsque des problèmes surviennent, les protocoles Matter sous-jacents communs permettent aux entreprises de diagnostiquer et de résoudre plus facilement les problèmes de connectivité sans avoir à prendre en compte plusieurs écosystèmes. Cela rationalise le processus de support. Grâce à une application unique et à une compatibilité vocale commune, les clients apprennent également

plus facilement à utiliser les appareils, ce qui réduit le besoin d'assistance dans de nombreux cas. L'expérience client et le dépannage simplifiés proposés par Matter contribuent à réduire les coûts de support à long terme pour les fabricants.

Considérations relatives à la stratégie de certification Matter

Matter permet l'interopérabilité entre différents appareils et plateformes domotiques. Cependant, la certification avec Matter n'est pas toujours le meilleur choix pour les fabricants d'appareils. Les coûts de mise en œuvre et de certification peuvent ne pas être judicieux du point de vue pratique ou financier, selon le type d'appareil et les cas d'utilisation. Cette section explore certaines des principales raisons pour lesquelles un fabricant peut choisir de ne pas certifier certains appareils avec Matter.

Alors que la norme Matter vise à simplifier le développement et à permettre une compatibilité universelle, certains types d'appareils domotiques peuvent se heurter à des obstacles pratiques en matière de certification qui l'emportent sur les avantages. Pour les produits soumis à des contraintes strictes, à des protocoles non IP, à un public limité ou à des types d'appareils non définis dans Matter, obtenir la certification Matter n'est peut-être pas la meilleure stratégie au départ. Ce sont peut-être les raisons pour lesquelles un fabricant pourrait éviter d'adopter Matter. Cependant, Matter autorise les passerelles compatibles IP à utiliser des proxys pour les points de terminaison non IP. Pour certains appareils existants, une approche passerelle peut être une voie viable vers la compatibilité avec Matter, tout en évitant une refonte complète de l'appareil.

À mesure que la norme Matter évolue et que son champ d'application s'élargit pour couvrir de nouveaux cas d'utilisation, les arguments en faveur de la certification pourraient se renforcer au fil du temps, même pour ces catégories de produits. Les fabricants d'appareils doivent évaluer leurs situations spécifiques et leurs feuilles de route afin de déterminer la meilleure approche en matière de conformité aux normes Matter. Dans de nombreuses situations, de bonnes raisons techniques ou commerciales peuvent justifier le refus de la certification, au moins temporairement.

Protocoles de connectivité non IP

Pour adopter la norme Matter, les appareils doivent fonctionner sur des réseaux IP, tels que le Wi-Fi, l'Ethernet et le Thread. Les protocoles sans fil non IP, tels que Zigbee, Z-Wave et Bluetooth LE, sont couramment utilisés dans les appareils à faible bande passante. Ces protocoles nécessitent un traducteur de protocole supplémentaire non IP vers IP pour être compatibles avec Matter. La mise à niveau du module de communication ou l'introduction d'une passerelle de traduction augmentent généralement le coût matériel de l'appareil.

L'ajout de la prise en charge de la pile IP signifie allouer plus de mémoire et de puissance de traitement à la gestion du réseau. Cela peut dépasser les capacités des appareils à très faible coût

et à faible consommation d'énergie. L'ajout de mémoire ou de flash supplémentaire pour prendre en charge la technologie IP augmenterait également les coûts de fabrication et réduirait l'autonomie de la batterie. Pour les cas d'utilisation où l'alimentation en marche et hors tension ou les données des capteurs sont suffisantes, les protocoles non IP peuvent fournir une solution efficace.

La matière exclut essentiellement la certification de tout appareil qui repose sur des normes sans fil propriétaires non IP. Cela pourrait limiter les fabricants qui souhaitent utiliser des méthodes de connectivité alternatives pour leurs produits bas de gamme. Bien que les protocoles IP tels que le Wi-Fi et l'Ethernet soient nécessaires pour interfacer différents écosystèmes, les normes non IP ont tout de même du mérite pour la connectivité de base des capteurs et des commutateurs dans certaines applications.

