Creating an enterprise encryption strategy for data at rest

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Creating an enterprise encryption strategy for data at rest

Table of Contents

Creating an enterprise encryption strategy for data at rest

Venki Srivatsav, Andrea Di Fabio et Vikramaditya Bhatnagar, Amazon Web Services ()AWS

Septembre 2022 (historique du document)

De nombreuses entreprises sont préoccupées par la menace de cybersécurité que représente une violation de données. Lorsqu'une violation de données se produit, une personne non autorisée accède à votre réseau et vole les données de l'entreprise. Les pare-feux et les services de protection contre les programmes malveillants peuvent vous aider à vous protéger contre cette menace. Une autre protection que vous pouvez mettre en œuvre est le chiffrement des données. Dans la section À propos du chiffrement des données de ce guide, vous pouvez en savoir plus sur le fonctionnement du chiffrement des données et les types disponibles.

Lorsque vous parlez de chiffrement, d'une manière générale, il existe deux types de données. Les données en transit sont les données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau. Les données au repos sont des données stationnaires et dormantes, telles que les données stockées. Cette stratégie met l'accent sur les données au repos. Pour plus d'informations sur le chiffrement des données en transit, consultez la section Protection des données en transit (AWS Well-Architected Framework).

Une stratégie de chiffrement comprend quatre parties que vous développez en phases séquentielles. La politique de chiffrement est déterminée par la haute direction et décrit les exigences réglementaires, de conformité et commerciales en matière de chiffrement. Les normes de chiffrement aident ceux qui mettent en œuvre la politique à la comprendre et à s'y conformer. Les normes peuvent être technologiques ou procédurales. Le cadre comprend les procédures opérationnelles, les structures et les garde-corps standard qui soutiennent la mise en œuvre des normes. Enfin, l'architecture est la mise en œuvre technique de vos normes de chiffrement, telles que l'environnement, les services et les outils que vous utilisez. L'objectif de ce document est de vous aider à créer une stratégie de chiffrement adaptée à vos besoins commerciaux, de sécurité et de conformité. Il inclut des recommandations sur la manière de revoir et de mettre en œuvre les normes de sécurité pour les données au repos afin que vous puissiez répondre à vos besoins commerciaux et de conformité de manière globale.

Cette stratégie utilise AWS Key Management Service (AWS KMS) pour vous aider à créer et à gérer des clés cryptographiques qui contribuent à protéger vos données. AWS KMS s'intègre à de nombreux AWS services pour chiffrer toutes vos données au repos. Même si vous choisissez un

autre service de chiffrement, vous pouvez toujours adopter les recommandations et les phases de ce guide.

Public visé

La stratégie est conçue pour s'adresser aux publics suivants :

- Les dirigeants qui formulent les politiques de leur entreprise CEOs, tels que les directeurs de la technologie (CTOs), les directeurs informatiques (CIOs) et les responsables de la sécurité informatique (CISOs)
- Les responsables technologiques chargés de définir les normes techniques, tels que les vice-présidents et directeurs techniques
- Responsables de la conformité et de la gouvernance chargés de contrôler le respect des politiques de conformité, y compris les régimes de conformité statutaires et volontaires

Résultats commerciaux ciblés

- Data-at-rest politique de chiffrement — Les décideurs et les décideurs peuvent créer une politique de chiffrement et comprendre les facteurs critiques qui influent sur cette politique.
- Data-at-rest normes de chiffrement — Les responsables techniques peuvent développer des normes de chiffrement basées sur la politique de chiffrement.
- Cadre de chiffrement — Les responsables techniques et les responsables de la mise en œuvre peuvent créer un cadre servant de pont entre ceux qui déterminent la politique et ceux qui créent les normes. Dans ce contexte, le cadre signifie identifier le processus et le flux de travail appropriés qui vous aident à mettre en œuvre les normes dans les limites de la politique. Un cadre est similaire à une procédure opérationnelle standard ou à un processus de gestion du changement pour modifier les politiques ou les normes.
- Architecture technique et mise en œuvre — Les implémenteurs pratiques, tels que les développeurs et les architectes, connaissent les références d'architecture disponibles qui peuvent les aider à mettre en œuvre la stratégie de chiffrement.

Limites

Ce document est destiné à vous aider à formuler une stratégie de chiffrement personnalisée qui répond le mieux aux besoins de votre entreprise. Il ne s'agit pas d'une stratégie de chiffrement en soi, ni d'une liste de contrôle de conformité. Les sujets suivants ne sont pas inclus dans ce document :

- chiffrement des données en transit
- Création de jeton
- Hachage
- Conformité et gouvernance des données
- Budgétisation de votre programme de chiffrement

Pour plus d'informations sur certains de ces sujets, consultez la Ressources section.

