AWS Base de base de sécurité au démarrage

AWS Directives prescriptives

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Directives prescriptives: AWS Base de base de sécurité au démarrage

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez 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

Introduction ... 1
Public visé ... 2
Cadre de base et responsabilités en matière de sécurité ... 2
Sécurisation de votre compte ... 3
ACCT.01 Définir les contacts au niveau du compte ... 3
ACCT.02 Restreindre l'utilisation de l'utilisateur root ... 4
ACCT.03 Configuration de l'accès à la console ... 5
ACCT.04 Attribuer des autorisations ... 6
ACCT.05 Exiger le MFA ... 7
ACCT.06 Appliquer une politique de mots de passe ... 9
ACCT.07 Enregistrer les événements ... 9
ACCT.08 Empêcher l'accès public aux compartiments S3 privés ... 11
ACCT.09 Supprimer les ressources inutilisées ... 11
ACCT.10 Surveiller les coûts ... 12
ACCT.11 Activer GuardDuty ... 12
ACCT.12 Surveiller les problèmes à haut risque ... 13
Sécurisation de vos charges de travail ... 14
WKLD.01 Utiliser les rôles IAM pour les autorisations ... 14
WKLD.02 Utiliser des politiques basées sur les ressources ... 15
WKLD.03 Utiliser des secrets éphémères ou un service de gestion des secrets ... 16
WKLD.04 Protéger les secrets des applications ... 18
WKLD.05 Détecter et corriger les secrets exposés ... 18
WKLD.06 Utiliser Systems Manager au lieu de SSH ou RDP ... 19
WKLD.07 Enregistrer les événements relatifs aux données pour certains compartiments S3 ... 20
WKLD.08 Chiffrer les volumes Amazon EBS ... 21
WKLD.09 Chiffrer les bases de données Amazon RDS ... 21
WKLD.10 Déployer des ressources privées dans des sous-réseaux privés ... 21
WKLD.11 Utiliser des groupes de sécurité pour restreindre l'accès ... 22
WKLD.12 Utiliser des points de terminaison VPC pour accéder aux services ... 23
WKLD.13 Exiger le protocole HTTPS pour tous les points de terminaison Web publics ... 25
WKLD.14 Utiliser des services de protection des bords pour les terminaux publics ... 26
WKLD.15 Utiliser des modèles pour déployer des contrôles de sécurité ... 27
Collaborateurs ... 28
Historique du document ... 29

Glossaire 31
..... 31
A 32
B 35
C 37
D 40
E 44
F 47
G 49
H 50
I 52
L 54
M 55
O 60
P 62
Q 66
R 66
S 69
T 73
U 75
V 75
W 76
Z 77
..... lxxviii

AWS Base de référence de sécurité au démarrage

Amazon Web Services (contributeurs)

Mai 2023 (historique du document)

Le AWS Startup Security Baseline (AWS SSB) est un ensemble de contrôles qui constituent une base minimale sur laquelle les entreprises peuvent s'appuyer en toute sécurité AWS sans pour autant diminuer leur agilité. Ces contrôles constituent la base de votre posture de sécurité et visent à sécuriser les informations d'identification, à permettre la journalisation et la visibilité, à gérer les coordonnées et à mettre en place des limites de données de base.

Les contrôles présentés dans ce guide sont conçus en se souciant des start-ups, afin d'atténuer les risques de sécurité les plus courants sans nécessiter d'efforts importants. De nombreuses startups commencent leur parcours AWS Cloud avec un single Compte AWS. À mesure que les entreprises se développent, elles migrent vers des architectures à comptes multiples. Les conseils de ce guide sont conçus pour les architectures à compte unique, mais ils vous aident à configurer des contrôles de sécurité faciles à migrer ou à modifier lors de la transition vers une architecture à comptes multiples.

Les contrôles du AWS SSB sont séparés en deux catégories : compte et charge de travail. Les contrôles de compte contribuent à assurer votre Compte AWS sécurité. Ils incluent des recommandations pour configurer l'accès, les politiques et les autorisations des utilisateurs, ainsi que des recommandations sur la manière de surveiller votre compte afin de détecter toute activité non autorisée ou potentiellement malveillante. Les contrôles de charge de travail aident à sécuriser vos ressources et votre code dans le cloud, tels que les applications, les processus backend et les données. Ils incluent des recommandations telles que le chiffrement et la réduction de la portée de l'accès.

> **Note**
>
> Certains des contrôles recommandés dans ce guide remplacent les valeurs par défaut définies lors de la configuration initiale, tandis que la plupart configurent de nouveaux paramètres et de nouvelles politiques. Ce document ne doit en aucun cas être considéré comme exhaustif quant à tous les contrôles disponibles.

Public visé

Ce guide est particulièrement adapté aux start-ups qui en sont aux tout premiers stades de développement, avec un personnel et des opérations minimum.

Les start-ups ou autres entreprises qui en sont à un stade avancé de leurs activités et de leur croissance peuvent encore tirer un avantage significatif de l'examen de ces contrôles par rapport à leurs pratiques actuelles. Si vous identifiez des lacunes, vous pouvez implémenter les contrôles individuels décrits dans ce guide, puis évaluer leur pertinence en tant que solution à long terme.

> **Note**
>
> Les contrôles recommandés dans ce guide sont de nature fondamentale. Les start-ups ou autres entreprises opérant à un stade ultérieur de la mise à l'échelle ou de la sophistication devraient ajouter des contrôles supplémentaires, le cas échéant.

Cadre de base et responsabilités en matière de sécurité

AWS Well-Architected aide les architectes du cloud à créer une infrastructure sécurisée, performante, résiliente et efficace pour leurs applications et leurs charges de travail. Le AWS Startup Security Baseline s'aligne sur le pilier de sécurité du AWS Well-Architected Framework. Le pilier de sécurité décrit comment tirer parti des technologies cloud pour protéger les données, les systèmes et les actifs de manière à améliorer votre posture de sécurité. Cela vous permet de répondre à vos exigences commerciales et réglementaires en suivant les AWS recommandations actuelles.

Vous pouvez évaluer votre adhésion aux meilleures pratiques de Well-Architected en utilisant AWS Well-Architected Toolle. Compte AWS

La sécurité et la conformité sont une responsabilité partagée entre le client AWS et le client. Le modèle de responsabilité partagée est souvent décrit en disant que AWS vous êtes responsable de la sécurité du cloud (c'est-à-dire de la protection de l'infrastructure qui exécute tous les services proposés dans le AWS Cloud) et que vous êtes responsable de la sécurité dans le cloud (telle que déterminée par les AWS Cloud services que vous sélectionnez). Dans le modèle de responsabilité partagée, l'implémentation des contrôles de sécurité décrits dans ce document fait partie de votre responsabilité en tant que client.

Sécurisation de votre compte

Les contrôles et les recommandations présentés dans cette section contribuent à la sécurité de votre AWS compte. Il met l'accent sur l'utilisation d'utilisateurs AWS Identity and Access Management (IAM), de groupes d'utilisateurs et de rôles (également appelés principaux) pour l'accès humain et machine, en limitant l'utilisation de l'utilisateur root et en exigeant une authentification multifactorielle. Dans cette section, vous confirmez que vous AWS disposez des informations de contact nécessaires pour vous contacter concernant l'activité et le statut de votre compte. Vous configurez également des services de surveillance AWS Trusted Advisor, tels qu'Amazon GuardDuty AWS Budgets, afin d'être informé de toute activité sur votre compte et de pouvoir réagir rapidement si l'activité est non autorisée ou inattendue.