Limitations matérielles

Un autre défi est que Matter nécessite un niveau minimum de puissance de traitement et de mémoire sur l'appareil pour prendre en charge la pile logicielle nécessaire. Cependant, les appareils domestiques intelligents les plus basiques ont souvent des capacités de puce intégrées très limitées, en raison de contraintes de coût et de taille.

Par exemple, un simple capteur de porte ou de fenêtre peut contenir uniquement un microcontrôleur avec moins de 100 Ko de mémoire flash et 10 Ko de RAM. Cela ne fournit pas une marge de stockage et de traitement suffisante pour une implémentation complète de Matter. L'ajout de silicium plus puissant et plus coûteux augmenterait considérablement les factures de matériaux.

Dans les cas où le coût et la taille sont les priorités absolues, les fabricants peuvent constater que les exigences de Matter ne correspondent pas à leurs budgets matériels. La certification de capteurs, de commutateurs ou de contrôleurs très basiques avec Matter pourrait entraîner des mises à niveau matérielles inutiles qui auraient une incidence sur le prix.

Écosystèmes clients

Un autre facteur à prendre en compte est de savoir si la clientèle cible d'un fabricant utilise des plateformes domotiques compatibles avec Matter. Si la plupart des consommateurs de ce segment n'utilisent pas de manettes Matter ou de hubs et d'applications compatibles Matter, ils ne seront peut-être pas incités à certifier les produits.

Par exemple, une entreprise qui se concentre sur les besoins des utilisateurs âgés peut constater que ses clients disposent de configurations simples sans administrateurs Matter. Ou encore, les

passionnés de domotique do-it-yourself (DIY) peuvent préférer des solutions personnalisées et ne pas avoir besoin de l' plug-and-play expérience de Matter, quelle que soit la marque.

Dans les scénarios où le groupe démographique cible n'interagit pas avec l'infrastructure Matter, la certification ajoute de la complexité sans avantages évidents. Il serait peut-être préférable de consacrer les ressources à l'optimisation de l'expérience utilisateur sur les plateformes concernées plutôt que de consacrer les efforts à la conformité avec Matter.

Types d'appareils non encore définis

Matter définit actuellement uniquement les profils et les spécifications des appareils pour les catégories courantes de maisons intelligentes, telles que l'éclairage, le CVC, les serrures, les stores et le divertissement. Tous les types de produits de niche situés en dehors de ces zones définies doivent utiliser un profil personnalisé jusqu'à ce que le type d'appareil soit standardisé. Les catégories d'appareils situées en dehors des secteurs verticaux répertoriés, telles que les contrôleurs d'irrigation, les équipements de piscine et les appareils de niche, ne peuvent pas encore utiliser Matter.

Si une entreprise développe des types d'appareils uniques qui ne sont pas couverts par les profils Matter existants, la certification n'est pas possible tant que les nouveaux profils ne sont pas rédigés. Cela pourrait retarder le lancement d'un nouveau produit en attendant que Matter élargisse sa portée.

Plutôt que de retarder la publication d'innovations, certains fabricants préféreront peut-être commercialiser des solutions de niche plus rapidement par des moyens propriétaires. Il est toujours possible de certifier ultérieurement une fois que les profils concernés auront atteint leur maturité. Pour profiter des avantages du premier arrivé, il peut être préférable de se direct-to-consumer passer de Matter dans certains cas.

Une alternative : utiliser un proxy sur les passerelles

Dans les situations où un terminal présente des limites qui empêchent la certification Matter directe, une autre approche consiste à transférer la capacité Matter de l'appareil par proxy à une passerelle. La passerelle sert de pont entre le protocole sans fil local du terminal et le protocole Matter basé sur IP.

Par exemple, un capteur de température de base communiquant via un standard radio propriétaire peut toujours apparaître comme un appareil Matter pour l'administrateur Matter. La passerelle reçoit les données des capteurs sur une interface non IP mais expose aux contrôleurs des entités Matter

virtuelles représentant ces données via IP. Cela vous permet d'utiliser le matériel existant et de bénéficier de certains avantages d'interopérabilité via la passerelle.

