Guide journalisation et surveillance pour les propriétaires d'applications

AWS Directives prescriptives

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Directives prescriptives: Guide journalisation et surveillance pour les propriétaires d'applications

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Guide journalisation et surveillance pour les propriétaires d'applications

John Buckley, Amazon Web Services (AWS)

Janvier 2023 (historique du document)

Une charge de travail est un ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend. Une charge de travail peut consister en un sous-ensemble de ressources réunies dans une seul Compte AWS, ou elle peut s'étendre sur plusieurs Comptes AWS. Dans le cloud, une application est un type de charge de travail. Elle peut être déployée exclusivement dans l'environnement cloud, ou également être prise en charge par du matériel local sur site. De nombreuses publications se concentrent sur la journalisation et la surveillance de l'infrastructure cloud et sont destinées aux équipes de sécurité. Ce guide est destiné aux propriétaires d'applications et met l'accent sur les approches efficaces et efficientes de la journalisation et de la surveillance des applications dans le AWS Cloud.

Ce guide vous aide à configurer la journalisation et la surveillance à un niveau approprié afin que vous puissiez identifier les anomalies et y répondre rapidement. Cela vous permet également de vous assurer que les journaux de vos applications prennent en charge une analyse détaillée et la résolution de tout problème.

Bien que ce guide soit écrit en tenant compte des déploiements du AWS Cloud, vous pouvez appliquer ces principes aux applications exécutées sur site ou sur l'infrastructure d'un autre fournisseur cloud.

Résultats commerciaux ciblés

Après avoir lu ce guide, vous devriez être en mesure de comprendre les points suivants :

- Les types d'événements couramment journalisés pour les applications
- Les attributs des événements (tels que qui, quoi et quand) que vous devriez envisager de journaliser
- Les types de données que vous devriez envisager d'exclure des journaux, comme les données susceptibles de compromettre votre sécurité ou les données d'identification personnelle
- Comment configurer la journalisation et la surveillance au niveau approprié pour votre application

- Qui devrait être en mesure de gérer les journaux de vos applications et d'y accéder
- Les Services AWS et les fonctionnalités que vous pouvez configurer pour surveiller et journaliser vos applications dans le AWS Cloud
- Comment utiliser les données de journaux de votre application, ainsi que les Services AWS et les fonctionnalités permettant de trier et de diagnostiquer les problèmes

À propos de la journalisation et de la surveillance des applications

La journalisation, la surveillance, les alertes et les rapports sont des processus de sécurité différents qui fonctionnent de concert pour assurer une visibilité sur l'état et les performances de votre application. Il est essentiel que vous créiez et teniez à jour un enregistrement détaillé des actions et des événements de votre application afin de pouvoir surveiller, alerter et établir des rapports en fonction de l'activité enregistrée.

La journalisation des applications est le processus qui consiste à collecter les événements générés par votre application et à les enregistrer dans un ou plusieurs fichiers journaux. Cet historique des événements peut vous aider à effectuer des analyses de sécurité et des performances, à suivre l'évolution des ressources et à résoudre les problèmes liés aux applications.

La surveillance des applications est le processus d'évaluation des performances globales et de l'état de votre application. Vous devriez être en mesure de surveiller le frontend et le backend de l'application en permanence. Les applications hébergées dans le cloud étant hautement distribuées, les outils de journalisation et de surveillance peuvent vous aider à résoudre rapidement les problèmes de performance ou à identifier et corriger les menaces de sécurité en temps réel. Les données du journal constituent une entrée essentielle pour la surveillance.

L'observabilité est similaire à la surveillance, mais elle introduit des moyens de mesurer le comportement des applications à l'aide de différents paramètres et permet d'établir des corrélations complexes. La mesure du taux de réussite HTTP un jour donné, pour un ensemble d'utilisateurs dans une région géographique spécifique, est un exemple. Pour plus d'informations, veuillez consulter Surveillance et observabilité (marketing AWS).

En fin de compte, l'objectif des propriétaires d'applications est de faire en sorte que les applications restent sécurisées et saines, mais aussi que les expériences utilisateur avec ces applications restent positives. En implémentant la journalisation et la surveillance, vos développeurs et vos équipes opérationnelles peuvent planifier et résoudre plus rapidement les problèmes liés aux applications.

Le niveau de journalisation et de surveillance requis varie pour chaque application. Les facteurs susceptibles d'affecter les niveaux de surveillance et de journalisation incluent les stratégies et procédures organisationnelles, le niveau de risque de sécurité que représente l'application, son importance pour les opérations métier et la sensibilité des données gérées par l'application. En général, les applications publiques ou destinées aux clients nécessitent un niveau de surveillance

et de journalisation plus élevé que les applications utilisées en interne dans l'organisation. Ce guide contient des informations et des recommandations générales. Vous devez donc personnaliser votre approche en fonction des exigences de votre application.

> **Note**
>
> Les normes ou procédures de votre organisation peuvent imposer des attributs de journalisation et de surveillance spécifiques. Le transfert des autorisations des utilisateurs à un système d'examen des droits d'entreprise en est un exemple. Assurez-vous que votre plan de journalisation et de surveillance répond aux exigences de votre organisation.

Journalisation d'applications dans le AWS Cloud

Pour la journalisation d'applications dans le AWS Cloud, examinez les types d'événement courants, les attributs des événements et les bonnes pratiques.