Cette section contient les rubriques suivantes :

- ACCT.01 Affecter les contacts au niveau du compte à des listes de distribution d'e-mails valides
- ACCT.02 Restreindre l'utilisation de l'utilisateur root
- ACCT.03 Configurer l'accès à la console pour chaque utilisateur
- ACCT.04 Attribuer des autorisations
- ACCT.05 Exiger une authentification multifactorielle pour se connecter
- ACCT.06 Appliquer une politique de mots de passe
- ACCT.07 Transmettre les CloudTrail journaux à un compartiment S3 protégé
- ACCT.08 Empêcher l'accès public aux compartiments S3 privés
- ACCT.09 Supprimer les sous-réseaux VPCs, les groupes de sécurité et les sous-réseaux non utilisés
- ACCT.10 Configurez AWS Budgets pour surveiller vos dépenses
- ACCT.11 Activer les notifications et y répondre GuardDuty
- ACCT.12 Surveillez et résolvez les problèmes à haut risque en utilisant Trusted Advisor

ACCT.01 Affecter les contacts au niveau du compte à des listes de distribution d'e-mails valides

Lorsque vous configurez des contacts principaux et secondaires pour votre AWS compte, utilisez une liste de distribution d'e-mails plutôt que l'adresse e-mail d'un individu. L'utilisation d'une liste de distribution par e-mail garantit que la propriété et l'accessibilité sont préservées à mesure que les

membres de votre organisation vont et viennent. Définissez d'autres contacts pour la facturation, les opérations et les notifications de sécurité, et utilisez les listes de distribution d'e-mails appropriées en conséquence. AWS utilise ces adresses e-mail pour vous contacter, il est donc important que vous conserviez l'accès à celles-ci.

Pour modifier le nom de votre compte, le mot de passe utilisateur root ou l'adresse e-mail de l'utilisateur root

1. Connectez-vous à la page des paramètres du compte dans la console Billing and Cost Management.
2. Sur la page Paramètres du compte, en regard de Paramètres du compte, choisissez Modifier.
3. En regard du champ à mettre à jour, choisissez Modifier.
4. Lorsque vous avez saisi vos modifications, choisissez Enregistrer les modifications.
5. Lorsque vous avez apporté toutes vos modifications, choisissez Effectué.

Pour modifier vos informations de contact

1. Sur la page Paramètres du compte, sous Informations de contact, choisissez Modifier.
2. Pour les champs à modifier, saisissez les informations mises à jour, puis choisissez Mettre à jour.

Pour ajouter, mettre à jour ou supprimer d'autres contacts

1. Sur la page Paramètres du compte, sous Autres contacts, choisissez Modifier.
2. Pour les champs à modifier, saisissez les informations mises à jour, puis choisissez Mettre à jour.

ACCT.02 Restreindre l'utilisation de l'utilisateur root

L'utilisateur root est créé lorsque vous créez un AWS compte, et cet utilisateur dispose de tous les privilèges et autorisations de propriété sur le compte qui ne peuvent pas être modifiés. N'utilisez l'utilisateur root que pour les tâches qui le nécessitent. Pour plus d'informations, voir Tâches nécessitant des informations d'identification de l'utilisateur root (documentation IAM). Effectuez toutes les autres actions sur votre compte en utilisant d'autres types d'identités IAM, tels que des utilisateurs fédérés dotés de rôles IAM. Pour plus d'informations, veuillez consulter Informations d'identification de sécuritéAWS (documentation IAM).

Pour restreindre l'utilisation de l'utilisateur root

1. Exigez une authentification multifactorielle (MFA) pour l'utilisateur root, comme décrit dans ACCT.05 Exiger une authentification multifactorielle pour se connecter.
2. Créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes. Pour obtenir des informations sur la configuration de l'accès utilisateur, veuillez consulter ACCT.03 Configurer l'accès à la console pour chaque utilisateur.

ACCT.03 Configurer l'accès à la console pour chaque utilisateur

Il est AWS recommandé d'utiliser des informations d'identification temporaires pour accorder l'accès aux ressources Comptes AWS et à ces dernières. Les informations d'identification temporaires ont une durée de vie limitée. Vous n'avez donc pas besoin d'en effectuer une rotation ou de les révoquer de manière explicite une fois celles-ci devenues inutiles. Pour plus d'informations, veuillez consulter Informations d'identification de sécurité temporaires (documentation IAM).

Pour les utilisateurs humains, AWS recommande d'utiliser des identités fédérées provenant d'un fournisseur d'identité centralisé (IdP), AWS IAM Identity Center tel qu'Okta, Active Directory ou Ping Identity. La fédération des utilisateurs vous permet de définir des identités dans un emplacement unique et central, et les utilisateurs peuvent s'authentifier en toute sécurité auprès de plusieurs applications et sites Web AWS, notamment en utilisant un seul ensemble d'informations d'identification. Pour plus d'informations, consultez la section Fédération des identités dans AWS et IAM Identity Center (AWS site Web).

> **Note**
>
> La fédération d'identité peut compliquer le passage d'une architecture à compte unique à une architecture à comptes multiples. Il est courant que les start-ups retardent l'implémentation de la fédération d'identité jusqu'à ce qu'elles aient établi une architecture à comptes multiples gérée dans AWS Organizations.

Mise en place de la fédération d'identité

1. Si vous utilisez IAM Identity Center, veuillez consulter Getting started (documentation IAM Identity Center).

Si vous utilisez un IdP externe ou tiers, consultez la section Fournisseurs d'identité et fédération (documentation IAM).

2. Assurez-vous que votre IdP applique l'authentification multifactorielle (MFA).
3. Appliquez les autorisations conformément à ACCT.04 Attribuer des autorisations.

Pour les start-ups qui ne sont pas prêtes à configurer la fédération d'identité, vous pouvez créer des utilisateurs directement dans IAM. Il ne s'agit pas d'une bonne pratique de sécurité recommandée, car ce sont des informations d'identification à long terme qui n'expirent jamais. Il s'agit toutefois d'une pratique courante pour les start-ups en phase de démarrage afin d'éviter les difficultés liées à la transition vers une architecture à comptes multiples lorsqu'elles sont prêtes sur le plan opérationnel.

À titre de référence, vous pouvez créer un utilisateur IAM pour chaque personne devant accéder à l' AWS Management Console. Si vous configurez des utilisateurs IAM, ne partagez pas les informations d'identification entre les utilisateurs et effectuez régulièrement une rotation des informations d'identification à long terme.

> **Warning**
>
> Les utilisateurs IAM disposent d’informations d’identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu’elles ne sont plus nécessaires.

Pour créer un utilisateur IAM

1. Création d'utilisateurs IAM (documentation IAM).
2. Appliquez les autorisations conformément à ACCT.04 Attribuer des autorisations.

ACCT.04 Attribuer des autorisations

Configurez les autorisations utilisateur dans le compte en attribuant des politiques à leur identité IAM (groupe d'utilisateurs ou rôle). Vous pouvez personnaliser les autorisations ou associer des politiques AWS gérées, qui sont des politiques autonomes conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants. AWS Si vous personnalisez les autorisations, suivez les bonnes pratiques de sécurité qui consistent à accorder le moindre privilège. Le moindre privilège

est la pratique qui consiste à accorder l'ensemble minimal d'autorisations dont chaque utilisateur a besoin pour effectuer ses tâches.

Si vous utilisez des identités fédérées, les utilisateurs accèdent au compte en endossant un rôle IAM via le fournisseur d'identité externe. Le rôle IAM définit ce que les utilisateurs authentifiés par l'IdP de votre organisation sont autorisés à faire. AWS Vous appliquez des politiques personnalisées ou AWS gérées à ce rôle pour configurer les autorisations.