À propos du chiffrement des données

Cette section contient une présentation détaillée des concepts et de la terminologie du chiffrement. Le chiffrement des données vous aide à garantir la confidentialité des données. En mettant en œuvre le chiffrement et les contrôles d'accès, vous pouvez contribuer à protéger les données de votre entreprise.

À propos des clés de chiffrement

Les services de chiffrement utilisent une clé de chiffrement pour chiffrer les données. Une clé de chiffrement est une chaîne cryptographique de bits aléatoires générée par un algorithme de chiffrement. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique. La force du chiffrement dépend généralement de deux facteurs : la longueur de la clé et l'algorithme utilisé. En général, les clés plus longues fournissent un cryptage plus puissant.

À propos des algorithmes de chiffrement

Il existe deux types d'algorithmes pour générer des clés de chiffrement, symétriques et asymétriques.

Le chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer les données. Ce type de chiffrement est généralement plus rapide et est donc efficace pour de grandes quantités de données. Ce type de cryptage est largement utilisé et généralement considéré comme sécurisé. Comme une seule clé est utilisée à la fois pour le chiffrement et le déchiffrement, la meilleure pratique consiste à changer fréquemment la clé afin d'empêcher toute personne non autorisée de l'obtenir. Pour plus d'informations sur les cas Quand ai-je besoin d'un chiffrement symétrique ? dans lesquels le chiffrement symétrique est recommandé, consultez la section FAQ.

Le chiffrement asymétrique utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint. Le chiffrement asymétrique est généralement considéré comme plus sûr que le chiffrement symétrique, mais il est plus lent car il utilise des clés de plus grande longueur et nécessite des calculs de chiffrement plus complexes. Pour plus d'informations sur les cas Quand ai-je besoin d'un chiffrement asymétrique ? dans lesquels le chiffrement asymétrique est recommandé, consultez la section FAQ.

À propos du chiffrement des enveloppes

Lorsque vous chiffrez vos données, elles ne sont protégées que tant que votre clé de chiffrement reste secrète. La clé utilisée pour chiffrer les données est connue sous le nom de clé de données. Le chiffrement d'enveloppe consiste à chiffrer votre clé de données à l'aide d'une autre clé de chiffrement, appelée clé de chiffrement par clé. Vous pouvez même chiffrer cette clé avec une autre clé de chiffrement, et ainsi de suite. Finalement, une clé doit rester en texte brut pour que vous puissiez déchiffrer les clés et vos données. Cette clé de chiffrement de clé en texte brut de niveau supérieur porte le nom de clé racine.

Le chiffrement d'enveloppe offre plusieurs avantages :

- Commodité — Votre clé de données étant cryptée, vous pouvez la stocker avec les données cryptées.
- Efficacité — Les opérations de chiffrement peuvent prendre beaucoup de temps, en particulier lorsqu'il s'agit d'une grande quantité de données. Au lieu de rechiffrer des données brutes plusieurs fois avec des clés différentes, vous pouvez rechiffrer uniquement les clés de données qui protègent les données brutes. Cela vous permet de fournir au moins deux couches de protection par chiffrement sans rechiffrer les données.
- Performances — Vous pouvez combiner des algorithmes de chiffrement. Par exemple, vous pouvez utiliser le chiffrement symétrique pour les données brutes, mais utiliser le chiffrement asymétrique pour la clé de données, qui combine les points forts des deux algorithmes de chiffrement.

Pour plus d'informations sur le chiffrement des enveloppes, consultez la section Chiffrement des enveloppes (AWS Key Management Service documentation). Pour plus d'informations sur la manière de décider si vous avez besoin du chiffrement des enveloppes, consultez Quand ai-je besoin du chiffrement des enveloppes ? la section FAQ.

Phases de l'élaboration d'une stratégie de chiffrement

L'élaboration d'une stratégie de chiffrement au niveau de l'entreprise nécessite une approche en plusieurs étapes. Chaque phase définit un ensemble de contrôles pour vous aider à obtenir les résultats tangibles souhaités. Ce document vous guide tout au long de ces phases et vous pose des questions spécifiques pour vous aider à personnaliser votre stratégie de chiffrement.

L'élaboration d'une stratégie de chiffrement pour les données au repos comprend les phases séquentielles suivantes :

1. Politique de chiffrement— Élaborez une politique qui définit les objectifs de data-at-rest chiffrement de votre entreprise.
2. Normes de chiffrement— Définissez les normes techniques et procédurales qui vous aident à mettre en œuvre la politique de votre entreprise.
3. Cadre de chiffrement— Créez le cadre qui aide toutes les parties prenantes à comprendre, modifier et mettre en œuvre vos normes de chiffrement.
4. Mise en œuvre— Déployez votre infrastructure de chiffrement.