Bien entendu, cela ajoute de la complexité aux développeurs et nécessite des passerelles pour prendre en charge la couche de traduction nécessaire. Mais cela peut constituer un compromis viable dans les cas où la certification directe est trop difficile pour l'appareil lui-même. Les proxys pourraient aider les solutions de faible consommation ou de niche à participer aux écosystèmes Matter sans une refonte complète du matériel.

Connectivité au cloud avec Matter

Bien que Matter permette l'interopérabilité de base des appareils locaux, une connectivité cloud supplémentaire est nécessaire pour fournir des over-the-air mises à jour robustes, des données de télémétrie, une gestion à distance et une intégration avec les services des fournisseurs propriétaires. Les fabricants d'appareils disposent d'options, telles que l'expédition d'un hub Matter, l'utilisation du hub certifié Matter d'un foyer ou l'intégration d'une connectivité cloud directe aux terminaux. Les normes de atter-to-cloud connectivité M émergent, mais les fabricants doivent encore intégrer des piles de logiciels de connectivité supplémentaires dans les appareils Matter. Pour tirer le meilleur parti des appareils domotiques dans des domaines tels que les diagnostics et les mises à jour des nouvelles fonctionnalités, les fabricants de Matter doivent envisager l'intégration dans le cloud, au-delà du simple fonctionnement local.

Activation des fonctionnalités avancées des appareils grâce à la connectivité au cloud pour les terminaux Matter

La norme Matter promet d'unifier les appareils IoT de différents fournisseurs via un protocole commun. Il indique comment les appareils domotiques découvrent, communiquent et interagissent les uns avec les autres sur le réseau local à l'aide de technologies réseau basées sur IP, telles que Ethernet, Wi-Fi et Thread. Cette interopérabilité locale permet aux appareils certifiés Matter de différents fournisseurs de fonctionner ensemble de manière fluide pour des activités telles que les scènes automatisées et le contrôle vocal. Cependant, Matter ne définit pas les interfaces cloud et ne nécessite pas de connectivité Internet pour les terminaux de l'appareil.

De nombreux appareils intelligents s'appuient aujourd'hui sur une connectivité cloud supplémentaire pour les fonctionnalités clés, telles que les mises à jour over-the-air (OTA), l'accès à distance et les intégrations avec les plateformes des fabricants. Les fabricants d'appareils qui cherchent à créer des produits conformes à Matter tout en conservant des fonctionnalités avancées sont confrontés à certaines considérations de conception lorsqu'il s'agit de compléter Matter par une connectivité cloud. Bien que le contrôle local de base et l'intégration de l'assistant vocal fonctionnent pour les appareils Simple Matter, une connectivité cloud supplémentaire est nécessaire pour permettre des fonctionnalités plus avancées.

Cas d'utilisation nécessitant une connectivité au cloud

Bien que Matter gère l'interopérabilité des appareils locaux, la connectivité supplémentaire au cloud permet plusieurs fonctionnalités importantes des appareils domotiques :