Pour attribuer des autorisations aux identités fédérées

- Si vous utilisez IAM Identity Center, veuillez consulter Use IAM policies in permission sets (documentation IAM Identity Center).

  Si vous utilisez un IdP externe ou tiers, veuillez consulter Ajout des autorisations d'identité IAM (documentation IAM).

Si vous utilisez des utilisateurs IAM, vous pouvez utiliser des groupes d'utilisateurs ou des rôles pour gérer les autorisations de plusieurs utilisateurs IAM. Nous recommandons les groupes d'utilisateurs pour les start-ups, car ils sont plus faciles à gérer et moins sujets aux erreurs de configuration susceptibles de présenter des risques pour la sécurité de votre compte. Attribuez des utilisateurs à des groupes d'utilisateurs sur la base de leurs fonctions. Les exemples de groupes d'utilisateurs incluent les ingénieurs des applications, des données, des réseaux et des opérations de développement (DevOps). Vous pouvez également diviser les types d'utilisateurs en groupes d'utilisateurs plus petits en fonction de l'autorité décisionnelle, par exemple pour les ingénieurs seniors ou non expérimentés.

Pour attribuer des autorisations aux utilisateurs IAM

1. Création de groupes d'utilisateurs IAM (documentation IAM).
2. Associez une politique AWS gérée à un groupe d'utilisateurs IAM (documentation IAM).

ACCT.05 Exiger une authentification multifactorielle pour se connecter

Avec l'authentification multifactorielle (MFA), les utilisateurs disposent d'un appareil qui génère une réponse à un défi d'authentification. Les informations d'identification de l'utilisateur et la réponse générée par le périphérique sont requis pour mener à bien le processus du connexion. Comme

bonne pratique de sécurité, il est recommandé d'activer la MFA pour l'accès aux Compte AWS , en particulier pour les informations d'identification à long terme telles que l'utilisateur root du compte et les utilisateurs IAM.

Pour configurer la MFA pour l'utilisateur root

1. Connectez-vous à la AWS Management Console.
2. À droite de la barre de navigation, choisissez le nom de votre compte, puis Mes informations d'identification de sécurité.
3. Au besoin, choisissez Passer aux informations d'identification de sécurité.
4. Développez la section Multi-Factor Authentication (MFA).
5. Choisissez Activer MFA.
6. Suivez les instructions de l'assistant pour configurer vos appareils MFA en conséquence. Pour plus d'informations, voir Authentification AWS multifactorielle dans IAM (documentation IAM).

Pour configurer la MFA dans IAM Identity Center

- Enable MFA (documentation IAM Identity Center)

Pour configurer la MFA pour votre propre utilisateur IAM

1. À l'aide de vos informations de connexion, connectez-vous à la console IAM.
2. Dans la barre de navigation en haut à droite, choisissez votre nom d'utilisateur, puis My Security Credentials (Mes informations d'identification de sécurité).
3. Dans l'onglet AWS IAM credentials (Informations d'identification AWS IAM), sous la section Multi-factor authentication (Authentification multi-facteur), sélectionnez Manage MFA device (Gérer le dispositif MFA).

Pour configurer la MFA pour les autres utilisateurs IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la.
2. Dans le panneau de navigation, choisissez utilisateurs.
3. Choisissez le nom de l'utilisateur pour lequel vous voulez activer la fonction MFA, puis choisissez l'onglet Security credentials (informations d'identification de sécurité).
4. En regard de Assigned MFA device (Dispositif MFA affecté), choisissez Manage (Gérer).

5. Suivez les instructions de l'assistant pour configurer vos appareils MFA en conséquence. Pour plus d'informations, voir Authentification AWS multifactorielle dans IAM (documentation IAM).

ACCT.06 Appliquer une politique de mots de passe

Les utilisateurs se connectent au en AWS Management Console fournissant des informations d'identification, et le MFA est recommandé. Exigez que les mots de passe respectent une politique de mot de passe fort afin d'empêcher leur découverte par la force ou l'ingénierie sociale.

Pour plus d'informations sur les dernières recommandations en matière de mots de passe forts, veuillez consulter Password Policy Guide sur le site Web de Center for Internet Security (CIS).

Pour les utilisateurs IAM, vous pouvez configurer les exigences en matière de mot de passe dans une politique de mot de passe IAM personnalisée. Pour plus d'informations, veuillez consulter Setting an account password policy (documentation IAM).

Pour créer une politique de mot de passe personnalisée

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la.
2. Dans le panneau de navigation, choisissez Paramètres du compte.
3. Dans la section Politique de mot de passe, sélectionnez Modifier la politique de mot de passe.
4. Sélectionnez les options que vous souhaitez appliquer à votre politique de mot de passe, puis sélectionnez Enregistrer les modifications.

ACCT.07 Transmettre les CloudTrail journaux à un compartiment S3 protégé

Les actions entreprises par les utilisateurs, les rôles et les services de votre AWS compte sont enregistrées sous forme d'événements dans AWS CloudTrail. CloudTrail est activé par défaut, et dans la CloudTrail console, vous pouvez accéder à 90 jours d'informations sur l'historique des événements. Pour consulter, rechercher, télécharger, archiver, analyser et répondre à l'activité du compte dans l'ensemble de votre AWS infrastructure, consultez la section Affichage des CloudTrail événements avec l'historique des événements (CloudTrail documentation).

Pour conserver CloudTrail l'historique au-delà de 90 jours avec des données supplémentaires, vous créez une nouvelle trace qui fournit les fichiers journaux à un compartiment Amazon Simple Storage

Service (Amazon S3) pour tous les types d'événements. Lorsque vous créez un parcours dans la CloudTrail console, vous créez un parcours multirégional.

Pour créer un journal qui fournit des journaux Régions AWS pour tous dans un compartiment S3

1. Créez un parcours (CloudTrail documentation). Sur la page Choisir des événements de journaux, procédez comme suit :

   a. Pour Activité de l'API, choisissez Lecture et Écriture.

   b. Pour les environnements de préproduction, choisissez Exclure les événements AWS KMS . Cela exclut tous les AWS Key Management Service (AWS KMS) événements de votre parcours. AWS KMS lit des actions telles que `EncryptDecrypt`, et `GenerateDataKey` peut générer un grand nombre d'événements.

      Pour les environnements de production, choisissez de journaliser les événements de gestion en écriture et décochez la case Exclure les événements AWS KMS . Cela exclut les événements de AWS KMS lecture à volume élevé, mais enregistre toujours les événements d'écriture pertinents, tels que `DisableDelete`, et`ScheduleKey`. Il s'agit des paramètres de AWS KMS journalisation minimaux recommandés pour un environnement de production.

2. Le nouveau journal de suivi s’affiche sur la page Journaux de suivi. En 15 minutes environ, CloudTrail publie des fichiers journaux qui indiquent les appels d'interface de programmation d' AWS applications (API) effectués dans votre compte. Les fichiers journaux se trouvent dans le compartiment S3 que vous avez spécifié.

Pour aider à sécuriser les compartiments S3 dans lesquels vous stockez les fichiers CloudTrail journaux

1. Consultez la politique relative aux compartiments Amazon S3 (CloudTrail documentation) pour tous les compartiments dans lesquels vous stockez des fichiers journaux et ajustez-la si nécessaire pour supprimer tout accès inutile.
2. En tant que bonne pratique en matière de sécurité, veillez à ajouter manuellement une clé de condition `aws:SourceArn` à la politique de compartiment. Pour plus d'informations, consultez Créer ou mettre à jour un compartiment Amazon S3 à utiliser pour stocker les fichiers journaux d'un journal d'entreprise (CloudTrail documentation).
3. Enable MFA Delete (documentation Amazon S3).