Cette section comprend les rubriques suivantes:

Types d'événements

L'une des considérations les plus importantes à prendre en compte lors de l'établissement d'une stratégie de journalisation des applications est de décider des événements et des actions à journaliser. Bien que les exigences de votre organisation et de votre application puissent influencer cette décision, nous vous recommandons de toujours journaliser les informations suivantes si elles s'appliquent à votre application :

- Échecs de validation des entrées : les exemples incluent les violations de protocole, les codages inacceptables, ainsi que les noms et valeurs de paramètres non valides.
- Échecs de validation des sorties : les exemples incluent les incohérences entre les ensembles d'enregistrements de base de données et le codage de données non valides.
- Succès et échecs de l'authentification d'identité : journalisez les activités d'authentification, mais pas les noms d'utilisateur et les mots de passe. Étant donné que les utilisateurs peuvent saisir accidentellement leur mot de passe dans un champ de nom d'utilisateur, nous vous recommandons de ne pas enregistrer les noms d'utilisateur. Cela peut exposer involontairement les informations d'identification et donner lieu à un accès autorisé. Implémentez des contrôles de sécurité pour tous les journaux contenant des données d'authentification.
- Échecs d'autorisation (contrôle d'accès) : pour les systèmes d'autorisation associés, journalisez les tentatives d'accès infructueuses. Vous pouvez surveiller les données de ce journal pour détecter des modèles susceptibles d'indiquer une attaque ou des problèmes liés au système d'autorisation dans l'application.
- Échecs de gestion de session : les exemples incluent la modification des cookies ou des jetons de session. Les applications utilisent souvent des cookies ou des jetons pour gérer les états des

utilisateurs. Les utilisateurs malveillants peuvent essayer de modifier les valeurs des cookies pour obtenir un accès non autorisé. La journalisation des jetons de session falsifiés permet de détecter ce comportement.

- Erreurs d'application et événements du système : à titre d'exemple, citons les erreurs de syntaxe et d'exécution, les problèmes de connectivité, les problèmes de performance, les messages d'erreur provenant de services tiers, les erreurs de système de fichiers, la détection de virus lors des chargements de fichiers et les modifications de la configuration.
- État de l'application : démarrage ou arrêt de l'application et de ses ressources associées.
- État de la journalisation : démarrage, arrêt ou pause de la journalisation.
- Utilisation de fonctionnalités présentant un risque accru : à titre d'exemple, citons les modifications de la connexion réseau, l'ajout ou la suppression d'utilisateurs, la modification des privilèges, l'attribution d'utilisateurs à des jetons, l'ajout ou la suppression de jetons, l'utilisation de privilèges administratifs système, l'accès par les administrateurs d'applications, toutes les actions effectuées par des utilisateurs dotés de privilèges administratifs, l'accès aux données des titulaires de cartes de paiement, l'utilisation de clés de chiffrement des données, la modification de clés de chiffrement, la création et la suppression d'objets au niveau du système, la soumission de contenu généré par les utilisateurs (en particulier les chargements de fichiers), ainsi que l'importation et l'exportation de données (y compris les rapports).
- Abonnements légaux et autres : à titre d'exemple, citons les autorisations relatives aux fonctionnalités des téléphones portables, les conditions d'utilisation, les conditions générales, le consentement à l'utilisation des données personnelles et les autorisations à recevoir des communications marketing.

Outre les attributs recommandés, pour votre application, déterminez quels attributs supplémentaires peuvent fournir des données utiles pour la surveillance, les alertes et la génération de rapports. En voici quelques exemples :

- Défaillances du séquençage
- Attributs qui vous aident à évaluer le comportement des utilisateurs qui enfreignent la stratégie d'utilisation acceptable de votre organisation.
- Modifications des données
- Attributs requis pour se conformer aux normes ou aux réglementations, tels que la prévention des crimes financiers, la limitation des transactions sur actions ou la collecte d'informations médicales ou d'autres informations personnelles.

- Attributs qui vous aident à identifier les comportements suspects ou inattendus, tels que les tentatives d'exécution d'actions non autorisées.
- Configuration changes
- Modifications du fichier de code de l'application ou de la mémoire

Attributs d'événement

Chaque entrée de journal doit inclure des informations suffisamment détaillées pour le suivi et l'analyse. Vous pouvez journaliser des données de contenu complètes, mais il est plus efficace de journaliser un extrait ou des propriétés récapitulatives. Les journaux d'application doivent enregistrer les facteurs quand, où, qui, quoi et quel/quelle de chaque événement. Leurs propriétés seront différentes en fonction de l'architecture, de la classe d'application et du système ou périphérique hôte.

Lorsque vous journalisez des horodatages, utilisez le temps universel coordonné (UTC) et les formats de date et d'heure internationalement reconnus de la norme ISO 8601 (site Web de l'ISO).

> **Note**
>
> Envisagez d'utiliser un service de synchronisation de l'heure réseau pour garantir l'exactitude des horodatages. Amazon propose le Service de synchronisation temporelle d'Amazon, qui est utilisé par de nombreux Services AWS, notamment Amazon Elastic Compute Cloud (Amazon EC2). Le Service de synchronisation temporelle d'Amazon utilise une flotte d'horloges de référence atomiques et connectées à des satellites, dans chaque Région AWS pour fournir des mesures temporelles précises selon la norme internationale UTC via le NTP (Network Time Protocol). Pour plus d'informations, veuillez consulter Keeping Time with Amazon Time Sync Service (billet de blog AWS).

Les attributs d'événements suivants sont généralement inclus dans les journaux.

Catégorie d'attribut	Attribut d'événement	Description
Lorsque	Date et heure de journalisation	Enregistrez la date et l'heure auxquelles l'événement a été ajouté au journal.

	Date et heure de l'événement	Enregistrez la date et l'heure auxquelles l'événement s'est produit. Elles peuvent être différentes de l'enregistrement de journalisation, par exemple lorsque la journalisation est retardée parce que l'applica tion cliente est hébergée sur un appareil distant connecté périodiquement ou par intermittence.
	Identifiant de l'événement	Journalisez un nom d'utilisa teur, un numéro de compte ou un autre attribut unique garantissant que l'événement peut toujours être identifié.
Où	Identifiant de l'application	Journalisez le nom et la version de l'application.
	Adresse de l'application	Journalisez le cluster ou le nom d'hôte, l'adresse IPv4 ou IPv6 du serveur, le numéro de port, l'identité du poste de travail et l'identifiant du périphérique local.
	Service	Journalisez le nom du service et le protocole.
	Géolocalisation	Journalisez les emplacements géographiques de l'utilisateur.