- Mises à jour O ver-the-air (OTA) — La diffusion de mises à jour de micrologiciels et de logiciels via Internet permet aux fournisseurs d'améliorer facilement les appareils déjà déployés. Sans OTA, les mises à jour seraient gérées manuellement. Bien que la norme Matter décrit la manière dont les mises à jour OTA sont gérées et fournies aux points de terminaison certifiés Matter, elle dépend des fonctionnalités prises en charge par le hub Matter auquel le point de terminaison est connecté. En outre, il existe des restrictions concernant les mises à jour fournies au terminal. Par exemple, lorsque le point de terminaison demande une mise à jour, seule la dernière mise à jour disponible est fournie. Tous les appareils du même type bénéficient de cette mise à jour unique. Il n'est pas possible d'effectuer une mise à jour séquentielle, ni même une annulation OTA ou la suppression d'une mise à jour. L'activation de la connectivité cloud sur le terminal peut pallier ce manque de gestion précise des mises à jour OTA.
- Accès et contrôle à distance — L'accès et le contrôle à distance des appareils depuis l'extérieur du réseau domestique nécessitent un point de terminaison dans le cloud. La matière, telle que définie actuellement, ne prend en charge que l'accès local. Bien qu'un point de terminaison Matter puisse être contrôlé à l'aide d'une application utilisateur sur le réseau local, le contrôle à distance n'est disponible que s'il est pris en charge par le hub Matter. Même dans ce cas, seules les télécommandes de base sont généralement disponibles.
- Télémétrie et diagnostic — L'agrégation des données de terrain, telles que les journaux d'erreurs et les flux de capteurs, dans le cloud permet aux fournisseurs de surveiller l'état de santé des appareils et d'identifier les problèmes. Bien que Matter prenne en charge les diagnostics liés à la radio et aux protocoles via le cluster de diagnostic général, tout diagnostic détaillé spécifique à l'appareil nécessite une connectivité au cloud afin que le fabricant puisse récupérer les données de l'appareil.
- Intégrations spécifiques au fournisseur — Toutes les fonctionnalités et tous les types de données personnalisés qui ne sont pas définis dans la spécification Matter nécessitent une connectivité aux plateformes cloud des fournisseurs.
- Intégrations externes — La création de liens vers des services tiers tels que des assistants vocaux ne faisant pas partie de l'écosystème Matter ou des passerelles de paiement tierces (selon les besoins) nécessite une connectivité Internet au-delà de l'administrateur Matter.

Ces fonctionnalités critiques s'appuyant sur la connectivité au cloud, les terminaux Matter ont souvent besoin d'options supplémentaires pour accéder à Internet.

Architectures pour permettre la connectivité au cloud

Pour les appareils Matter, il existe trois approches générales pour fournir la connectivité cloud nécessaire tout en respectant les spécifications de fonctionnement locales.

Hub domotique avec passerelle intégrée

Certains fabricants d'appareils peuvent choisir de proposer un hub domestique propriétaire intégrant à la fois l'administrateur Matter et une passerelle vers leurs services cloud. Ce hub domestique gérerait les points de terminaison Matter connectés localement conformément à la norme, tout en facilitant les connexions au cloud pour les fonctions avancées. Le hub pourrait prendre en charge les mises à jour OTA, l'accès à distance et la collecte de données télémétriques pour les terminaux.

Déchargez la connectivité cloud vers un hub Matter existant

Plutôt que de regrouper un hub personnalisé, les appareils pourraient être conçus pour se connecter à des hubs Matter tels qu'Amazon Echo ou Google Home pour la connectivité Internet. Dans ce cas, le hub Matter existant gère les communications entre appareils locaux conformément à la norme et fournit également une passerelle vers le cloud pour les terminaux qui en ont besoin. Cela permet de tirer parti de l'infrastructure dont disposent peut-être déjà les consommateurs. Cependant, cette approche dépend du niveau de support offert par le hub Matter pour les fonctionnalités qui ne sont pas spécifiées comme normatives pour les hubs Matter dans le standard.

Connectivité directe au cloud dans les terminaux

Les appareils dotés d'une connectivité directe à Internet, tels que le Wi-Fi, pourraient intégrer une connectivité distincte pour le réseau local Matter et pour les services cloud des fournisseurs. Cela permet à l'appareil d'agir comme sa propre passerelle vers le cloud. Cependant, des solutions sont nécessaires pour les terminaux non Wi-Fi qui s'appuient sur des protocoles tels que Thread. Cela permet aux appareils de se connecter au cloud de manière indépendante, mais cela peut ne pas être faisable pour les appareils simples, peu coûteux et alimentés par batterie.

Bridging Matter et les plateformes cloud des fabricants

Bien que Matter simplifie l'interopérabilité locale, des efforts supplémentaires sont nécessaires pour connecter en douceur les systèmes d'administration Matter aux plateformes cloud des fabricants.