ACCT.08 Empêcher l'accès public aux compartiments S3 privés

Par défaut, seuls l'utilisateur root Compte AWS et le principal IAM, le cas échéant, sont autorisés à lire et à écrire dans les compartiments Amazon S3 créés par ce principal. L'accès est accordé à des principaux IAM supplémentaires en utilisant des politiques basées sur l'identité, et les conditions d'accès peuvent être appliquées à l'aide d'une politique de compartiment. Vous pouvez créer des politiques de compartiment qui accordent l'accès au grand public au compartiment, un compartiment public.

Les compartiments créés au plus tard le 28 avril 2023 ont le paramètre Blocage d'accès public activé par défaut. Pour les compartiments créés avant cette date, les utilisateurs peuvent mal configurer la politique de compartiment et accorder involontairement l'accès au public. Vous pouvez éviter cette mauvaise configuration en activant le paramètre Blocage d'accès public pour chaque compartiment. Si vous n'avez aucun cas d'utilisation actuel ou futur pour un compartiment S3 public, activez ce paramètre au Compte AWS niveau correspondant. Ce paramètre empêche les politiques qui autorisent l'accès public.

Pour empêcher l'accès public aux compartiments S3

- Configuration des paramètres de blocage d'accès public pour vos compartiments S3 (documentation Amazon S3).

AWS Trusted Advisor génère un résultat jaune pour les compartiments S3 qui autorisent l'accès au public par liste ou en lecture et un résultat rouge pour les compartiments qui autorisent les téléchargements ou les suppressions publics. À titre de référence, suivez le contrôle ACCT.12 Surveillez et résolvez les problèmes à haut risque en utilisant Trusted Advisor pour identifier et corriger les compartiments mal configurés. Les compartiments S3 accessibles au public sont également indiqués dans la console Amazon S3.

ACCT.09 Supprimer les sous-réseaux VPCs, les groupes de sécurité et les sous-réseaux non utilisés

Pour réduire les risques de problèmes de sécurité, supprimez ou désactivez les ressources qui ne sont pas utilisées. Dans un nouveau AWS compte, un cloud privé virtuel (VPC) est créé automatiquement par défaut dans chaque compte Région AWS, ce qui vous permet d'attribuer des adresses IP publiques dans des sous-réseaux publics. Toutefois, s' VPCs ils ne sont pas nécessaires, cela présente un risque d'exposition involontaire des ressources.

S'ils ne sont pas utilisés, supprimez la valeur par défaut VPCs dans toutes les régions, et pas uniquement dans celles des régions où vous pourriez déployer des charges de travail. La suppression d'un VPC entraîne également la suppression de ses composants, tels que les sous-réseaux et les groupes de sécurité.

> **Note**
>
> Vous pouvez consulter toutes les régions ainsi que VPCs sur la console Amazon EC2 Global View. Pour plus d'informations, consultez Répertorier et filtrer les ressources par région à l'aide d'Amazon EC2 Global View (EC2documentation Amazon).

Pour supprimer les valeurs par défaut non utilisées VPCs

1. Supprimer votre VPC (documentation Amazon VPC).
2. Répétez l'opération si nécessaire pour VPCs les autres régions.

ACCT.10 Configurez AWS Budgets pour surveiller vos dépenses

AWS Budgets permettre le suivi des coûts mensuels et de l'utilisation avec des notifications lorsque les coûts sont prévus pour dépasser les seuils cibles. Les notifications de coûts prévisionnels peuvent fournir une indication d'une activité imprévue, fournissant ainsi une protection supplémentaire en plus des autres systèmes de surveillance, tels qu' AWS Trusted Advisor Amazon GuardDuty. Le suivi et la compréhension de vos AWS coûts font également partie d'une bonne hygiène opérationnelle.

Pour établir un budget dans AWS Budgets

- Créez un budget de coûts (AWS Budgets documentation).

ACCT.11 Activer les notifications et y répondre GuardDuty

Amazon GuardDuty est un service de détection des menaces qui surveille en permanence les comportements malveillants ou non autorisés afin de protéger vos AWS comptes, vos charges de travail et vos données. Lorsqu'il détecte une activité inattendue et potentiellement malveillante, il GuardDuty fournit des résultats de sécurité détaillés à des fins de visibilité et de correction. GuardDuty peut détecter des menaces telles que l'activité d'extraction de cryptomonnaies, l'accès depuis les clients et les relais Tor, les comportements inattendus et les informations

d'identification IAM compromises. Activez GuardDuty et répondez aux résultats pour mettre fin aux comportements potentiellement malveillants ou non autorisés dans votre AWS environnement. Pour plus d'informations sur les résultats dans GuardDuty, consultez la section Types de recherche (GuardDuty documentation).

Vous pouvez utiliser Amazon CloudWatch Events pour configurer des notifications automatiques lors de la GuardDuty création ou de la modification d'une constatation. Dans un premier temps, vous configurez une rubrique Amazon Simple Notification Service (Amazon SNS), vous y ajoutez des points de terminaison, ou des adresses e-mail. Ensuite, vous configurez un CloudWatch événement pour les GuardDuty résultats, et la règle de l'événement informe les points de terminaison dans la rubrique Amazon SNS.

Pour activer GuardDuty et envoyer GuardDuty des notifications

1. Activez Amazon GuardDuty (GuardDuty documentation).
2. Créez une règle d' CloudWatch événements pour vous informer des GuardDuty résultats (GuardDutydocumentation).

ACCT.12 Surveillez et résolvez les problèmes à haut risque en utilisant Trusted Advisor

AWS Trusted Advisor analyse passivement votre AWS infrastructure pour détecter les problèmes à haut risque ou à fort impact liés à la sécurité, aux performances, aux coûts et à la fiabilité. Il fournit des informations détaillées sur les ressources concernées et des recommandations de mesures correctives. Pour une liste complète des vérifications et des descriptions, voir AWS Trusted Advisor la référence des vérifications (Trusted Advisor documentation).

Passez en revue les Trusted Advisor résultats régulièrement et corrigez les problèmes si nécessaire. Si vous avez souscrit aux plans AWS Business Support ou Enterprise Support, vous pouvez vous abonner à un e-mail de résultats hebdomadaire. Pour plus d'informations, veuillez consulter Set up notification preferences (documentation AWS Support).

Pour consulter les problèmes dans Trusted Advisor

- Passez en revue chaque catégorie de contrôle conformément aux instructions de la section Afficher les catégories de chèques (Support documentation). Nous vous recommandons d'examiner au moins les problèmes d'action recommandée qui sont en rouge.

Sécurisation de vos charges de travail

Les contrôles et les recommandations de cette section vous aident à sécuriser vos charges de travail qui s'exécutent dans AWS, pendant que vous les générez. Ils mettent l'accent sur les pratiques sécurisées pour gérer les secrets des applications et la portée de l'accès, réduire les routes d'accès aux ressources privées et utiliser le chiffrement pour protéger les données en transit et au repos.