	Fenêtre, formulaire ou page	Journalisez l'URL du point d'entrée, la méthode HTTP d'une application Web ou le nom de la boîte de dialogue dans laquelle l'action a été effectuée.
	Emplacement du code	Journalisez le nom du script ou du module.
Qui (utilisateur humain ou machine)	Adresse source	Journalisez l'identifiant de l'appareil, l'adresse IP, l'identifiant de la tour de radiofréquence (RF) ou le numéro de téléphone portable de l'utilisateur.
	Identité de l'utilisateur	Si l'utilisateur est authentifié ou connu, journalisez la valeur de la clé primaire de la table de base de données utilisateur, le nom d'utilisateur ou le numéro de licence.
	Classification des types de données	Journalisez le type d'utilisateur, tel que public, authentifié, CMS, moteur de recherche, testeur de pénétration autorisé ou moniteur de disponibilité. Pour plus d'informations sur les moniteurs de disponibilité, veuillez consulter Précautions et exclusions dans ce guide.

	En-têtes HTTP de requête ou agent utilisateur HTTP	(Applications Web uniquement) Journalisez les informations d'en-tête de requête HTTP, y compris la chaîne agent-utilisateur HTTP, car ces valeurs affectent les informations que le client envoie au serveur.
Quoi	Type d'événement	Journalisez si l'événement est informatif, s'il s'agit d'un avertissement ou d'une erreur.
	Gravité de l'événement	Classez la gravité de l'événement, par exemple élevée, moyenne ou faible.
	Indicateur d'événement de sécurité	Si le journal contient des données non liées à des événements de sécurité, créez un indicateur pour les événements liés à la sécurité afin de vous aider à les identifier.
	Description de l'événement	(Facultatif) Incluez une brève description de l'événement.
	Action ou intention	Journalisez l'objectif initial de la demande, tel que la connexion, l'actualisation de l'ID de session, la déconnexion ou la mise à jour d'un profil.

Réponse de l'utilisateur ou de l'application	Journalisez la réponse de l'utilisateur ou de l'application à l'événement, telle qu'un code d'état, des messages textuels personnalisés, l'arrêt de la session ou des alertes de l'administrateur.
État du résultat	Journalisez la réussite éventuelle de l'action, par exemple réussite, échec ou reportée.
Motif du résultat	Journalisez le motif pour lequel l'état s'est présenté. Par exemple, une demande de connexion peut échouer, car l'utilisateur n'est pas authentifié dans la base de données.
Détails étendus	Journalisez toutes les informations supplémentaires associées à l'événement, telles qu'une trace de pile, des messages d'erreur système, des informations de débogage et le corps de la requête HTTP.
Code d'état de la réponse HTTP	(Applications Web uniquement) Journalisez le code d'état de la réponse HTTP renvoyé à l'utilisateur, tel que `200` ou `301`. Pour plus d'informations, consultez Niveaux de journalisation dans ce guide.

Quel/Quelle	Ressources touchées	Journalisez les ressources qui ont été utilisées.
	Objet	Journalisez les composants ou autres objets concernés, tels qu'un compte utilisateur, une ressource de données, un fichier, une URL ou un ID de session.
	Nom de la ressource	Journalisez les noms des ressources concernées.
	Étiquettes de ressources	Journalisez les balises attribuées aux ressource s concernées. Pour plus d'informations sur les balises, veuillez consulter Tagging AWS resources dans la Référence générale AWS.
Autre	Confiance analytique	Journalisez la confiance du service de journalisation dans la détection des événement s, par exemple l'attribution d'une note faible, moyenne ou élevée ou une valeur numérique.
	Classifications internes	Journalisez toutes les classific ations internes pour vérifier le respect des normes ou de la conformité.

Classifications externes	Journalisez toutes les classifications externes pour vérifier le respect des normes ou de la conformité, telles que le protocole SCAP (Security Content Automation Protocol) du NIST.

Journalisation des bonnes pratiques

Niveaux de journalisation

Veillez à ne pas journaliser une quantité excessive de données. Les journaux doivent recueillir des données utiles et exploitables. Une journalisation excessive peut avoir un impact négatif sur les performances et peut également augmenter les coûts de stockage et de traitement de la journalisation. Une journalisation excessive peut également avoir pour conséquence que des problèmes et des événements de sécurité ne soient pas détectés.

La journalisation des codes d'état de réponse HTTP peut générer une quantité importante de données de journal, en particulier des codes d'état de niveau 200 (réussite) et de niveau 300 (redirection). Nous vous recommandons de ne journaliser que les codes d'état de niveau 400 (erreurs côté client) et 500 (erreurs côté serveur).

Les cadres de journalisation des applications fournissent différents niveaux de journalisation, tels que info, débogage ou erreur. Pour les environnements de développement, vous pouvez utiliser une journalisation détaillée, par exemple en incluant info et débogage, afin d'aider vos développeurs. Nous vous recommandons toutefois de désactiver les niveaux info et débogage pour les environnements de production, car ceux-ci peuvent générer des données de journalisation excessives.

Précautions et exclusions

- Assurez-vous que les données que vous journalisez sont autorisées par la loi, en particulier dans les juridictions où votre organisation exerce ses activités.
- N'excluez aucun événement provenant d'utilisateurs connus (tels que d'autres systèmes internes), de tiers de confiance, de robots de moteurs de recherche, de contrôleurs de disponibilité ou de

processus et d'autres systèmes de surveillance à distance. Vous pouvez toutefois inclure un indicateur de classification pour chacune d'entre elles dans les données enregistrées. N'oubliez pas que les fichiers journaux générés par votre application peuvent être utilisés par des parties, telles que des solutions tierces de surveillance des journaux ou des fournisseurs de services externes, qui ne sont pas autorisés à consulter les données sensibles traitées par l'application.