Organisations telles que la Connectivity Standards Alliance (CSA) s'efforcent de normaliser la manière dont les appareils Matter interagissent avec le cloud pour des fonctionnalités telles que les mises à jour OTA. L'adoption généralisée de normes pour cette connectivité cloud faciliterait le développement pour les fabricants d'appareils.

Le chemin optimal dépend des cas d'utilisation, des prix et des modèles commerciaux de produits spécifiques. Il est clair qu'un accès robuste aux services cloud est nécessaire pour bénéficier de toutes les fonctionnalités attendues par les consommateurs de maisons intelligentes, même pour les appareils compatibles Matter axés sur l'interopérabilité locale. Les fabricants d'appareils ont la possibilité d'utiliser Matter à des fins d'interopérabilité tout en fournissant des fonctionnalités avancées grâce à une connectivité cloud soigneusement conçue.

Sécurité

La sécurité dès la conception est la pratique qui consiste à intégrer des fonctions de sécurité au cours de la phase de conception de l'appareil, plutôt qu'après coup lors des étapes ultérieures du développement. Les communications cryptées et les mises à jour over-the-air (OTA) sont des exemples de sécurité dès la conception. Matter fournit une base solide pour les appareils domotiques en mettant en œuvre la sécurité dès la conception, en commençant par une usine de fabrication fiable et sécurisée. Les appareils Matter ne peuvent être fabriqués et approvisionnés que par les propriétaires d'une autorité de certification (CA) connue et fiable.

Authentification des appareils

Les appareils Matter doivent s'authentifier les uns auprès des autres et auprès d'un contrôleur avant de pouvoir communiquer. Seuls les appareils autorisés peuvent se connecter au Matter Fabric. Au cours de la fabrication, les appareils sont fournis avec une identité unique et un certificat X.509 connu sous le nom de certificat d'attestation de périphérique (DAC). Lorsque l'appareil tente de se connecter au Matter Fabric pour la première fois, le dispositif du commissaire vérifie la validité du DAC et s'il est signé par une autorité de certification PAI (Product Attestation Intermediate) connue et fiable. Le dispositif du commissaire vérifie également si l'appareil qui tente de se connecter au réseau respecte les spécifications, les protocoles et les normes de sécurité de Matter. L'appareil n'a accès au tissu Matter que si tous les contrôles sont réussis.

Communication cryptée

Une fois que l'appareil a obtenu l'accès à la Matter Fabric, toutes les données transmises entre les appareils sont sécurisées par un cryptage renforcé. L'intégrité des données est préservée grâce à une approche à plusieurs niveaux. Le commissaire Matter effectue l'échange de clés et la vérification des signatures à l'aide de la courbe ECC-256 secp256r1. Une fois les clés échangées, les appareils Matter cryptent les données en transit à l'aide du protocole AES-256. Pour chaque message, les appareils utilisent l'algorithme SHA-256 pour vérifier que les données n'ont pas été altérées pendant la transmission.

O ver-the-air mises à jour

La norme Matter exige également que les appareils mettent en œuvre une posture de sécurité robuste pour les mises à jour over-the-air (OTA). L'OTA est un élément essentiel d'un écosystème

domotique afin que les appareils puissent recevoir des mises à jour de sécurité ainsi que de nouvelles fonctionnalités. Chaque mise à jour du microprogramme pour les appareils Matter doit être signée par la clé privée du fabricant. Le dispositif vérifie la signature de la charge utile à l'aide de la clé publique asymétrique correspondante. Une fois la signature de la charge utile vérifiée, le périphérique peut valider l'image dans son chargeur de démarrage et la réinitialiser. Au cours du processus de démarrage, le périphérique doit à nouveau vérifier l'image pour s'assurer qu'elle n'a pas été altérée, et le périphérique vérifie également qu'il exécute la dernière version connue.

Développement avec la matière

Utilisation d'Alexa

Amazon propose une suite complète d'outils pour le développement de Matter. Ces outils permettent de créer rapidement des produits Matter compatibles avec tous les principaux écosystèmes et parfaitement compatibles avec Amazon Alexa.