Cette section contient les rubriques suivantes :

- WKLD.01 Utiliser les rôles IAM pour les autorisations d'environnement de calcul
- WKLD.02 Restreindre le champ d'utilisation des informations d'identification à l'aide de politiques et d'autorisations basées sur les ressources
- WKLD.03 Utiliser des secrets éphémères ou un service de gestion des secrets
- WKLD.04 Empêcher l'exposition des secrets des applications
- WKLD.05 Détecter et corriger les secrets exposés
- WKLD.06 Utiliser Systems Manager au lieu de SSH ou RDP
- WKLD.07 Enregistrer les événements de données pour les compartiments S3 contenant des données sensibles
- WKLD.08 Chiffrer les volumes Amazon EBS
- WKLD.09 Chiffrer les bases de données Amazon RDS
- WKLD.10 Déployer des ressources privées dans des sous-réseaux privés
- WKLD.11 Restreindre l'accès au réseau en utilisant des groupes de sécurité
- WKLD.12 Utiliser des points de terminaison VPC pour accéder aux services pris en charge
- WKLD.13 Exiger le protocole HTTPS pour tous les points de terminaison Web publics
- WKLD.14 Utiliser des services de protection des bords pour les terminaux publics
- WKLD.15 Définissez les contrôles de sécurité dans les modèles et déployez-les en utilisant les pratiques CI/CD

WKLD.01 Utiliser les rôles IAM pour les autorisations d'environnement de calcul

Dans AWS Identity and Access Management (IAM), un rôle représente un ensemble d'autorisations qui peuvent être assumées par une personne ou un service pendant une période configurable. En

utilisant des rôles, vous n'avez plus besoin de stocker ou de gérer des informations d'identification à long terme, ce qui réduit considérablement les risques d'utilisation involontaire. Attribuez un rôle IAM directement aux instances, AWS Fargate tâches et services Amazon Elastic Compute Cloud (Amazon EC2), aux AWS Lambda fonctions et aux autres services de AWS calcul lorsque cela est pris en charge. Les applications qui utilisent un AWS SDK et s'exécutent dans ces environnements informatiques utilisent automatiquement les informations d'identification du rôle IAM pour l'authentification.

L'approche et les instructions relatives à l'utilisation des rôles IAM pour chaque service se trouvent dans la documentation AWS pour le service. Par exemple, consultez ce qui suit :

- Rôles IAM pour Amazon EC2 (EC2 documentation Amazon)
- IAM roles for tasks (documentation Amazon Elastic Container Service)
- Rôle d'exécution Lambda (documentation Lambda)

WKLD.02 Restreindre le champ d'utilisation des informations d'identification à l'aide de politiques et d'autorisations basées sur les ressources

Les politiques sont des objets qui peuvent définir des autorisations ou des conditions d'accès. Il existe deux principaux types de politique :

- Les politiques basées sur l'identité sont associées aux principaux et définissent les autorisations du principal dans l'environnement. AWS
- Les politiques basées sur les ressources sont attachées à une ressource, telle qu'un compartiment Amazon Simple Storage Service (Amazon S3) ou un point de terminaison de cloud privé virtuel (VPC). Ces politiques spécifient les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

Pour qu'un principal soit autorisé à effectuer une action sur une ressource, il doit disposer d'une autorisation accordée dans sa politique basée sur l'identité et satisfaire aux conditions de la politique basée sur les ressources. Pour plus d'informations, veuillez consulter Politiques basées sur l'identité et Politiques basées sur une ressource (documentation IAM).

Les conditions recommandées pour les politiques basées sur les ressources sont les suivantes :

- Limitez l'accès aux seuls directeurs d'une organisation spécifiée (définie dans AWS Organizations) en utilisant `aws:PrincipalOrgID` cette condition.
- Limiter l'accès au trafic provenant d'un VPC ou d'un point de terminaison d'un VPC spécifique en utilisant respectivement la condition `aws:SourceVpc` ou `aws:SourceVpce`.
- Autoriser ou refuser le trafic en fonction de l'adresse IP source à l'aide d'une condition `aws:SourceIp`.

L'exemple suivant est une politique basée sur les ressources qui utilise la condition `aws:PrincipalOrgID` pour autoriser uniquement les principaux dans l'organisation **<o-xxxxxxxxxxx>** à accéder au compartiment S3 **<bucket-name>** :