- Les attributs suivants ne doivent pas être enregistrés directement dans les journaux. Supprimez, masquez, nettoyez, hachez ou chiffrez les éléments suivants :
  - Code source de l'application
  - Valeurs d'identification de session (envisagez de les remplacer par une valeur hachée si vous devez suivre des événements propres à la session)
  - Jetons d'accès
  - Des données sensibles et certaines formes de données d'identification personnelle (PII), telles que des données d'identification médicale ou des identifiants émis par le gouvernement
  - Mots de passe d'authentification
  - Chaînes de connexion à la base de données
  - Clés de chiffrement et autres secrets principaux
  - Données du titulaire de compte bancaire ou de carte de paiement
  - Données d'un niveau de sécurité supérieur à celui que le système de journalisation est autorisé à stocker
  - Informations sensibles du point de vue commercial
  - Informations dont la collecte est illégale dans les juridictions concernées
  - Informations dont l'utilisateur a refusé la collecte ou pour lesquelles il n'a pas donné son consentement explicite.
  - Informations dont le consentement à la collecte a expiré

Types de données spéciaux

Parfois, les données suivantes peuvent également être enregistrées dans des journaux. Bien que cela puisse être utile à des fins d'investigation et de dépannage, elles peuvent révéler des informations sensibles sur le système. Vous devrez peut-être anonymiser, hacher ou chiffrer ces types de données avant que l'événement ne soit enregistré :

- Chemins de fichier

- Noms et adresses des réseaux internes
- Données personnelles non sensibles, telles que les noms personnels, les numéros de téléphone et les adresses e-mail

Utilisez l'anonymisation des données si l'identité réelle de la personne n'est pas requise dans le journal ou si le risque est jugé comme trop important.

Gestion des accès et des modifications

- Les utilisateurs non-administrateurs ne devraient pas être en mesure de désactiver la journalisation des événements, en particulier ceux qui sont nécessaires pour répondre aux exigences de conformité.
- Seuls les utilisateurs administratifs devraient être en mesure de suspendre ou d'arrêter les services de journalisation ou de modifier les configurations.
- Si votre service de journalisation dispose d'une fonctionnalité de validation de l'intégrité des fichiers journaux, activez-la. Cela vous permet de détecter les modifications, les suppressions ou les falsifications de fichiers journaux. Pour plus d'informations sur cette fonctionnalité dans Services AWS, veuillez consulter Utiliser CloudTrail dans ce guide.
- Les modifications de journalisation doivent être intrinsèques à l'application, par exemple effectuées automatiquement par l'application sur la base d'un algorithme approuvé, ou suivre un processus de gestion des modifications approuvé, par exemple lorsque vous modifiez les données de configuration ou le code source.

Services AWS pour la journalisation et la surveillance

Ce guide porte sur les applications de journalisation et de surveillance déployées dans le AWS Cloud. Vous pouvez utiliser les Services AWS pour implémenter votre plan de journalisation et de surveillance, ou pour améliorer vos solutions actuelles. Par exemple, si vous résolvez un problème lié à votre application, vous pouvez effectuer les opérations suivantes :

- Trier les journaux d'applications à l'aide de la fonctionnalité Journaux de flux VPC d'Amazon Virtual Private Cloud (Amazon VPC) et consulter le trafic réseau correspondant au problème.
- Utiliser AWS CloudTrail pour afficher les appels d'API correspondant aux heures de survenue du problème.
- Consulter les journaux d'Amazon CloudWatch Logs pour vérifier les pics du processeur correspondant aux heures de survenue du problème.

Vous pouvez déployer les Services AWS et les fonctionnalités de journalisation et de surveillance de votre application ci-dessous :

- AWS CloudTrail vous aide à vérifier la gouvernance, la conformité et le risque opérationnel de votre Compte AWS en enregistrant les actions entreprises par un utilisateur, un rôle ou un Service AWS. Pour plus d'informations sur l'utilisation de ce service pour journaliser ou surveiller des événements pour votre application, consultez CloudTrail dans ce guide.
- Amazon CloudWatch vous aide à analyser les journaux et à surveiller en temps réel les métriques de vos ressources AWS et applications hébergées. Vous pouvez également utiliser la fonctionnalité ServiceLens pour surveiller l'état de votre application ou utiliser la fonction Synthetics pour créer des scripts canary qui surveillent vos points de terminaison et vos API. Pour plus d'informations sur l'utilisation de ce service pour surveiller votre application, consultez CloudWatch dans ce guide.
- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes, applications et Services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité. Pour plus d'informations sur l'utilisation de ce service pour journaliser des événements pour votre application, consultez CloudWatch Logs dans ce guide.
- La fonctionnalité Journaux de flux VPC d'Amazon Virtual Private Cloud (Amazon VPC) capture des informations sur le trafic IP circulant vers et depuis les interfaces réseau de votre VPC. Pour plus d'informations sur l'utilisation de ce service pour journaliser des événements pour votre application, consultez Journaux de flux VPC dans ce guide.

- AWS X-Ray collecte des données sur des demandes servies par votre application, et vous aide à afficher, filtrer et avoir un aperçu de ces données afin d'identifier les problèmes et les occasions d'optimiser votre application. Pour plus d'informations sur l'utilisation de ce service pour surveiller votre application, consultez X-Ray dans ce guide.

Journalisation et surveillance des applications à l'aide d'AWS CloudTrail

AWS CloudTrail est un Service AWS qui vous aide à assurer la gouvernance, la conformité, ainsi que l'audit opérationnel et des risques de votre Compte AWS. Les actions effectuées par un utilisateur, un rôle ou un Service AWS sont enregistrées en tant qu'événements dans CloudTrail. Les événements peuvent inclure les actions réalisées dans l'AWS Management Console, l'AWS Command Line Interface (AWS CLI), les API et les kits SDK AWS.