Politique de chiffrement

L'objectif d'une politique de chiffrement est d'établir, au niveau de la haute direction, les attentes commerciales et de conformité auxquelles l'organisation doit répondre. La politique sert de point de départ pour définir une stratégie de chiffrement adaptée. La politique doit être suffisamment abstraite pour garantir la liberté et la flexibilité nécessaires à sa mise en œuvre. En même temps, il doit être suffisamment précis pour définir les limites d'une mise en œuvre acceptable répondant aux objectifs de l'organisation. En général, les politiques sont indépendantes de la technologie et sont très rarement modifiées, car elles définissent les caractéristiques fondamentales de la stratégie de chiffrement de votre entreprise.

En général, les politiques de chiffrement contiennent, sans toutefois s'y limiter, les éléments suivants :

- Tous les régimes réglementaires ou de conformité auxquels votre entreprise doit se conformer
- Tout engagement commercial ou toute attente en matière de chiffrement des données
- Le type de données qui doivent être cryptées

- Critères relatifs à l'utilisation de techniques de protection des données autres que le chiffrement, telles que le hachage ou la tokenisation

Le niveau de gestion le plus élevé de l'organisation, tel que le CIO, le CTO et le CISO, définit et approuve généralement la politique de chiffrement.

Tenez compte des points suivants lors de la création de votre politique de chiffrement :

- Votre secteur d'activité détermine les régimes de conformité et de réglementation que vous devez respecter. Ces régimes dictent les exigences en matière de chiffrement des données. Les décisions prises au niveau de la direction pour étendre l'activité à de nouvelles régions ou étendre l'offre de produits peuvent avoir une incidence sur les réglementations applicables à vos données. Par exemple, si une banque décide de proposer des cartes de crédit à ses clients, ils doivent probablement se conformer à la norme de sécurité des données (PCI-DSS) du secteur des cartes de paiement, qui exige le cryptage des données.
- Votre politique doit spécifier le type de données à chiffrer. Cela varie en fonction des exigences de conformité et des objectifs de traitement des données de votre entreprise. Par exemple, votre politique peut stipuler que toutes les données capturées ou détenues par l'entreprise doivent être cryptées au repos.
- Votre politique de chiffrement doit être conforme à vos normes internes de catégorisation des données. Pour formuler une politique de chiffrement efficace, il est nécessaire de déterminer les catégories de données au niveau des métadonnées. Par exemple, vos catégories peuvent inclure des données publiques, internes, confidentielles, secrètes ou des données clients.
- Incluez des critères permettant de déterminer quelles données doivent être cryptées et quelles données doivent être protégées par une autre technique, telle que la tokenisation ou le hachage. Par exemple, votre politique peut stipuler que toutes les informations personnelles identifiables (PII) qui sont enregistrées dans les journaux d'audit, de suivi ou d'application doivent être tokenisées.

Normes de chiffrement

Les normes sont dérivées de votre politique. Ils ont une portée plus étroite et aident à définir le cadre et l'architecture de mise en œuvre. Par exemple, si la politique de votre entreprise consiste à chiffrer vos données au repos, une norme définira le type de chiffrement requis et fournira des directives générales sur la manière de respecter cette politique.

Les normes de chiffrement spécifient généralement les éléments suivants :

- Les types de chiffrement à utiliser
- Spécifications minimales pour les clés de chiffrement
- Qui a accès aux clés de chiffrement
- Où les clés de chiffrement doivent être stockées
- Critères de sélection d'une force de clé appropriée lors du choix des techniques de chiffrement ou de hachage
- Fréquence de rotation des touches

Bien qu'il soit rarement nécessaire de mettre à jour une politique de chiffrement, les normes de chiffrement sont susceptibles de changer. Le secteur de la cybersécurité évolue constamment pour répondre au paysage des menaces en constante évolution. Par conséquent, vos normes devraient changer pour adopter les dernières technologies et les meilleures pratiques afin de fournir la meilleure protection possible aux données de votre entreprise.

Dans une entreprise, les vice-présidents, les directeurs ou les responsables des données définissent généralement les normes de chiffrement, et un responsable de la conformité les examine et les approuve généralement.

Tenez compte des catégories de facteurs suivantes lors de la définition et de la mise à jour des normes de chiffrement dans votre organisation :

- Considérations relatives aux coûts et aux performances
- Contrôle d'accès par clé
- Types de chiffrement
- Spécifications des clés de chiffrement
- Emplacement de stockage des clés

Considérations relatives aux coûts et aux performances

Tenez compte des facteurs opérationnels suivants lors de la détermination des normes de chiffrement pour les données au repos :

- Les ressources matérielles disponibles doivent être en mesure de prendre en charge vos normes à grande échelle.

- Le coût du chiffrement varie en fonction de la longueur de la clé, de la quantité de données et du temps nécessaire pour effectuer le chiffrement. Par exemple, comparé au chiffrement symétrique, le chiffrement asymétrique utilise des clés plus longues et prend plus de temps.
- Tenez compte des exigences de performance de vos applications d'entreprise. Si votre application nécessite une faible latence et un débit élevé, vous pouvez utiliser le chiffrement symétrique.