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
     }
   ]
}
```

WKLD.03 Utiliser des secrets éphémères ou un service de gestion des secrets

Les secrets d'application sont principalement constitués d'informations d'identification, telles que des paires de clés, des jetons d'accès, des certificats numériques et des informations d'identification de connexion. L'application utilise ces secrets pour accéder à d'autres services dont elle dépend, comme une base de données. Pour protéger ces secrets, nous recommandons qu'ils soient éphémères (générés au moment de la demande et de courte durée, comme avec des rôles IAM) ou qu'ils soient récupérés auprès d'un service de gestion des secrets. Cela permet d'éviter toute exposition accidentelle par le biais de mécanismes moins sécurisés, tels que la persistance dans des fichiers

de configuration statiques. Cela facilite également la promotion du code d'application depuis les environnements de développement vers les environnements de production.

Pour un service de gestion des secrets, nous vous recommandons d'utiliser à la fois Parameter Store, une fonctionnalité de AWS Systems Manager et : AWS Secrets Manager

- Utilisez Parameter Store pour gérer les secrets et d'autres paramètres qui sont des paires clé-valeur individuelles, basés sur des chaînes, courts et fréquemment consultés. Vous utilisez une clé AWS Key Management Service (AWS KMS) pour chiffrer le secret. Le stockage des paramètres dans le niveau standard de Parameter Store est gratuit. Pour plus d'informations sur les niveaux de paramètres, veuillez consulter Gestion des niveaux de paramètres (documentation Systems Manager).
- Utilisez Secrets Manager pour stocker des secrets sous forme de document (tels que plusieurs paires clé-valeur associées), dont la taille est supérieure à 4 Ko (tels que des certificats numériques) ou qui bénéficieraient d'une rotation automatique.

Vous pouvez utiliser Parameter Store APIs pour récupérer les secrets stockés dans Secrets Manager. Cela vous permet de normaliser le code de votre application lorsque vous utilisez une combinaison des deux services.

Pour gérer les secrets dans Parameter Store

1. Créez une AWS KMS clé symétrique (AWS KMS documentation).
2. Créez un SecureString paramètre (documentation Systems Manager). Les secrets dans Parameter Store utilisent le type de données `SecureString`.
3. Dans votre application, récupérez un paramètre depuis Parameter Store à l'aide du AWS SDK correspondant à votre langage de programmation. Pour des exemples de code, consultez GetParameter(Bibliothèque de codes AWS SDK).

Pour gérer les secrets dans Secrets Manager

1. Créer un secret (documentation Secrets Manager).
2. Récupération des secrets à partir de AWS Secrets Manager (documentation Secrets Manager).

   Il est important de lire Utiliser les bibliothèques de mise en cache AWS Secrets Manager côté client pour améliorer la disponibilité et la latence liées à l'utilisation de vos secrets (AWS article

de blog). L'utilisation du côté client SDKs, qui intègre déjà les meilleures pratiques, devrait accélérer et simplifier l'utilisation et l'intégration de Secrets Manager.

WKLD.04 Empêcher l'exposition des secrets des applications

Lors du développement local, les secrets des applications peuvent être stockés dans des fichiers de configuration ou de code locaux et enregistrés accidentellement dans des référentiels de code source. Les référentiels non sécurisés hébergés par des fournisseurs de services publics peuvent faire l'objet d'un accès non autorisé et d'une découverte ultérieure de ces secrets. Utilisez les outils disponibles pour empêcher l'enregistrement de secrets. Intégrez la vérification des secrets exposés dans le cadre de vos processus d'examen manuel du code.

Voici quelques outils courants qui peuvent empêcher l'enregistrement des secrets des applications dans les référentiels de code source :

- Gitleaks (GitHubdépôt)
- Whispers (GitHubréférentiel)
- detect-secrets (dépôt) GitHub
- git-secrets (dépôt) GitHub
- TruffleHog(GitHubréférentiel)

WKLD.05 Détecter et corriger les secrets exposés

Dans WKLD.03 Utiliser des secrets éphémères ou un service de gestion des secrets et WKLD.04 Empêcher l'exposition des secrets des applications, vous avez mis en place des mesures de protection des secrets. Dans le cadre de ce contrôle, vous déployez une solution capable de détecter si des secrets ont contourné ces mesures de prévention, et vous pouvez y remédier en conséquence.

Amazon CodeGuru Reviewer détecte les secrets des applications dans le code source et fournit un mécanisme permettant de corriger et de publier les secrets détectés dans Secrets Manager. Le code d'application permettant de récupérer le secret depuis Secrets Manager est également fourni. Réalisez une analyse coûts-avantages pour déterminer si cette solution convient à votre entreprise. Comme alternative, certaines des solutions open source de WKLD.04 Empêcher l'exposition des secrets des applications proposent une fonctionnalité de détection pour les secrets existants.

Pour configurer l'intégration de CodeGuru Reviewer à Secrets Manager

- Utilisez CodeGuru Reviewer pour identifier les secrets codés en dur et les AWS Secrets Manager sécuriser (article de AWS blog et visite guidée).

WKLD.06 Utiliser Systems Manager au lieu de SSH ou RDP

Les sous-réseaux publics, qui ont une route par défaut pointant vers une passerelle Internet, présentent par nature un risque de sécurité plus important que les sous-réseaux privés, qui n'ont aucun accès à Internet. Vous pouvez exécuter EC2 des instances dans des sous-réseaux privés et utiliser la fonctionnalité du gestionnaire de session AWS Systems Manager pour accéder à distance aux instances via AWS Command Line Interface (AWS CLI) ou AWS Management Console. Vous pouvez ensuite utiliser la console AWS CLI or pour démarrer une session qui se connecte à l'instance via un tunnel sécurisé, évitant ainsi de devoir gérer les informations d'identification supplémentaires utilisées pour Secure Shell (SSH) ou le protocole RDP (Windows Remote Desktop Protocol).

Utilisez le gestionnaire de session au lieu d'exécuter des EC2 instances dans des sous-réseaux publics, d'exécuter des boîtes de renvoi ou d'exécuter des hôtes bastions.

Pour configurer Session Manager

1. Assurez-vous que l' EC2 instance utilise le dernier système d'exploitation Amazon Machine Images (AMIs), tel qu'Amazon Linux ou Ubuntu. L' AWS Systems Manager agent (agent SSM) est préinstallé sur l'AMI.
2. Assurez-vous que l'instance est connectée, via une passerelle Internet ou via des points de terminaison VPC, aux adresses suivantes (en les **`<Region>`** remplaçant par les adresses appropriées) : Région AWS
   a. `ec2messages.`**`<Region>`**`.amazonaws.com`
   b. `ssm.`**`<Region>`**`.amazonaws.com`
   c. `ssmmessages.`**`<Region>`**`.amazonaws.com`
3. Associez la politique AWS gérée `AmazonSSMManagedInstanceCore` au rôle IAM associé à vos instances.

Pour plus d'informations, veuillez consulter Configuration de Session Manager (documentation Systems Manager).

Pour démarrer une session

- Démarrer une session (documentation Systems Manager).

WKLD.07 Enregistrer les événements de données pour les compartiments S3 contenant des données sensibles

Par défaut, AWS CloudTrail capture les événements de gestion, c'est-à-dire les événements qui créent, modifient ou suppriment des ressources dans votre compte. Ces événements de gestion ne capturent pas les opérations de lecture ou d'écriture sur des objets individuels dans les compartiments Amazon Simple Storage Service. Lors d'un événement de sécurité, il est important de capturer les accès non autorisés aux données ou leur utilisation non autorisée au niveau d'un enregistrement ou d'un objet individuel. CloudTrail À utiliser pour enregistrer les événements de données pour tous les compartiments S3 qui stockent des données sensibles ou critiques pour l'entreprise, à des fins de détection et d'audit.

> **Note**
>
> Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour en savoir plus, consultez Pricing AWS CloudTrail (Tarification).

Pour journaliser des événements de données pour les journaux de suivi

1. Connectez-vous à la CloudTrailconsole AWS Management Console et ouvrez-la
2. Dans le panneau de navigation de gauche, choisissez Trails (Journaux de suivi), puis le nom du journal de suivi.
3. Dans Renseignements généraux, choisissez Modifier pour modifier les paramètres suivants. Vous ne pouvez pas modifier le nom d’un journal de suivi.
   a. Pour Événements de données, choisissez Modifier.
   b. Pour Data event source (Source d'événements de données), choisissez S3.
   c. Pour Tous les compartiments S3 actuels et futurs, désélectionnez Lecture et Écriture.
   d. Dans Sélection du compartiment individuel, recherchez le compartiment sur lequel journaliser les événements de données. Il est possible de sélectionner plusieurs compartiments dans cette fenêtre. Choisissez Ajouter un compartiment pour journaliser

les événements de données pour d'autres compartiments. Choisissez de journaliser les événements Lecture tels que `GetObject`, les événements Écriture tels que `PutObject`, ou les deux.

e. Choisissez Update trail (Mettre à jour un journal de suivi).

WKLD.08 Chiffrer les volumes Amazon EBS

Appliquez le chiffrement des volumes Amazon Elastic Block Store (Amazon EBS) comme comportement par défaut dans votre compte AWS . Les volumes chiffrés ont les mêmes performances d'opérations d'entrée/sortie par seconde (IOPS) que les volumes non chiffrés, avec un effet minimal sur la latence. Cela empêche de régénérer les volumes ultérieurement pour des raisons de conformité ou pour d'autres raisons. Pour plus d'informations, consultez les meilleures pratiques à connaître en matière de chiffrement Amazon EBS (article de AWS blog).

Pour chiffrer les volumes Amazon EBS

- Activez le chiffrement par défaut (documentation Amazon EBS).

WKLD.09 Chiffrer les bases de données Amazon RDS