Programme : Fonctionne avec Alexa

Ce programme garantit que vos appareils connectés à Alexa offrent une expérience client exceptionnelle. Le badge Works with Alexa (WWA) renforce la confiance des clients, ce qui contribue à définir les préférences pour vos appareils certifiés. Pour plus d'informations, consultez Annonce du lancement de Matter et Présentation de Works with Alexa (WWA) pour les appareils Matter (article de blog Amazon).

SDK : Develop Matter avec Alexa

Ce SDK vous permet d'ajouter une connectivité Matter locale à votre appareil tout en incluant une connectivité cloud gérée, des informations commerciales et un support OTA. Pour plus d'informations, consultez Tirez le meilleur parti de Matter avec Alexa.

Kit : Kit de développement Alexa Ambient Home

Ce kit vous permet d'intégrer des appareils à travers différents protocoles afin de créer une maison intelligente ambiante et unifiée avec Alexa. Pour plus d'informations, consultez Amazon Alexa.

Point de terminaison : point de terminaison commandable

Pour les appareils Matter connectés aux compétences, l'API Commissionable Endpoint crée une connexion locale basée sur Matter avec les appareils Alexa sans aucune étape requise par votre client avec son autorisation. Pour plus d'informations, consultez Alexa.Commissionable Interface 1.0 (Alexa Skills Kit).

Autorité de certification privée AWS support pour Matter

AWS Private Certificate Authority (Autorité de certification privée AWS) fournit des conseils sur l'utilisation de la norme Matter.

DAC pour Matter

Matter nécessite un certificat d'attestation d'appareil (DAC), qui doit être délivré par une autorité de certification d'appareil conforme à la politique de certification (CP) de Matter en matière d'infrastructure à clé publique (PKI). Les fournisseurs d'appareils peuvent Autorité de certification privée AWS effectuer les opérations suivantes :

- Héberger l'autorité de certification (CA) de l'autorité d'attestation du produit (PAA)
- Hébergez le CA intermédiaire d'attestation de produit (PAI)
- Émission, signature et maintenance du DAC de chaque appareil

Pour plus d'informations, consultez la section Utiliser AWS Private Certificate Authority pour émettre des certificats d'attestation d'appareil pour Matter dans le blog sur la AWS sécurité.

L'infrastructure pour la matière

AWS fournit un exemple illustrant l'utilisation de AWS Cloud Development Kit (AWS CDK)pour configurer une infrastructure PKI pour Matter. Vous devez Autorité de certification privée AWS répondre aux exigences du Matter PKI CP. Pour plus d'informations, consultez le projet Matter PKI CDK sur. GitHub

Exemples Java

Autorité de certification privée AWS fournit des exemples Java pour créer des certificats PAA (Product Attestation Authority) conformes à Matter, des certificats PAI (Product Attestation Intermediate) et des certificats d'attestation d'appareil (DAC) conformes à la norme Matter. Pour plus d'informations, consultez la section Utilisation de l' Autorité de certification privée AWS API pour implémenter le standard Matter (exemples Java) dans la AWS Private Certificate Authority documentation.

Guide de conformité à la PKI de Matter

Ce guide de conformité Matter PKI explique comment mettre en œuvre et démontrer la conformité aux exigences CSA Matter PKI CP. Il fournit des informations sur la manière dont vous pouvez créer et exploiter des autorités de certification (CA) conformes à Matter. Autorité de certification privée AWS

FAQ

Quels sont les niveaux d'adhésion à Matter ?

En janvier 2023, Matter comptait les quatre niveaux d'adhésion suivants.

Type de membre	Frais d'adhésion annuels (USD)	Description
Promoteur	105 000$	Diriger l'alliance avec l'approbation finale de toutes les normes, siéger au conseil d'administration et participer aux comités du conseil
Participant	20 000$	Contribuez aux normes et accédez aux projets de spécifications pour accélérer la mise sur le marché
Adopteur	7 000$	Utiliser des spécifications approuvées pour créer et certifier des produits
Associé	0 $*	Étiqueter un produit certifié par le biais du programme de transfert de certification

*Pour les membres associés qui mettent en marque blanche ou renomment un produit, cela coûte des frais initiaux de 2 500$ (USD) par produit et des frais permanents de 500$ par produit et par an.

