Mise en œuvre de contrôles de sécurité sur AWS

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Mise en œuvre de contrôles de sécurité sur AWS

Table of Contents

Implémentation de contrôles de sécurité sur AWS

Iqbal Umair, Gurpreet Kaur Cheema, Wasim Hossain, Joseph Nguyen, San Brar et Lucia Vanta, Amazon Web Services (AWS)

Décembre 2023 (historique du document)

La sécurité est essentielle pour toutes les entreprises et elle constitue un pilier essentiel du cadre AWS Well-Architected. Cependant, nombreux sont ceux qui ne savent pas comment aborder les questions de sécurité et créer une stratégie globale de test de sécurité et de correction automatisée pour leurs environnements cloud. Grâce aux Services AWS et à des outils tels qu'AWS Config, Amazon GuardDuty et AWS CloudFormation, vous pouvez créer une stratégie de test de sécurité et l'intégrer à vos environnements AWS Cloud.

Pour vous aider à respecter la politique et les normes de sécurité de votre entreprise, les contrôles de sécurité sont les barrières de protection techniques ou administratives qui permettent de prévenir, de détecter ou de réduire la capacité d'un acteur malveillant à exploiter une vulnérabilité de sécurité. Ils sont conçus pour protéger la confidentialité, l'intégrité et la disponibilité des ressources et des données. Voici des exemples de contrôles de sécurité :

- Implémentation de l'authentification multifactorielle pour les utilisateurs qui doivent se connecter à une application
- Actions de journalisation, de surveillance et d'interrogation dans le but d'effectuer des audits en temps réel de l'activité du compte
- S'assurer que les données sensibles sont chiffrées
- S'assurer que les journaux sont stockés conformément à la politique de conservation de votre entreprise

Il existe quatre types de contrôle de sécurité : préventif, proactif, de détection et réactif. Ce guide décrit chaque type de manière plus détaillée et met l'accent sur la manière d'implémenter et d'automatiser ces contrôles dans le AWS Cloud. Ce guide vous aide à mettre en œuvre des contrôles de sécurité continus et proactifs.

Public visé

Ce guide est destiné aux architectes et aux ingénieurs de sécurité chargés d'implémenter les contrôles de sécurité dans le AWS Cloud. Si votre entreprise n'a pas défini de politique de sécurité,

d'objectifs de contrôle ou de normes, comme décrit dans Contrôles de sécurité dans le cadre de gouvernance, nous vous recommandons de mener à bien ces tâches de gouvernance avant de poursuivre ce guide.

Résultats commerciaux ciblés

Les entreprises utilisent des contrôles de sécurité pour atténuer les risques liés à leurs systèmes informatiques ou pour servir de contre-mesures. Les contrôles définissent la référence des exigences pour satisfaire les principaux objectifs de sécurité d'un programme informatique et de sa stratégie de sécurité. La mise en place de contrôles améliore le niveau de sécurité d’une entreprise en protégeant la confidentialité, l’intégrité et la disponibilité de ses données et de ses actifs informatiques. Sans contrôles, il serait difficile de savoir où il convient de se concentrer et d’investir pour établir une référence en matière de sécurité.

Les contrôles de sécurité peuvent être utilisés pour faire face à divers scénarios. Les exemples incluent le respect des exigences découlant des évaluations des risques, le respect des normes du secteur ou le respect des réglementations. Des contrôles de sécurité satisfaisants démontrent que vous avez mesuré le risque concernant un système, déterminé le niveau de protection nécessaire et implémenté des solutions de manière proactive. D'autres facteurs, tels que l'activité, le secteur d'activité et la géographie, peuvent tous dicter les contrôles de sécurité dont vous avez besoin.