Contrôle d'accès par clé

Identifiez les politiques de contrôle d'accès pour vos clés de chiffrement en fonction du principe du moindre privilège. Le moindre privilège est la bonne pratique en matière de sécurité qui consiste à accorder aux utilisateurs l'accès minimum dont ils ont besoin pour exécuter leurs tâches. Dans vos normes, définissez une politique de contrôle d'accès qui :

- Identifie les rôles qui gèrent les clés de chiffrement des clés et les clés de données.
- Définit et associe les autorisations clés aux rôles. Par exemple, il définit qui possède les principaux privilèges d'administrateur et qui possède les principaux privilèges d'utilisateur. Les administrateurs de clés peuvent créer ou modifier des clés de chiffrement des clés, et les utilisateurs clés peuvent chiffrer et déchiffrer les données et générer des clés de données.

Types de chiffrement

Dans vos normes, définissez les types et fonctionnalités de chiffrement adaptés à votre organisation :

- Documentez quand utiliser des algorithmes de chiffrement symétriques et asymétriques. Pour plus d'informations, consultez Quand ai-je besoin d'un chiffrement symétrique ? et Quand ai-je besoin d'un chiffrement asymétrique ? consultez la section FAQ.
- Décidez si vous devez utiliser le chiffrement des enveloppes et définissez les circonstances. Pour plus d'informations, consultez Quand ai-je besoin du chiffrement des enveloppes ? la section FAQ.
- Définissez les critères d'utilisation des alternatives de chiffrement, telles que la tokenisation et le hachage.

Spécifications des clés de chiffrement

Définissez les spécifications requises pour vos clés de chiffrement, telles que la puissance des clés et les algorithmes. Ces spécifications doivent être conformes aux régimes réglementaires et de conformité définis dans la politique. Pensez à définir les spécifications suivantes :

- Définissez la puissance de clé minimale et les algorithmes pour les types de chiffrement symétriques et asymétriques. Les principaux facteurs de force incluent la longueur, le caractère aléatoire et le caractère unique.
- Définissez à quel moment vous souhaitez implémenter les nouvelles versions des algorithmes de chiffrement. Par exemple, vos normes peuvent indiquer « Implémenter la dernière version de l'algorithme dans les 30 jours suivant sa publication » ou « Toujours utiliser une version antérieure à la dernière version ».
- Définissez l'intervalle de rotation de vos clés de chiffrement.

Emplacement de stockage des clés

Dans vos normes, tenez compte des points suivants lorsque vous décidez où stocker vos clés de chiffrement :

- Les exigences réglementaires et de conformité peuvent dicter l'endroit où vos clés de chiffrement peuvent être stockées.
- Décidez si vous souhaitez stocker les clés dans un emplacement centralisé ou avec les données correspondantes. Pour plus d'informations, consultez Pourquoi devrais-je gérer les clés de chiffrement de manière centralisée ? la section FAQ.
- Si vous optez pour le stockage centralisé, décidez si vous souhaitez stocker les clés dans une infrastructure gérée par l'entreprise, telle qu'un module de sécurité matériel (HSM), ou dans un fournisseur de services gérés, tel que. AWS Key Management Service Pour plus d'informations, consultez Quand dois-je utiliser un module de sécurité matériel (HSM) ? la section FAQ.

Cadre de chiffrement

Dans ce contexte, un framework fait référence à un ensemble de procédures opérationnelles standard qui doivent être suivies lorsque vous modifiez les normes ou la politique de chiffrement. Le cadre est l'échafaudage qui vous aide à mettre en œuvre les normes. Cela aide à transformer les paroles en actions. Le cadre relie les personnes qui définissent les normes à celles qui les mettent en œuvre.

Les frameworks incluent généralement les sujets suivants :

- Classification des données
- Classification environnementale

- Événements et processus de changement

Classification des données

La classification des données joue un rôle essentiel dans la création d'une stratégie de chiffrement. La classification des données est le processus qui consiste à attribuer des données à une catégorie en fonction de leur sensibilité. Les catégories de classification des données les plus courantes sont les suivantes, classées par ordre croissant de sensibilité : public, privé, interne, confidentiel et restreint.

Votre infrastructure de chiffrement doit inclure les informations suivantes concernant la classification des données :

- Les catégories de classification des données pour votre entreprise.
- Les critères de classification utilisés pour classer les données dans la catégorie appropriée. Par exemple, la recette commerciale d'une entreprise peut être considérée comme restreinte, les informations personnelles des employés peuvent être confidentielles et les communications internes entre les employés via les canaux officiels peuvent être internes.
- Processus utilisé pour promouvoir et rétrograder les données entre les catégories.
- Les critères d'accès pour chaque catégorie de classification des données.
- Le type de clé de chiffrement requis pour chaque catégorie.