Le niveau d'adhésion que vous choisissez dépend de votre intérêt à certifier un produit (adoptant) ou à définir le type de produit dans le cadre de la norme (participant). Pour plus d'informations sur les niveaux d'adhésion, consultez Impact the Future of the IoT sur le site Web de la CSA.

Quels sont les avantages de Matter pour les consommateurs de maisons intelligentes ?

Les consommateurs bénéficient de Matter des manières suivantes :

- Intégration simplifiée d'un appareil Matter à domicile
- Gestion unifiée de tous les appareils domotiques via une seule application
- Contrôle des appareils à partir d'un ou plusieurs assistants vocaux de différents écosystèmes

Pour plus d’informations, consultez Avantages de la certification Matter pour les consommateurs de maisons intelligentes dans ce guide.

Comment les fabricants d'appareils bénéficient-ils de Matter ?

Les fabricants d'appareils tirent parti de Matter des manières suivantes :

- Une certification unique pour un appareil au lieu de plusieurs certifications pour chaque écosystème, comme Amazon Alexa ou Google Home.
- Le développement de l'application n'est plus nécessaire
- Réduction des coûts des matériaux grâce au fait qu'il n'est pas nécessaire d'expédier les éléments d'infrastructure (tels qu'un routeur Thread Border)
- Réduction des coûts liés à l'assistance aux clients confrontés à des problèmes d'infrastructure et de connectivité

Pour plus d’informations, consultez Avantages de la certification Matter pour les fabricants d'appareils dans ce guide.

Matter remplace-t-il le Wi-Fi, le Bluetooth ou le Thread ?

Non, Matter est un protocole au niveau de l'application qui s'exécute sur les réseaux IP. Les appareils qui utilisent le Wi-Fi, l'Ethernet ou le Thread pour la connectivité peuvent obtenir la certification Matter. Le tableau suivant résume le contraste entre Matter et le Wi-Fi, le Bluetooth et le Thread.

Fonctionnalité	Matière	Wi-Fi	Bluetooth	Thread
Objectif	Communication domestique intelligente	Accès à Internet et transfert de données	Communication sans fil à courte portée	Réseau maillé sans fil basse consommation
Range	Varie en fonction du protocole sous-jacent	Jusqu'à 300 pieds	Jusqu'à 30 pieds	Jusqu'à 300 pieds
Bande passante	Varie en fonction du protocole sous-jacent	Jusqu'à 10 gigabits par seconde	Jusqu'à 2 mégabits par seconde	Jusqu'à 250 kilobits par seconde
Consommation d’énergie	Varie en fonction du protocole sous-jacent	Relativement élevé	Relativement faible	Très faible
Sécurité	Varie en fonction du protocole sous-jacent	WPA2, WPA3	Connexions sécurisées AES, BLE	AES
Coût	Varie en fonction de l'appareil	Relativement peu coûteux	Relativement peu coûteux	Relativement cher

Qu'est-ce qu'un identifiant de fournisseur et un identifiant de produit ?

Les membres de la CSA peuvent demander un identifiant de fournisseur qui les identifie en tant que fournisseur. Les produits de l'entreprise sont désormais associés à cet identifiant et peuvent être retracés jusqu'à leur origine. En outre, ils reçoivent un identifiant de produit unique. Le code numérique à 16 chiffres accompagne les produits, comme un numéro de passeport, et les rend aussi identifiables que le vendeur.

Quels appareils doivent être certifiés Matter ?

Tous les appareils qui doivent s'authentifier et faire partie de la structure Matter doivent être certifiés Matter. Toutefois, les appareils conçus pour interagir uniquement avec le hub spécifié par le fournisseur via un protocole non standard (propriétaire) ne bénéficieraient pas du processus de certification Matter. Par exemple, un hub de système de sécurité domestique intelligent doit être certifié conforme à la norme Matter, mais un capteur de porte ou de fenêtre qui communique avec le hub n'a pas besoin d'être certifié conforme à Matter. Le choix de faire certifier un produit pour Matter est principalement motivé par cette considération.