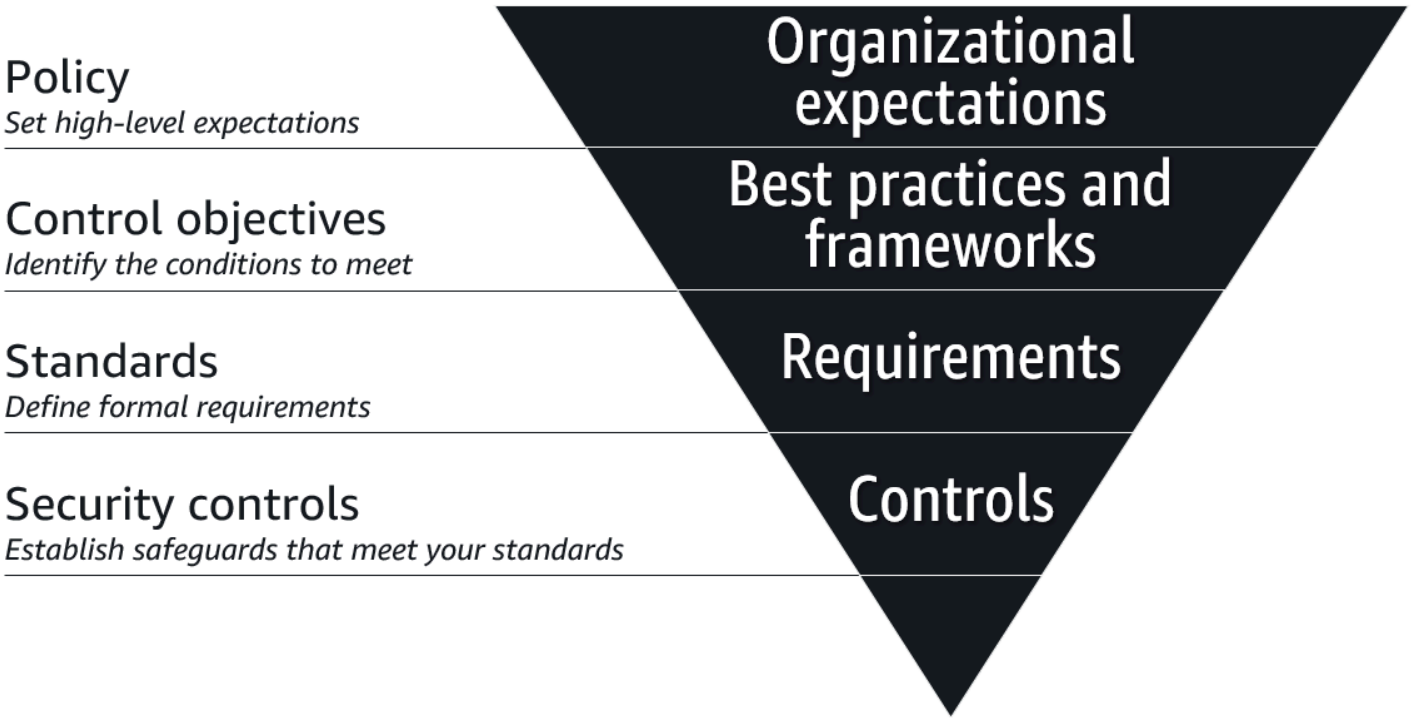
Voici des cas d'utilisation courants pour l'implémentation de contrôles de sécurité :

- Une évaluation de la sécurité d'une application a identifié le besoin de contrôler les accès en fonction de la sensibilité des données traitées.
- Vous devez respecter les normes de sécurité, telles que la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), la loi HIPAA (Health Insurance Portability and Accountability Act) ou le National Institute of Standards and Technology (NIST).
- Vous devez protéger les informations sensibles pour les transactions métier.
- Votre entreprise s'est développée dans une région géographique qui nécessite des contrôles de sécurité, telle qu'une région qui exige le respect du règlement général sur la protection des données (RGPD).

Après avoir lu ce guide, vous devriez être familiarisé avec les quatre types de contrôle de sécurité, comprendre en quoi ils font partie de votre cadre de gouvernance de la sécurité et être prêt à commencer à implémenter et à automatiser les contrôles de sécurité dans l’AWS Cloud.

Contrôles de sécurité dans le cadre de gouvernance

Il est important de planifier à partir du niveau de base. Comment commencer ? L'illustration suivante montre comment élaborer une stratégie de gouvernance de la sécurité basée sur une stratégie, des objectifs de contrôle, des normes et des contrôles de sécurité.