Utiliser CloudTrail

CloudTrail est activé sur votre Compte AWS lors de la création de celui-ci. Lorsqu'une activité se produit dans votre Compte AWS, elle est enregistrée dans un événement CloudTrail. Vous pouvez facilement afficher des événements récents dans la console CloudTrail en accédant à l'historique des événements.

Pour un enregistrement continu des activités et des événements dans votre Compte AWS, vous créez un journal de suivi. Vous pouvez créer des journaux de suivi pour une Région AWS ou pour toutes les régions. Les journaux d'activité permettent de journaliser les fichiers journaux dans chaque région, tandis que CloudTrail peut livrer les fichiers journaux à un compartiment Amazon Simple Storage Service (Amazon S3) consolidé.

Vous pouvez configurer plusieurs journaux de suivi différemment pour que ceux-ci traitent et journalisent uniquement les événements que vous spécifiez. Cela peut être utile lorsque vous souhaitez trier les événements qui se produisent dans votre Compte AWS avec les événements qui se produisent dans votre application.

> **Note**
>
> CloudTrail dispose d'une fonctionnalité de validation que vous pouvez utiliser pour déterminer si un fichier journal a été modifié, supprimé ou inchangé après que CloudTrail l'a livré. Cette fonction est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage

et SHA-256 avec RSA pour la signature numérique. Elle empêche de modifier, supprimer ou falsifier des fichiers journaux CloudTrail par traitement informatique sans détection. Vous pouvez utiliser la AWS CLI pour valider les fichiers à l'emplacement où CloudTrail les a livrés. Pour plus d'informations sur cette fonctionnalité et sur la façon de l'activer, veuillez consulter Validating CloudTrail log file integrity (documentation CloudTrail).

Cas d'utilisation pour CloudTrail

- Aide à la conformité : l'utilisation de CloudTrail peut vous aider à respecter les stratégies internes et les normes réglementaires en fournissant un historique des événements survenus dans votre Compte AWS.
- Analyse de sécurité : vous pouvez effectuer une analyse de sécurité et détecter les modèles de comportement des utilisateurs en intégrant les fichiers journaux CloudTrail dans des solutions de gestion des journaux et analytiques, telles que CloudWatch Logs, Amazon EventBridge, Amazon Athena, Amazon OpenSearch Service ou une autre solution tierce.
- Exfiltration de données : vous pouvez détecter l'exfiltration de données en collectant des données d'activité sur les objets Amazon S3 par le biais d'événements d'API au niveau de l'objet enregistrés dans CloudTrail. Une fois les données d'activité collectées, vous pouvez utiliser d'autres Services AWS, tels qu'EventBridge et AWS Lambda, pour déclencher une réponse automatique.
- Résolution des problèmes opérationnels : vous pouvez résoudre les problèmes opérationnels à l'aide des fichiers journaux CloudTrail. Par exemple, vous pouvez rapidement identifier les modifications les plus récentes apportées aux ressources de votre environnement, notamment la création, la modification et la suppression de ressources AWS.

Bonnes pratiques pour CloudTrail

- Activez CloudTrail dans toutes les Régions AWS.
- Activez la validation de l'intégrité des fichiers journaux.
- Chiffrez les journaux.
- Intégrez les fichiers journaux CloudTrail dans CloudWatch Logs.
- Centralisez les journaux de tous les Comptes AWS et de toutes les régions.
- Appliquez des stratégies de cycle de vie aux compartiments S3 contenant des fichiers journaux.

- Empêchez les utilisateurs de désactiver la journalisation dans CloudTrail. Appliquez les politiques de contrôle des services (SCP) suivantes dans AWS Organizations. Cette SCP définit une règle de refus explicite pour les actions `StopLogging` et `DeleteTrail` au sein de l'organisation.

```
{
"Version": "2012-10-17",
"Statement":
       [
                 { "Action":
                     [
                     "cloudtrail:StopLogging",
                     "cloudtrail:DeleteTrail"
                      ],
                      "Resource": "*",
                      "Effect": "Deny"
                  }
        ]
}
```

Journalisation et surveillance des applications à l'aide d'Amazon CloudWatch

Amazon CloudWatch contrôle vos ressources AWS et les applications que vous exécutez sur AWS en temps réel. Vous pouvez utiliser CloudWatch pour recueillir et suivre les métriques, qui sont des variables que vous pouvez mesurer pour vos ressources et applications.

Utilisation de CloudWatch

CloudWatch est essentiellement un référentiel de métriques. Un Service AWS, tel qu'Amazon EC2, place des métriques dans ce référentiel ; vous récupérez ensuite les statistiques basées sur ces métriques. Si vous mettez vos propres métriques personnalisées dans le référentiel, vous pouvez extraire des statistiques sur ces métriques. Pour plus d'informations, veuillez consulter Using CloudWatch metrics (documentation CloudWatch).

Vous pouvez également configurer des alarmes qui permettent de lancer des actions automatiquement en votre nom. Une alerte surveille une métrique unique sur une période de temps définie et exécute une ou plusieurs actions spécifiées en fonction de la valeur de la métrique par rapport à un seuil sur la période. Par exemple, l'alarme pourrait envoyer une notification à une

rubrique Amazon Simple Notification Service (Amazon SNS). Vous pouvez également ajouter des alertes aux tableaux de bord. Pour plus d'informations, veuillez consulter Using CloudWatch alarms (documentation CloudWatch).

La console CloudWatch affiche automatiquement les métriques relatives à chaque Service AWS que vous utilisez. Vous pouvez créer d'autres tableaux de bord personnalisés afin d'afficher les métriques et les alarmes pour vos applications. Pour plus d'informations, veuillez consulter Using CloudWatch dashboards (documentation CloudWatch).