Comme pour WKLD.08 Chiffrer les volumes Amazon EBS, activez le chiffrement des bases de données Amazon Relational Database Service (Amazon RDS). Ce chiffrement est effectué au niveau du volume sous-jacent et offre les mêmes performances d'IOPS que les volumes non chiffrés, avec un effet minimal sur la latence. Pour plus d'informations, veuillez consulter Présentation du chiffrement des ressources Amazon RDS (documentation Amazon RDS).

Pour chiffrer une instance de base de données RDS

- Encrypt a database instance (documentation Amazon RDS).

WKLD.10 Déployer des ressources privées dans des sous-réseaux privés

Déployez des ressources qui ne nécessitent pas d'accès direct à Internet, telles que les EC2 instances, les bases de données, les files d'attente, la mise en cache ou toute autre infrastructure, dans un sous-réseau privé VPC. Aucune route n'est déclarée dans la table de routage des sous-

réseaux privés vers une passerelle Internet attachée, et les sous-réseaux ne peuvent pas recevoir de trafic Internet. Le trafic provenant d'un sous-réseau privé destiné à Internet doit être soumis à une traduction d'adresses réseau (NAT) via une passerelle AWS NAT gérée ou une EC2 instance exécutant des processus NAT dans un sous-réseau public. Pour plus d'informations sur l'isolation du réseau, veuillez consulter Sécurité de l'infrastructure dans Amazon VPC (documentation Amazon VPC).

Respectez les pratiques suivantes lors de la création de ressources et de sous-réseaux privés :

- Lorsque vous créez un sous-réseau privé, désactivez l'attribution automatique d'une adresse publique IPv4.
- Lorsque vous créez des EC2 instances privées, désactivez l'attribution automatique d'une adresse IP publique. Cela empêche l'attribution d'une adresse IP publique si l'instance est déployée involontairement dans un sous-réseau public en raison d'une mauvaise configuration.

Vous spécifiez le sous-réseau d'une ressource dans le cadre de sa configuration, le cas échéant.

WKLD.11 Restreindre l'accès au réseau en utilisant des groupes de sécurité

Utilisez des groupes de sécurité pour contrôler le trafic vers les EC2 instances, les bases de données RDS et les autres ressources prises en charge. Les groupes de sécurité font office de pare-feu virtuel qui peut être appliqué à n'importe quel groupe de ressources connexes afin de définir de manière cohérente des règles autorisant le trafic entrant et sortant. Outre les règles basées sur les adresses IP et les ports, les groupes de sécurité prennent en charge des règles permettant d'autoriser le trafic provenant de ressources associées à d'autres groupes de sécurité. Par exemple, un groupe de sécurité de base de données peut avoir des règles autorisant uniquement le trafic provenant d'un groupe de sécurité d'un serveur d'applications.

Par défaut, les groupes de sécurité autorisent tout le trafic sortant, mais pas le trafic entrant. La règle du trafic sortant peut être supprimée, ou vous pouvez configurer des règles supplémentaires ajoutées pour restreindre le trafic sortant et autoriser le trafic entrant. Si le groupe de sécurité n'a pas de règles sortantes, aucun trafic sortant issu de votre instance n'est autorisé. Pour obtenir plus d'informations, veuillez consulter Control traffic to resources using security groups (documentation Amazon VPC).

Dans l'exemple suivant, trois groupes de sécurité contrôlent le trafic entre un Application Load Balancer et les EC2 instances connectées à une base de données Amazon RDS for MySQL.

Groupe de sécurité	Règles entrantes	Règles sortantes
Groupe de sécurité Application Load Balancer	Description : autoriser le trafic HTTPS depuis n'importe où Type : HTTPS Source : N'importe où- IPv4 (0.0.0.0/0)	Description : autoriser tout le trafic vers n'importe où Type : tout le trafic Destination : N'importe où- IPv4 (0.0.0.0/0)
EC2 groupe de sécurité d'instance	Description : autoriser le trafic HTTP depuis l'Application Load Balancer Type : HTTP Source: groupe de sécurité d'Application Load Balancer	Description : autoriser tout le trafic vers n'importe où Type : tout le trafic Destination : N'importe où- IPv4 (0.0.0.0/0)
Groupe de sécurité de base de données RDS	Description : Autoriser le trafic MySQL depuis l' EC2instance Type : MySQL Source : groupe de sécurité d' EC2 instance	Aucune règle sortante

WKLD.12 Utiliser des points de terminaison VPC pour accéder aux services pris en charge

Dans VPCs, les ressources qui ont besoin d'accéder AWS à d'autres services externes nécessitent soit une route vers Internet (`0.0.0.0/0`), soit vers l'adresse IP publique du service cible. Utilisez les points de terminaison VPC pour activer une route IP privée depuis votre VPC vers des services pris en charge AWS ou d'autres services, évitant ainsi d'avoir à utiliser une passerelle Internet, un périphérique NAT, une connexion à un réseau privé virtuel (VPN) ou une connexion. AWS Direct Connect

Les points de terminaison d'un VPC permettent d'associer des politiques et des groupes de sécurité afin de mieux contrôler l'accès à un service. Par exemple, vous pouvez écrire une politique de point de terminaison d'un VPC pour Amazon DynamoDB afin d'autoriser uniquement les actions au niveau de l'élément et d'empêcher les actions au niveau de la table pour toutes les ressources du VPC, quelle que soit leur propre politique d'autorisation. Vous pouvez également écrire une politique de compartiment S3 pour autoriser uniquement les demandes provenant d'un point de terminaison d'un VPC spécifique, en refusant tout autre accès externe. Un point de terminaison VPC peut également disposer d'une règle de groupe de sécurité qui, par exemple, restreint l'accès aux seules EC2 instances associées à un groupe de sécurité spécifique à une application, tel que le niveau de logique métier d'une application Web.

Il existe différents types de point de terminaison d'un VPC. Vous accédez à la plupart des services en utilisant un point de terminaison d'interface d'un VPC. L'accès à DynamoDB se fait à l'aide d'un point de terminaison d'une passerelle. Amazon S3 prend en charge les points de terminaison de passerelle et d'interface. Les points de terminaison Gateway sont recommandés pour les charges de travail contenues dans un seul AWS compte et une seule région, et sont proposés sans frais supplémentaires. Les points de terminaison d'interface sont recommandés si un accès plus extensible est requis, par exemple à un compartiment S3 depuis un autre réseau VPCs, depuis un réseau sur site ou depuis un autre réseau. Régions AWS Les points de terminaison de l'interface sont soumis à des frais de disponibilité horaire et à des frais de traitement des données par Go, tous deux inférieurs aux frais respectifs d'envoi des données via NAT Gateway. `0.0.0.0/0` AWS

Pour plus d'informations sur l'utilisation de points de terminaison d'un VPC, consultez les ressources suivantes :

- Pour plus d'informations sur le choix entre les points de terminaison de passerelle et d'interface pour Amazon S3, consultez Choisir votre stratégie de point de terminaison VPC pour Amazon S3AWS (article de blog).
- Accédez et Service AWS utilisez un point de terminaison VPC d'interface (documentation Amazon VPC).
- Points de terminaison de passerelle (documentation Amazon VPC).
- Pour un exemple de politiques de compartiment S3 qui limitent l'accès à un VPC ou à un point de terminaison d'un VPC spécifique, veuillez consulter Restriction de l'accès à un point de terminaison d'un VPC spécifique (documentation Amazon S3).
- Pour un exemple de politiques de point de terminaison DynamoDB qui limitent les actions, veuillez consulter Politiques de point de terminaison pour DynamoDB (documentation Amazon VPC).

WKLD.13 Exiger le protocole HTTPS pour tous les points de terminaison Web publics

Exigez le protocole HTTPS pour renforcer la crédibilité de vos points de terminaison Web, autoriser vos points de terminaison à utiliser des certificats pour prouver leur identité et confirmer que tout le trafic entre votre point de terminaison et les clients connectés est chiffré. Pour les sites Web publics, l'avantage supplémentaire obtenu est un meilleur classement dans les moteurs de recherche.

De nombreux AWS services fournissent des points de terminaison Web publics pour vos ressources, tels qu'Amazon AWS Elastic Beanstalk CloudFront, Amazon API Gateway, Elastic Load Balancing et AWS Amplify. Pour savoir comment exiger le protocole HTTPS pour chacun de ces services, consultez les rubriques suivantes :

- Elastic Beanstalk (documentation Elastic Beanstalk)
- CloudFront(CloudFront documentation)
- Application Load Balancer (centre de AWS connaissances)
- Classic Load Balancer (centre de AWS connaissances)
- Amplify (documentation Amplify)

Les sites Web statiques hébergés sur Amazon S3 ne prennent pas en charge le protocole HTTPS. Pour exiger le protocole HTTPS pour ces sites Web, vous pouvez utiliser CloudFront. L'accès public aux compartiments S3 qui diffusent du contenu n' CloudFront est pas obligatoire.

À utiliser CloudFront pour diffuser un site Web statique hébergé sur Amazon S3

1. CloudFront À utiliser pour diffuser un site Web statique hébergé sur Amazon S3 (AWS Knowledge Center).
2. Si vous configurez l'accès à un compartiment S3 public, exigez le protocole HTTPS entre les utilisateurs et CloudFront (CloudFrontdocumentation).

   Si vous configurez l'accès à un compartiment S3 privé, limitez l'accès au contenu Amazon S3 en utilisant une identité d'accès d'origine (CloudFront documentation).

En outre, configurez les points de terminaison HTTPS pour exiger des chiffrements et des protocoles TLS (Transport Layer Security) modernes, sauf si la compatibilité avec d'anciens protocoles est requise. Par exemple, utilisez `ELBSecurityPolicy-FS-1-2-Res-2020-10` ou la politique la plus