Les éléments hiérarchiques d'une stratégie de gouvernance en matière de sécurité sont les suivants :

- Politique : une stratégie est la base de toute stratégie de gouvernance de la cybersécurité. Il s'agit d'un document qui énonce les attentes de l'entreprise, telles que les obligations légales, réglementaires ou contractuelles auxquelles elle doit répondre. Les politiques peuvent varier selon le secteur d'activité et la région.
- Objectifs de contrôle : les objectifs de contrôle sont des cibles, telles que les bonnes pratiques reconnues par le secteur, qui vous aident à atteindre l'objectif défini par une politique. Pour le cloud computing, de nombreuses entreprises adoptent la Cloud Controls Matrix (CCM) (site Web de Cloud Security Alliance), qui est un cadre d'objectifs de contrôle de la cybersécurité.
- Normes : les normes sont des exigences officiellement établies qui répondent à un objectif de contrôle. Les normes peuvent inclure des processus, des actions ou des configurations, et elles sont quantifiables afin que vous puissiez mesurer les performances par rapport à la norme.

- Contrôles de sécurité : les contrôles de sécurité sont les mécanismes techniques ou administratifs que vous mettez en place pour implémenter les normes. Tous les contrôles de sécurité correspondent aux normes, mais toutes les normes ne correspondent pas aux contrôles de sécurité. Les tests des contrôles de sécurité sont conçus pour surveiller et mesurer votre capacité à respecter les normes définies.

Ce guide explique comment concevoir et implémenter des types de contrôles de sécurité courants dans le AWS Cloud.

Types de contrôles de sécurité

Il existe quatre principaux types de contrôle de sécurité :

- Contrôles préventifs : ces contrôles sont conçus pour empêcher qu'un événement ne se produise.
- Contrôles proactifs : ces contrôles visent à empêcher la création de ressources non conformes.
- Contrôles de détection : ces contrôles sont conçus pour détecter, journaliser et alerter après la survenue d'un événement.
- Contrôles réactifs : ces contrôles sont conçus pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence en matière de sécurité.

Une stratégie de sécurité efficace inclut les quatre types de contrôle de sécurité. Bien que les contrôles préventifs constituent une première ligne de défense pour empêcher les accès non autorisés ou les modifications indésirables apportées à votre réseau, il est important de vous assurer de mettre en place des contrôles de détection et réactifs afin de savoir quand un événement se produit et de prendre les mesures immédiates et appropriées pour y remédier. L'utilisation de contrôles proactifs ajoute une couche de sécurité, car elle s'ajoute aux contrôles préventifs, qui sont généralement plus stricts par nature.

Les sections suivantes décrivent chaque type de contrôle plus en détail. Ils traitent des objectifs, du processus d'implémentation, des cas d'utilisation, des considérations technologiques et des résultats visés de chaque type de contrôle.

Contrôles préventifs

Les contrôles préventifs sont des contrôles de sécurité conçus pour empêcher qu'un événement ne se produise. Ces barrières de protection constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Un rôle AWS Identity and Access Management (IAM) doté d'un accès en lecture seule est un exemple de contrôle préventif, car il permet d'empêcher les actions d'écriture involontaires de la part d'utilisateurs non autorisés.

Examinez les points suivants concernant ce type de contrôle :

- Objectifs
- Processus
- Cas d'utilisation

- Technologie
- Résultats métier

Objectifs

L'objectif principal des contrôles préventifs est de minimiser ou d'éviter la probabilité qu'un événement menaçant se produise. Le contrôle doit aider à empêcher tout accès non autorisé au système et que des modifications involontaires n'affectent le système. Les objectifs des contrôles préventifs sont les suivants :

- Séparation des tâches : les contrôles préventifs peuvent établir des limites logiques qui limitent les privilèges, en autorisant uniquement l'exécution de tâches spécifiques dans des comptes ou des environnements désignés. En voici quelques exemples :
  - Segmentation des charges de travail entre différents comptes pour des services spécifiques
  - Séparation et comptes dans des environnements de production, de développement et de test isolés
  - Délégation de l'accès et des responsabilités à plusieurs entités pour exécuter des fonctions spécifiques, telles que l'utilisation de rôles IAM ou de rôles endossés pour autoriser uniquement des fonctions spécifiques à effectuer certaines actions
- Contrôle d'accès : les contrôles préventifs peuvent systématiquement accorder ou refuser l'accès aux ressources et aux données de l'environnement. En voici quelques exemples :
  - Prévention des dépassements d’autorisation par les utilisateurs, connus sous le nom d’escalade de privilèges
  - Restreindre l'accès aux applications et aux données uniquement aux utilisateurs et aux services autorisés
  - Maintien d’un groupe d’administrateurs restreint
  - Prévention de l’utilisation des informations d’identification de l’utilisateur root
- Exécution : les contrôles préventifs peuvent aider votre entreprise à respecter ses politiques, directives et normes. En voici quelques exemples :
  - Verrouiller les configurations servant de référence de sécurité minimale
  - Implémenter des mesures de sécurité supplémentaires, telles que l'authentification multifactorielle
  - Éviter les tâches et les actions non standard exécutées par des rôles non approuvés