Dans CloudWatch, les fonctionnalités interrégionales sont automatiquement prises en charge. Vous n'avez pas besoin d'effectuer d'étapes supplémentaires pour afficher les métriques de différentes Régions AWS dans un seul compte sur le même graphique ou le même tableau de bord. Vous pouvez bénéficier des fonctionnalités à comptes multiples en implémentant l'observabilité entre comptes (documentation CloudWatch).

Pour plus d'informations et des conseils détaillés sur l'utilisation de CloudWatch afin de journaliser et de surveiller les charges de travail dans le AWS Cloud, veuillez consulter Designing and implementing logging and monitoring with Amazon CloudWatch (Recommandations AWS).

Cas d'utilisation pour CloudWatch

- Surveillance de l'état de l'application : CloudWatch ServiceLens améliore l'observabilité de vos services et applications en vous permettant d'intégrer des suivis, des métriques, des journaux, des alertes et d'autres informations sur l'état des ressources en un seul endroit. ServiceLens intègre CloudWatch à AWS X-Ray pour fournir une vue de bout en bout de votre application afin de vous aider à identifier plus efficacement les goulots d'étranglement des performances Pinpoint et à identifier les utilisateurs concernés. Pour plus d'informations, veuillez consulter Utilisation de ServiceLens pour surveiller l'état de vos applications (documentation CloudWatch).
- Surveillance Synthetics : vous pouvez utiliser CloudWatch Synthetics pour créer des scripts Canary configurables qui s'exécutent selon une planification pour contrôler vos points de terminaison et vos API. Les scripts Canary suivent les mêmes chemins et effectuent les mêmes actions qu'un client, ce qui vous permet de vérifier continuellement l'expérience de votre client, y compris en l'absence de trafic de clients sur vos applications. Les scripts Canary vérifient la disponibilité et la latence de vos points de terminaison, et peuvent stocker des données de temps de chargement et des captures d'écran de l'interface utilisateur. Ils surveillent vos API REST, vos URL et le contenu de votre site Web, et peuvent vérifier les modifications non autorisées apportées par des opérations de hameçonnage, l'injection de code et le scripting intersites. Pour plus d'informations, veuillez consulter Utilisation de la surveillance Synthetics (documentation CloudWatch).

- Surveillance utilisateur : avec CloudWatch RUM, vous pouvez effectuer une surveillance des utilisateurs réels pour collecter et afficher des données côté client sur les performances de votre application Web. Les données incluent les temps de chargement des pages, les erreurs côté client et le comportement des utilisateurs. Vous pouvez utiliser les données collectées pour identifier et déboguer rapidement les problèmes de performance côté client. Pour plus d'informations, veuillez consulter Utilisation de CloudWatch RUM (documentation CloudWatch).
- Détection de comportement anormal : lorsque vous activez la détection d'anomalies pour une métrique, CloudWatch applique des algorithmes statistiques et de machine learning. Ces algorithmes analysent en permanence les métriques des systèmes et des applications pour déterminer les références normales et les anomalies de surface. Pour plus d'informations, veuillez consulter Utilisation de la détection des anomalies CloudWatch (documentation CloudWatch).
- Validation des fonctionnalités et expériences A/B : Amazon CloudWatch Evidently vous permet de valider en toute sécurité les nouvelles fonctionnalités en les proposant à un pourcentage déterminé de vos utilisateurs pendant le déploiement de la fonctionnalité. Vous êtes également en mesure de réaliser des expériences A/B pour prendre des décisions relatives à la conception des fonctions en vous fondant sur des preuves et des données. Pour plus d'informations, veuillez consulter Réalisez des lancements et des expériences A/B à l'aide de CloudWatch Evidently (documentation CloudWatch).

Journalisation et surveillance des applications à l'aide d'Amazon CloudWatch Logs

Amazon CloudWatch Logs vous permet de centraliser les journaux de tous vos systèmes, ainsi que les applications et les Services AWS que vous utilisez au sein d'un seul service hautement évolutif. Vous pouvez ensuite les afficher facilement, y effectuer des recherches de codes d'erreur ou des modèles, les filtrer en fonction de champs spécifiques ou les archiver en toute sécurité pour procéder à une analyse ultérieure. Vous pouvez voir tous vos événements du journal, quelle que soit leur source, comme un flux unique et cohérent d'événements classés par temps. Vous pouvez les interroger et les trier, les regrouper par champs spécifiques, créer des calculs personnalisés et consulter les données des journaux dans des tableaux de bord.

Utilisation de CloudWatch Logs

Dans CloudWatch Logs, les événements du journal sont organisés en flux de journaux et en groupes de journaux. Un flux de journaux est une séquence d'événements de journaux qui partagent la même

source. Plus précisément, un flux de journal est généralement destiné à représenter la séquence des événements provenant de l'instance d'application ou de la ressource sous surveillance. Les groupes de journaux définissent un ou plusieurs flux de journaux qui partagent les mêmes paramètres de conservation, de surveillance et de contrôle d'accès. Chaque flux de journal doit appartenir à au moins un groupe de journaux. Pour plus d'informations, veuillez consulter Utilisation des groupes de journaux et des flux de journaux (documentation CloudWatch Logs).

Vous pouvez utiliser CloudWatch Logs Insights afin de rechercher et d'analyser les données de vos journaux dans Amazon CloudWatch Logs. Vous pouvez exécuter des requêtes pour répondre plus rapidement et plus efficacement aux problèmes opérationnels. Si un problème se produit, vous pouvez utiliser CloudWatch Logs Insights pour identifier les causes potentielles et valider les correctifs déployés. Pour plus d'informations, veuillez consulter Analyse des données de journaux avec CloudWatch Logs Insights (documentation CloudWatch Logs).