Classification environnementale

Votre entreprise peut disposer de plusieurs environnements, tels que le développement, les tests, le bac à sable, la préproduction et la production. Chaque environnement peut contenir différents types de données et avoir des exigences de chiffrement différentes.

Votre infrastructure de chiffrement doit inclure les informations suivantes concernant vos environnements :

- Définissez les environnements de votre entreprise.
- Définissez les exigences de chiffrement pour chaque environnement. Par exemple, vous pouvez utiliser une clé de chiffrement unique pour toutes les catégories de données de votre environnement de développement, et dans votre environnement de production, vous pouvez utiliser des clés de chiffrement différentes pour chaque application métier ou catégorie de classification de données.

Événements et processus de changement

Les normes de chiffrement sont soumises à de fréquentes modifications afin que vous puissiez rester au fait des dernières technologies, des meilleures pratiques et des innovations. Voici les événements de modification courants susceptibles de déclencher une révision de vos normes de chiffrement :

- Modifications de la longueur minimale des clés de chiffrement
- Modifications de la puissance d'un algorithme de chiffrement
- Modifications apportées aux personnes autorisées à accéder aux clés de chiffrement ou à la méthode
- Modification des intervalles de rotation de vos clés
- Modifications apportées au processus de suppression des clés
- Modifications apportées à l'emplacement ou aux politiques de stockage des clés
- Modifications apportées au processus de sauvegarde et de restauration des clés

Votre infrastructure de chiffrement doit inclure les éléments suivants afin de préparer votre organisation à gérer, mettre en œuvre et communiquer les modifications apportées aux normes ou politiques de chiffrement :

- Processus de contrôle du changement — Le but de ce processus est de planifier et de préparer le changement à venir. Lorsque vous devez modifier vos normes ou politiques de chiffrement, ce processus reproductible et évolutif est conçu pour définir :
  - Comment votre organisation évalue l'impact du changement
  - Qui peut initier les changements
  - Qui est responsable de la mise en œuvre du changement
  - Qui est responsable de l'approbation de la modification
  - Comment votre organisation annulerait le changement, si nécessaire
- Processus d'auditabilité et de traçabilité des modifications — Ce processus définit la manière dont votre organisation audite et suit les modifications, à la fois au niveau des métadonnées et au niveau des données. Il doit définir la manière dont vous conservez et accédez aux enregistrements des éléments suivants :
  - Qu'est-ce qui a changé
  - Quand il a été modifié
  - Qui a initié, approuvé et mis en œuvre le changement

Par exemple, si votre organisation modifie la puissance minimale de la clé de chiffrement, vous devriez être en mesure de déterminer les exigences initiales et nouvelles, la date d'entrée en vigueur de la modification et les personnes impliquées dans le processus de modification.

- Processus de mise en œuvre des modifications — L'objectif de ce processus est de définir comment votre organisation met en œuvre le changement une fois que vous avez décidé de le faire. Ce processus définit :
  - Qui sont les parties prenantes
  - Si vous devez réaliser un projet pilote ou une preuve de concept
  - Comment et quand vous devez communiquer le statut du changement
  - Comment annuler la modification, si nécessaire.
  - Quelle devrait être la période d'observation après la mise en œuvre du changement.
  - Quel sera le processus d'observation pour suivre l'impact du changement, y compris la manière de recueillir des commentaires sur le changement et d'évaluer son efficacité
- Processus de retrait — L'objectif de ce processus est de définir la manière dont votre organisation gère le retrait des ressources et des informations liées au chiffrement. Il comprend des instructions pour le départ à la retraite proprement dit ainsi que le processus de communication pour le départ à la retraite.

Mise en œuvre

Dans cette stratégie, l'architecture fait référence à la mise en œuvre technique de vos normes de chiffrement. Cette section contient des informations sur la manière dont Services AWSAWS Key Management Service (AWS KMS) et AWS CloudHSM, peuvent vous aider à mettre en œuvre votre stratégie de data-at-rest chiffrement conformément à votre politique et à vos normes.

AWS KMS est un service géré qui vous aide à créer et à contrôler les clés cryptographiques utilisées pour protéger vos données. Les clés KMS ne quittent jamais le service sans être chiffrées. Pour utiliser ou gérer vos clés KMS, vous interagissez avec elles AWS KMS, et bon nombre d'entre Services AWS elles sont intégrées AWS KMS.