récente disponible pour les écouteurs HTTPS Application Load Balancer, au lieu de la politique par défaut `ELBSecurityPolicy-2016-08`. Les politiques les plus récentes nécessitent au minimum le protocole TLS 1.2, la confidentialité directe et des chiffrements performants compatibles avec les navigateurs Web modernes.

Pour plus d'informations sur les politiques de sécurité disponibles pour les points de terminaison publics HTTPS, veuillez consulter :

- Politiques de sécurité SSL prédéfinies pour les Classic Load Balancers (documentation Elastic Load Balancing)
- Security policies for your Application Load Balancer (documentation Elastic Load Balancing)
- Protocoles et chiffrements pris en charge entre les lecteurs et CloudFront (documentation) CloudFront

WKLD.14 Utiliser des services de protection des bords pour les terminaux publics

Plutôt que de gérer le trafic directement à partir de services informatiques tels que des EC2 instances ou des conteneurs, utilisez un service de protection des bords. Cela fournit un niveau de sécurité supplémentaire entre le trafic entrant en provenance d'Internet et les ressources qui desservent ce trafic. Ces services peuvent filtrer le trafic indésirable, appliquer le chiffrement et appliquer des règles de routage ou autres, telles que l'équilibrage de charge, avant que le trafic n'atteigne vos ressources internes.

AWS les services qui peuvent fournir une protection des points de terminaison publics incluent Elastic Load Balancing, API Gateway et Amplify Hosting. AWS WAF CloudFront Exécutez des services basés sur VPC, tels qu'Elastic Load Balancing, dans un sous-réseau public en tant que proxy pour les ressources de service Web s'exécutant dans un sous-réseau privé.

CloudFront, API Gateway et Amazon Route 53 offrent une protection gratuite contre les attaques par déni de service (DDoS) distribué (S) des couches 3 et 4 et AWS WAF peuvent protéger contre les attaques de couche 7.

Les instructions pour démarrer avec chacun de ces services sont disponibles ici :

- Commencer avec AWS WAF (AWS site Web)
- Commencer à utiliser Amazon CloudFront (CloudFront documentation)

- Démarrez avec Elastic Load Balancing (documentation Elastic Load Balancing)
- Mise en route avec API Gateway (documentation API Gateway)
- Getting started with Amplify Hosting (documentation Amplify)

WKLD.15 Définissez les contrôles de sécurité dans les modèles et déployez-les en utilisant les pratiques CI/CD

L'infrastructure en tant que code (IaC) est la pratique qui consiste à définir toutes vos ressources et configurations de services AWS dans les modèles et le code que vous déployez à l'aide de pipelines d'intégration continue et de livraison continue (CI/CD), les mêmes pipelines que ceux que vous utilisez pour déployer les applications logicielles. Les services IaC, tels que AWS CloudFormation, prennent en charge à la fois les politiques basées sur l'identité IAM et les politiques basées sur les ressources et prennent en charge les services AWS de sécurité tels qu'Amazon GuardDuty et AWS WAF Amazon VPC. Capturez ces artefacts sous forme de modèles IaC, validez les modèles dans un référentiel de code source, puis déployez-les à l'aide de pipelines CI/CD.

Sauf indication contraire, validez les politiques d'autorisation des applications avec le code de l'application dans le même référentiel, et gérez les politiques de ressources générales et les configurations des services de sécurité dans des référentiels de code et des pipelines de déploiement distincts.

Pour plus d'informations sur la prise en main d' AWS iAc activé, consultez la AWS Cloud Development Kit (AWS CDK) documentation.

Collaborateurs

Les personnes qui ont contribué à ce document incluent :

- Jay Michael, architecte de solutions principal (auteur principal)
- Cole Calistra, Principal Solutions Architect
- Justin Plock, Principal Solutions Architect
- Faisal Farooq, Solutions Architect
- Michael Nguyen, Senior Solutions Architect
- Ritik Khatwani, Sr. Solutions Architect
- Paul Hawkins, Principal, Office of the Chief Information Security Officer (CISO)

Nous remercions tout particulièrement les personnes suivantes, qui ont également contribué à l'élaboration et à la révision de ce document :

- Robert Put
- Mike Sullivan
- Bob Lee III

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
Paramètres du compartiment Amazon S3	Nous avons mis à jour la section ACCT.08 Empêcher l'accès public aux compartiments S3 privés pour indiquer que le paramètre Bloquer l'accès public aux compartiments Amazon S3 créés après le 28 avril 2023 est activé par défaut.	18 mai 2023
Bonnes pratiques de sécurité IAM	Nous avons mis à jour ce guide afin de l'aligner sur les meilleures pratiques AWS Identity and Access Management (IAM) les plus récentes. Pour plus d'informations, veuillez consulter Bonnes pratiques de sécurité dans la documentation IAM.	1er février 2023
Rôles IAM	Nous avons fourni des liens supplémentaires vers la Service AWS documentation dans la section WKLD.01 Utiliser les rôles IAM pour les autorisations d'environnement de calcul.	22 septembre 2022
Politique relative aux mots de passe	Nous avons mis à jour les recommandations relatives	10 mai 2022

	aux mots de passe forts afin de respecter les dernières directives du Center for Internet Security (CIS).	
Publication initiale	—	13 avril 2022

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

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

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

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

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

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCo E

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

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

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

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

administrateur délégué

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

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

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

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

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Voir reprise après sinistre.

détection de dérive

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

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

épopée

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

branche de fonctionnalités

Voir succursale.

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le modèle de fondation.

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiens

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l'identité

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

application inactive

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

IIo T

Voir Internet industriel des objets.

infrastructure immuable

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

VPC entrant (d'entrée)

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

migration incrémentielle

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

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

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

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

VPC d'inspection

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

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

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

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

lift and shift

Voir 7 Rs.

système de poids faible

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

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

Voir succursale.

malware

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

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir Migration Acceleration Program.

mécanisme

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

compte membre

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

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

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

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

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

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

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

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

confidentialité dès la conception

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

zones hébergées privées

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

contrôle proactif

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

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

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

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

CHIFFON

Voir Retrieval Augmented Generation.

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

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

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif relatif au temps de rétablissement.

runbook

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

S

SAML 2.0

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

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

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

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

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

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir environnement.

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

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

VER

Voir écrire une fois, lire plusieurs.

WQF

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

écrire une fois, lire plusieurs (WORM)

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

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

Z

exploit Zero-Day

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

vulnérabilité « jour zéro »

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

invite Zero-Shot

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

application zombie

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

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