Vous pouvez rechercher et filtrer les données du journal entrant dans CloudWatch Logs en créant un ou plusieurs filtres métriques. Les filtres métriques définissent les termes et les modèles à rechercher dans les données du journal lorsqu'elles sont envoyées à CloudWatch Logs. CloudWatch Logs utilise ces filtres de métriques pour transformer les données du journal en métriques numériques CloudWatch que vous pouvez représenter graphiquement ou utiliser pour définir une alarme. Pour plus d'informations, veuillez consulter Création de métriques à partir d'événements du journal à l'aide de filtres (documentation CloudWatch Logs).

Cas d'utilisation pour CloudWatch Logs

- Surveillance des journaux CloudTrail : vous pouvez créer des alarmes dans CloudWatch et recevoir des notifications d'activité d'API particulière saisies par CloudTrail, puis utiliser ces notifications à des fins de dépannage. Pour plus d'informations, veuillez consulter Sending CloudTrail Events to CloudWatch Logs (documentation CloudTrail).
- Journalisation d'appels d'API AWS : si vous disposez d'une solution de surveillance tierce, vous pouvez utiliser CloudWatch Logs pour journaliser des appels d'API AWS. Vous avez configuré le service de surveillance tiers pour évaluer ce journal et les API au niveau de l'application.
- Configuration de la conservation des journaux : par défaut, les journaux dans CloudWatch Logs sont conservés indéfiniment et n'expirent jamais. Vous pouvez ajuster la stratégie de conservation pour chaque groupe de journaux. Elle peut être indéfinie ou comprise entre 10 ans et un jour.
- Archivage et stockage des journaux : vous pouvez utiliser CloudWatch Logs pour stocker les données de vos journaux dans un stockage hautement durable. L'agent CloudWatch Logs envoie

des données de journaux inversées et non inversées dans le service de journalisation. Vous pouvez ensuite accéder aux données brutes des journaux lorsque vous en avez besoin.

Journalisation et surveillance des applications à l'aide des journaux de flux VPC

La fonctionnalité Journaux de flux VPC d'Amazon Virtual Private Cloud (Amazon VPC) vous aide à capturer des informations sur le trafic IP circulant vers et depuis les interfaces réseau de votre VPC.

Utilisation des journaux de flux VPC

Vous pouvez créer un journal de flux pour un cloud privé virtuel (VPC), un sous-réseau ou une interface réseau. Si vous créez un journal de flux pour un sous-réseau ou VPC, chaque interface réseau du sous-réseau ou du VPC est surveillée. Pour plus d'informations, veuillez consulter Utiliser des journaux de flux (documentation Amazon VPC).

Les données de journal de flux pour une interface réseau surveillée sont enregistrées sous forme d'enregistrements de journal de flux. Un enregistrement de journal de flux représente un flux de réseau dans votre VPC. Par défaut, chaque enregistrement capture un flux de trafic IP réseau qui a lieu au cours d'un intervalle d'agrégation. Chaque enregistrement est une chaîne de caractères avec des champs séparés par des espaces. Un enregistrement inclut des valeurs pour les différents composants du flux IP, par exemple la source, la destination et le protocole. Lorsque vous créez un journal de flux, vous pouvez utiliser le format par défaut pour l'enregistrement de journal de flux ou spécifier un format personnalisé. Pour plus d'informations, veuillez consulter Exemples d'enregistrements de journaux de flux (documentation Amazon VPC).

Les journaux de flux ne capturent pas les informations suivantes :

- Le trafic généré par des instances lorsqu'elles contactent le serveur Amazon de système de nom de domaine (DNS). Si vous utilisez votre propre serveur DNS, tout le trafic vers ce dernier est consigné.
- Le trafic généré par une instance Windows pour l'activation de la licence Windows d'Amazon.
- Le trafic depuis et vers `254.169.254` pour les métadonnées de l'instance.
- Le trafic depuis et vers `254.169.123` pour le service de synchronisation temporelle d'Amazon.
- Trafic du protocole de configuration d'hôte dynamique (DHCP).
- Le trafic vers l'adresse IP réservée pour le routeur VPC par défaut.

- Trafic entre une interface réseau de point de terminaison et une interface réseau de Network Load Balancer.

Les données de journal de flux peuvent être publiées dans plusieurs Services AWS, dont Amazon CloudWatch Logs. Après avoir créé un journal de flux, vous pouvez récupérer et consulter les enregistrements du journal de flux dans CloudWatch Logs, dans le groupe de journaux que vous configurez. Pour plus d'informations, veuillez consulter Publier des journaux de flux vers CloudWatch Logs (documentation Amazon VPC).

Les données du journal de flux sont collectées en dehors du chemin d'accès de votre trafic réseau et n'affectent donc pas le débit réseau ou la latence. Vous pouvez créer ou supprimer des journaux de flux sans risque d'impact sur les performances du réseau.

Cas d'utilisation des journaux de flux VPC

- Diagnostiquer les règles de groupe de sécurité trop restrictives
- Surveiller le trafic qui accède à votre instance d'application
- Déterminer le sens du trafic

Journalisation et surveillance des applications à l'aide d'AWS X-Ray

AWS X-Ray collecte des données sur des demandes servies par votre application, et vous aide à afficher, filtrer et avoir un aperçu de ces données afin d'identifier les problèmes et les occasions d'optimiser votre application.

Utilisation de X-Ray

AWS X-Ray reçoit les suivis de votre application et, s'ils sont intégrés à X-Ray, des Services AWS que votre application utilise. X-Ray échantillonne et visualise les demandes sur un graphique des services lorsqu'elles transitent par les composants de votre application. X-Ray génère des identifiants de suivi afin que vous puissiez corréler une demande lorsqu'elle transite par plusieurs composants, ce qui vous permet de visualiser la demande de bout en bout. Vous pouvez encore améliorer cette fonction en incluant des annotations et des métadonnées pour permettre de rechercher et d'identifier de manière unique les caractéristiques d'une demande.