AWS CloudHSM est un service cryptographique permettant de créer et de gérer des modules de sécurité matériels (HSMs) dans votre AWS environnement. HSMs sont des dispositifs informatiques qui traitent des opérations cryptographiques et fournissent un stockage sécurisé pour les clés cryptographiques. Si vos normes vous obligent à utiliser du matériel validé FIPS 140-2 niveau 3, ou si vos normes imposent l'utilisation de normes industrielles APIs, telles que PKCS #11, Java

Cryptography Extensions (JCE) et Microsoft CryptoNG (CNG), vous pouvez envisager d'en utiliser. AWS CloudHSM

Vous pouvez AWS CloudHSM le configurer en tant que magasin de clés personnalisé pour AWS KMS. Cette solution combine la commodité et l'intégration des services AWS KMS avec les avantages supplémentaires en termes de contrôle et de conformité liés à l'utilisation d'un AWS CloudHSM cluster dans votre Compte AWS. Pour plus d'informations, consultez la section Stockages de clés personnalisés (AWS KMS documentation).

Ce document présente les AWS KMS fonctionnalités de haut niveau et explique comment AWS KMS vous pouvez répondre à votre politique et à vos normes.

Coût, commodité et contrôle

AWS KMS propose différents types de clés. Certains sont détenus ou gérés par des clients AWS, tandis que d'autres sont créés et gérés par des clients. Vous pouvez choisir entre les options suivantes en fonction du niveau de contrôle que vous souhaitez avoir sur les considérations clés et financières :

- AWS clés possédées : AWS possède et gère ces clés, et elles sont utilisées à plusieurs reprises Comptes AWS. Certains Services AWS prennent en charge les clés AWS détenues. Vous pouvez utiliser ces clés gratuitement. Ce type de clé vous évite les coûts et les frais administratifs liés à la gestion du cycle de vie des clés et à l'accès à celles-ci. Pour plus d'informations sur ce type de clé, consultez la section Clés AWS détenues (AWS KMS documentation).
- AWS clés gérées — Si un Service AWS est intégré à AWS KMS, il peut créer, gérer et utiliser ce type de clés en votre nom, afin de protéger vos ressources dans ce service. Ces clés sont créées dans votre Compte AWS et ne Services AWS peuvent être utilisées que par elles. Il n'y a pas de frais mensuels pour une clé AWS gérée. Ils peuvent être soumis à des frais d'utilisation en sus du niveau gratuit, mais certains Services AWS couvrent ces coûts pour vous. Vous pouvez utiliser des politiques d'identité pour contrôler l'accès à l'affichage et à l'audit de ces clés, mais vous gérez AWS le cycle de vie des clés. Pour plus d'informations sur ce type de clé, consultez la section Clés AWS gérées (AWS KMS documentation). Pour une liste complète de ceux Services AWS qui s'intègrent AWS KMS, voir Service AWS Intégration (AWS marketing).
- Clés gérées par le client : vous créez, détenez et gérez ce type de clé, et vous avez un contrôle total sur le cycle de vie des clés. Pour la séparation des tâches, vous pouvez utiliser des politiques basées à la fois sur l'identité et sur les ressources pour contrôler l'accès à la clé. Vous pouvez également configurer la rotation automatique des touches. Les clés gérées par le client entraînent des frais mensuels, et si vous dépassez le niveau gratuit, elles sont également soumises à des

frais d'utilisation. Pour plus d'informations sur ce type de clé, consultez la section Clés gérées par le client (AWS KMS documentation).

Pour plus d'informations sur le stockage et l'utilisation des clés, consultez la section AWS Key Management Service Tarification (AWS marketing).

Types de performances et de chiffrement

Selon le type de chiffrement choisi dans les normes, vous pouvez utiliser deux types de clés KMS.

- Symétrique : tous les AWS KMS key types prennent en charge le chiffrement symétrique. Lorsque vous chiffrez des clés gérées par le client, vous pouvez utiliser une clé à puissance unique pour le chiffrement et le déchiffrement avec l'AES-256-GCM.
- Asymétrique : les clés gérées par le client prennent en charge le chiffrement asymétrique. Vous pouvez choisir entre différents atouts clés et algorithmes, en fonction de l'utilisation que vous souhaitez en faire. Les clés asymétriques peuvent chiffrer et déchiffrer avec RSA et peuvent signer et vérifier les opérations avec RSA ou ECC. Les algorithmes de clé asymétriques permettent par nature de séparer les rôles et de simplifier la gestion des clés. Lorsque vous utilisez le chiffrement asymétrique avec AWS KMS, certaines opérations ne sont pas prises en charge, telles que la rotation des clés et l'importation de clés externes.

Pour plus d'informations sur les AWS KMS opérations prises en charge par les touches symétriques et asymétriques, consultez la section Référence des types de clés (AWS KMS documentation).