Mon type de produit n'est actuellement pas défini dans Matter. Quelles tâches supplémentaires dois-je prévoir pour obtenir la certification Matter pour les produits ?

Les spécifications Matter ne sont pas compatibles avec tous les types d'appareils. Si votre type d'appareil n'est pas pris en charge, la première étape consiste à rejoindre le CSA en tant que participant. Cela nécessite un investissement financier et en temps dans le CSA. En tant que membre participant, vous dirigez la définition des types d'appareils et avez accès aux projets de spécifications qui permettent une go-to-market stratégie plus rapide. Pour plus d'informations sur les niveaux d'adhésion, consultez Impact the Future of the IoT sur le site Web de la CSA.

Certains de mes appareils se connectent directement au réseau Wi-Fi domestique. Ces appareils doivent-ils être certifiés Matter ?

La certification Matter peut profiter aux appareils qui se connectent directement au réseau domotique, car ils peuvent se connecter à la structure Matter. Cela permet aux consommateurs de contrôler les appareils via leurs assistants virtuels sur la même structure Matter. Cependant, les consommateurs doivent utiliser une application spécifique à l'appareil pour toutes les opérations spécifiques au fournisseur et non définies dans la spécification Matter.

Ressources

AWS ressources

- Tirez le meilleur parti de Matter avec Alexa
- Annonce du lancement de Matter et présentation de Works with Alexa (WWA) pour les appareils Matter (blog Amazon Alexa)

Connectivity Standards Alliance (CSA) pour l'IoT

- Site Web du CSA
- Vue d'ensemble du processus de certification CSA
- Fournisseurs de tests agréés par la CSA
- Spécifications de la matière

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	—	5 février 2024

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle locale vers Oracle sur une EC2 instance du AWS Cloud.
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers AWS.
- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, la AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications afin de préparer l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

AWS Cadre de qualification de la charge de travail (AWS WQF)

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

AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez À propos des branches (GitHub documentation).

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement

peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCo E

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour accélérer votre adoption du cloud (par exemple, créer une zone de landing zone, définir un CCo E, établir un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog The Journey Toward Cloud-First & the Stages of Adoption publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le guide de préparation à la migration.

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs

configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

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

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD is commonly described as a pipeline. CI/CDpeut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive

des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

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

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des

catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Voir reprise après sinistre.

détection de dérive

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

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

épopée

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

branche de fonctionnalités

Voir succursale.

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le modèle de fondation.

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiens

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

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

application inactive

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

IIo T

Voir Internet industriel des objets.

infrastructure immuable

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

VPC entrant (d'entrée)

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

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer

progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, voir Élaboration d'une stratégie de transformation numérique de l'Internet des objets (IIoT) industriel.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

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

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

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

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

lift and shift

Voir 7 Rs.

système de poids faible

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

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

Voir succursale.

malware

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

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir Migration Acceleration Program.

mécanisme

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

compte membre

Tous, à l' Comptes AWS exception du compte de gestion, qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des professionnels travaillant dans le cadre de sprints.

Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

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

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 avec le service de migration AWS d'applications.

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez la section Stratégie de modernisation des applications dans le AWS Cloud.

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant

l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

confidentialité dès la conception

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

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs VPCs domaines. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est

pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

CHIFFON

Voir Retrieval Augmented Generation.

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

Technologie d'IA générative dans laquelle un LLM fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir Qu'est-ce que RAG ?

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif relatif au temps de rétablissement.

runbook

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

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

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

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

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

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir environnement.

V

mise à vide

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

contrôle de version

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

Appairage de VPC

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

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

VER

Voir écrire une fois, lire plusieurs.

WQF

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

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire,

mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

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

vulnérabilité « jour zéro »

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

invite Zero-Shot

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

application zombie

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

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