Nous vous recommandons de configurer chaque serveur ou point de terminaison de votre application avec X-Ray. X-Ray est implémenté dans le code de votre application en adressant des appels au service X-Ray. X-Ray fournit également des kits SDK AWS pour plusieurs langues, y compris des clients instrumentés qui envoient automatiquement des données à X-Ray. Les kits SDK X-Ray fournissent des correctifs aux bibliothèques courantes utilisées pour appeler d'autres services (par exemple, HTTP, MySQL, PostgreSQL ou MongoDB).

Pour plus d'informations, veuillez consulter Tracing applications with AWS X-Ray (Recommandations AWS).

Cas d'utilisation pour X-Ray

- Analyse et débogage des applications : les données de suivi peuvent vous aider à déboguer l'application en fournissant une vue de bout en bout de la demande afin que vous puissiez identifier les goulots d'étranglement et résoudre les problèmes. La cartographie des services X-Ray est un outil visuel qui vous aide à identifier les endroits où se produisent les erreurs, les connexions ayant une latence élevée ou les suivis de demandes ayant échoué.
- Analytique de performances : la console Analytics est un outil interactif pour l'interprétation des données de suivi. Elle permet de comprendre rapidement les performances de votre application et de ses services sous-jacents. La console vous permet d'explorer, d'analyser et de visualiser les suivis. Vous pouvez également comparer des ensembles de suivis présentant différentes conditions, à des fins d'analyse des causes premières.

Questions fréquentes (FAQ)

Puis-je utiliser mon service de surveillance actuel ?

Amazon CloudWatch est un service de surveillance et d'observabilité conçu pour les ingénieurs DevOps, les développeurs, les ingénieurs de fiabilité des sites (SRE), les responsables informatiques et les propriétaires d'applications. Il met à votre disposition des données et des informations exploitables pour vous aider à surveiller vos applications, à répondre aux variations de performances systémiques et à optimiser l'utilisation des ressources. Toutefois, si vous disposez d'un service de surveillance établi, vous n'avez pas besoin de le remplacer.

Comment empêcher la falsification des fichiers journaux ?

Vous pouvez activer la validation de l'intégrité des fichiers journaux. Il est recommandé de gérer et de stocker vos journaux dans un Compte AWS dédié et d'en limiter l'accès. Pour plus d'informations, consultez Utiliser CloudTrail dans ce guide.

Dois-je conserver des fichiers journaux distincts pour chaque application ?

Non, vous pouvez regrouper les données du journal de plusieurs applications dans le même fichier journal. Assurez-vous toutefois qu'un identifiant unique pour chaque application est enregistré dans le flux de journaux.

Ressources

Documentation AWS

- Documentation AWS CloudTrail
- Documentation AWS CloudWatch
- Documentation AWS CloudWatch Logs
- Documentation sur les journaux de flux Amazon VPC
- Documentation AWS X-Ray
- Designing and implementing logging and monitoring with Amazon CloudWatch (Recommandations AWS)

Marketing AWS

- AWS CloudTrail
- Amazon CloudWatch
- Journalisation centralisée dans AWS (Solutions AWS)
- Surveillance et observabilité (Opérations AWS Cloud)
- How to Monitor your Applications Effectively (AWS Startups)

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	—	6 janvier 2023

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle 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 la synchronisation des bases de données source et cible est maintenue, mais seule la base de données source gère les transactions provenant de la connexion d'applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

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

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, connus sous le nom de mauvais robots, sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCoE

Voir le Centre d'excellence du cloud.

CDC

Consultez la section 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 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 articles du CCoE sur le blog de 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 mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

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

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, AWS

Panorama propose des appareils qui ajoutent des CV aux réseaux de caméras locaux, et Amazon SageMaker fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

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

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs configurations. Vous utilisez généralement les données 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 source, de génération, de test, intermédiaire et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

Consultez la section Reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower

pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

informatique de périphérie

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres principaux Comptes AWS ou à AWS Identity and Access Management (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre

service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

épopée

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

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

branche de fonctionnalités

Voir la succursale.

fonctionnalités

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

importance des fonctionnalités

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

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

G

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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.

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir

constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation de l'historien

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

migration de base de données homogène

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

données chaudes

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

correctif

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

IIoT

Voir Internet industriel des objets.

infrastructure immuable

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

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 de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

migration incrémentielle

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

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

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau entre les VPC (identiques ou Régions AWS différents), Internet et les réseaux sur site. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. 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

Consultez la section 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.

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.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

Voir la succursale.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles

ou obtenir un accès non autorisé. 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 qui AWS gère 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

Petit service indépendant qui communique via des API bien définies 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 à l'aide d'API légères. 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 les opérations, les analystes commerciaux et les propriétaires, les ingénieurs de migration, les développeurs et les DevOps professionnels travaillant dans le cadre de sprints. Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

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

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 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, évaluer, prévenir ou réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

OU

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 de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

P

limite des autorisations

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

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les

exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

zones hébergées privées

Conteneur qui contient des informations concernant la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines dans un ou plusieurs VPC. 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.

pseudonymisation

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

publier/souscrire (pub/sub)

Modèle qui permet 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).

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. Cela permet de déterminer ce qui est considéré comme une perte de données acceptable entre le dernier point de restauration 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. Chacune Région AWS est isolée et indépendante 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.

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 d' 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.

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs

qui vous aident à mettre en œuvre les meilleures pratiques AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une 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 propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. Les SCP définissent des barrières de protection ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme

un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

Hub de transit de réseau que vous pouvez utiliser pour relier vos VPC et vos réseaux 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

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

Consultez le cadre de qualification des charges de travail AWS.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire, mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

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

vulnérabilité de type « jour zéro »

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

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.