Chiffrement d’enveloppe

Le chiffrement des enveloppes est intégré AWS KMS. Dans AWS KMS, vous générez des clés de données au format texte brut ou crypté. Les clés de données chiffrées sont chiffrées à l'aide d'une clé KMS. Vous pouvez stocker la clé KMS dans un magasin de clés personnalisé au sein d'un AWS CloudHSM cluster. Pour plus d'informations sur les avantages du chiffrement des enveloppes, consultezÀ propos du chiffrement des enveloppes.

Emplacement de stockage des clés

Vous utilisez des politiques pour gérer l'accès aux AWS KMS ressources. Les politiques décrivent qui peut accéder à quelles ressources. Les politiques associées à un principal Gestion des identités et des accès AWS (IAM) sont appelées politiques basées sur l'identité ou politiques IAM. Les politiques associées à d'autres types de ressources sont appelées politiques de ressources. AWS KMS les

politiques de ressources pour AWS KMS keys sont appelées politiques clés. Chaque clé KMS est associée à une politique clé.

Les politiques clés offrent la flexibilité de stocker la clé de chiffrement dans un emplacement central ou de la stocker plus près des données, de manière distribuée. Tenez compte AWS KMS des fonctionnalités suivantes lorsque vous décidez où stocker les clés KMS dans votre Compte AWS :

- Support de l'infrastructure à région unique : par défaut, les clés KMS sont spécifiques à une région et ne sont jamais déchiffrées. AWS KMS Si vos normes imposent des exigences strictes en matière de contrôle des clés dans une zone géographique spécifique, envisagez d'utiliser des clés à région unique.
- Support d'infrastructure multirégional : prend AWS KMS également en charge un type de clé à usage spécial appelé clés multirégionales. Le stockage de données multiples Régions AWS est une configuration courante pour la reprise après sinistre. En utilisant des clés multirégionales, vous pouvez transférer des données entre les régions sans les rechiffrer, et vous pouvez gérer les données comme si vous disposiez de la même clé dans chaque région. Cette fonctionnalité est très utile si vos normes exigent que votre infrastructure de chiffrement couvre plusieurs régions dans une configuration active-active. Pour plus d'informations, consultez la section Clés multirégionales (AWS KMS documentation).
- Gestion centralisée — Si vos normes exigent que vous stockiez les clés dans un emplacement centralisé, vous pouvez AWS KMS stocker toutes vos clés de chiffrement en un seul endroit Compte AWS. Vous utilisez des politiques clés pour accorder l'accès à d'autres applications, qui peuvent se trouver dans différents comptes dans la même région. La gestion centralisée des clés peut réduire les frais administratifs liés à la gestion du cycle de vie des clés et au contrôle de l'accès aux clés.
- Matériel clé externe — Vous pouvez importer du matériel clé généré en externe dans AWS KMS. Support pour cette fonctionnalité est disponible pour les clés symétriques à une ou plusieurs régions. Le matériau de la clé symétrique étant généré en externe, vous êtes responsable de la protection des matériaux clés générés. Pour plus d'informations, consultez la section Matériel clé importé (AWS KMS documentation).

Contrôle d’accès

Dans AWS KMS, vous pouvez implémenter un contrôle d'accès de niveau granulaire à l'aide des mécanismes de politique suivants : politiques clés, politiquesIAM et autorisations. À l'aide de ces contrôles, vous pouvez définir votre séparation des tâches en fonction des rôles, tels que les

administrateurs, les utilisateurs clés qui peuvent chiffrer les données, les utilisateurs clés qui peuvent déchiffrer les données et les utilisateurs clés qui peuvent à la fois chiffrer et déchiffrer les données. Pour plus d'informations, consultez Authentification et contrôle d'accès (AWS KMS documentation).

Audit et journalisation

AWS KMS s'intègre à Amazon AWS CloudTrail et à EventBridge des fins de journalisation et de surveillance. Toutes les opérations d' AWS KMS API sont enregistrées et auditables dans CloudTrail des journaux. Vous pouvez utiliser Amazon CloudWatch et configurer EventBridge des solutions AWS Lambda de surveillance personnalisées afin de configurer les notifications et la correction automatique. Pour plus d'informations, consultez la section Journalisation et surveillance (AWS KMS documentation).

FAQ

Cette section fournit des réponses aux questions fréquemment posées lors de la définition de vos normes de chiffrement ou lors de la création de votre infrastructure de chiffrement lors de la phase de mise en œuvre.

Quand ai-je besoin d'un chiffrement symétrique ?

Vous pouvez utiliser le chiffrement symétrique dans les cas suivants :

- La rapidité, le coût et la réduction des frais de calcul sont une priorité.
- Vous devez chiffrer une grande quantité de données.
- Les données chiffrées ne quittent pas les limites du réseau de l'entreprise.

Quand ai-je besoin d'un chiffrement asymétrique ?

Vous pouvez utiliser le chiffrement asymétrique dans les cas suivants :

- Vous devez partager les données en dehors de l'organisation.
- Les réglementations ou la gouvernance interdisent le partage de la clé.
- La non-répudiation est requise. (La non-répudiation empêche un utilisateur de nier des engagements ou des actions antérieurs.)
- Vous devez séparer strictement l'accès aux clés de chiffrement en fonction des rôles de l'organisation.

Quand ai-je besoin du chiffrement des enveloppes ?

Vous devez prendre en charge et implémenter le chiffrement des enveloppes si votre politique de chiffrement nécessite une rotation des clés. Certains régimes de gouvernance et de conformité nécessitent une rotation des clés, ou votre politique peut l'obliger à répondre à un besoin commercial.

Quand dois-je utiliser un module de sécurité matériel (HSM) ?

Vous pourriez avoir besoin d'un HSM si votre politique précise la conformité avec :

- La norme de cryptage FIPS (Federal Information Processing Standards) 140-2 de niveau 3. Pour plus d'informations, voir Validation FIPS (AWS CloudHSM documentation).
- Normes du secteur APIs, telles que PKCS #11, Java Cryptography Extension (JCE) ou Microsoft Cryptography API : Next Generation (CNG)

Pourquoi devrais-je gérer les clés de chiffrement de manière centralisée ?

Les avantages courants de la gestion centralisée des clés sont les suivants :

- Les clés étant utilisées et administrées à différents endroits, vous pouvez les réutiliser, ce qui permet de réduire les coûts.
- Vous avez un meilleur contrôle sur l'accès aux clés de chiffrement.
- Le stockage des clés au même endroit facilite la visualisation, l'audit et la mise à jour des clés en cas de modification des normes.

Dois-je utiliser une infrastructure de chiffrement spécialement conçue pour les données au repos ?

Votre entreprise a besoin d'une infrastructure de chiffrement si l'une des conditions suivantes est vraie :

- Votre entreprise gère et stocke les données de toute classification autre que publique.
- Votre entreprise capture et stocke des données sur les employés ou les clients.
- Votre entreprise gère les données d'identification personnelle.
- Votre entreprise doit se conformer aux régimes réglementaires ou de gouvernance qui exigent le chiffrement des données.
- La direction de votre entreprise a imposé le chiffrement de toutes les données inactives.

Comment puis-je AWS KMS aider mon entreprise à atteindre ses objectifs de chiffrement pour les données au repos ?

En plus de nombreuses autres fonctionnalités, AWS Key Management Service peut vous aider à :

- Utilisez le chiffrement des enveloppes.
- Contrôlez l'accès aux clés de chiffrement, par exemple en séparant l'administration des clés de leur utilisation.
- Partagez les clés entre plusieurs Régions AWS et Comptes AWS.
- Centralisez l'administration des clés.
- Automatisez et prescrivez la rotation des clés.

Ressources

Service AWS documentation

- AWS KMS Détails cryptographiques
- Guide du développeur AWS KMS
  - Concepts de AWS KMS
  - Clés spéciales
  - Authentification et contrôle d'accès pour AWS KMS
  - Sécurité de AWS KMS
  - Comment Services AWS utiliser AWS KMS
- AWS CloudHSM Guide de l'utilisateur

AWS commercialisation

- AWS KMS tarification
- AWS KMS intégration avec d'autres Services AWS

AWS Framework Well-Architected

- Protection des données en transit
- Protection des données au repos

Hachage et tokenisation

- Comment utiliser la tokenisation pour améliorer la sécurité des données et réduire la portée des audits (AWS article de blog)
- Recommandation pour les applications utilisant des algorithmes de hachage approuvés (publication du NIST)

Vidéos

- Comment fonctionne le chiffrement dans AWS
- Sécurisation de votre stockage par blocs sur AWS
- Atteindre les objectifs de sécurité avec AWS CloudHSM
- Meilleures pratiques pour la mise en œuvre AWS Key Management Service
- Une analyse approfondie des services AWS de chiffrement

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	—	15 septembre 2022

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Oracle sur une instance EC2 dans le. AWS Cloud
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application 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 les bases de données source et cible sont synchronisées, mais seule la base de données source gère les transactions liées à la connexion des 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 Gestion des identités et des accès AWS (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

Consultez la base de données de gestion des configurations.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub 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 est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du 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 Gestion des identités et des accès AWS (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 CI/CD pipeline, 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 CSPM 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

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, 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 lorsqu'il fonctionne. 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 AWS avec le service de migration 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

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. 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 peuvent accéder au contenu d'un compartiment S3 uniquement via une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

ORR

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

DE

Voir technologie opérationnelle.

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.

policy

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.

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 AWS capable d'effectuer des actions et d'accéder aux 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).

RAG

Voir Retrieval Augmented Generation.

rançongiciel

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

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 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 en matière de temps de rétablissement.

runbook

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

S

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 en matière AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une instance Amazon EC2 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, voir 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

tags

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.