Processus

Le mappage des contrôles préventifs est le processus qui consiste à mapper les contrôles aux exigences et à utiliser des politiques pour implémenter ces contrôles en les restreignant, en les désactivant ou en les bloquant. Lorsque vous mappez les contrôles, tenez compte de l'effet proactif qu'ils ont sur l'environnement, les ressources et les utilisateurs. Les bonnes pratiques en matière de mappage des contrôles sont les suivantes :

- Les contrôles stricts qui interdisent une activité doivent être mappés aux environnements de production où l'action nécessite des processus d'examen, d'approbation et de modification.
- Les environnements de développement ou confinés peuvent présenter moins de contrôles préventifs afin de fournir l'agilité nécessaire à la génération et aux tests.
- La classification des données, le niveau de risque d'un actif et la politique de gestion des risques dictent les contrôles préventifs.
- Mappez aux cadres existants afin de démontrer la conformité aux normes et aux réglementations.
- Implémentez des contrôles préventifs en fonction de l'emplacement géographique, de l'environnement, des comptes, des réseaux, des utilisateurs, des rôles ou des ressources.

Cas d’utilisation

Manipulation des données

Un rôle est créé pour accéder à toutes les données d'un compte. S’il existe des données sensibles et chiffrées, des privilèges trop permissifs peuvent présenter un risque, selon les utilisateurs ou les groupes susceptibles d’endosser le rôle. En utilisant une politique de clé dans AWS Key Management Service (AWS KMS), vous pouvez contrôler qui a accès à la clé et peut déchiffrer les données.

Escalade de privilèges

Si les autorisations d'administration et d'écriture sont attribuées avec trop de souplesse, un utilisateur peut contourner les limites des autorisations prévues et s'octroyer des privilèges supplémentaires. L'utilisateur qui crée et gère un rôle peut attribuer une limite des autorisations qui définit les privilèges maximum admissibles pour le rôle.

Confinement de la charge de travail

Si votre entreprise n'a pas de besoin prévisible d'utiliser des services spécifiques, activez une politique de contrôle des services qui limite les services pouvant fonctionner sur les comptes des

membres d'une organisation ou restreint les services en fonction du Région AWS. Ce contrôle préventif peut réduire la portée de l'impact si un acteur malveillant parvient à compromettre un compte de votre organisation et à y accéder. Pour plus d'informations, consultez Politiques de contrôle des services dans ce guide.

Incidence sur les autres applications

Les contrôles préventifs peuvent imposer l'utilisation de services et de fonctionnalités, comme IAM, le chiffrement et la journalisation, afin de répondre aux exigences de sécurité de vos applications. Vous pouvez également utiliser ces contrôles pour vous protéger contre les vulnérabilités en limitant les actions qu'un acteur malveillant peut exploiter en raison d'erreurs involontaires ou d'une mauvaise configuration.

Technologie

Politiques de contrôle des services

Dans AWS Organizations, les politiques de contrôle des services (SCP) définissent les autorisations maximales disponibles pour les comptes des membres d'une organisation. Ces politiques contribuent à ce que les comptes respectent les directives de contrôle d'accès de l'organisation. Tenez compte des points suivants lorsque vous concevez des SCP pour votre organisation :

- Les SCP sont des contrôles préventifs car ils définissent et appliquent les autorisations maximales autorisées pour les rôles et les utilisateurs IAM dans les comptes membres de l'organisation.
- Les SCP affectent uniquement les rôles et les utilisateurs IAM dans les comptes membres de l'organisation. Elles n'ont aucune incidence sur des utilisateurs ou des rôles dans le compte de gestion de l'organisation.

Vous pouvez faire en sorte qu'une SCP soit plus détaillée en définissant les autorisations maximales pour chaque Région AWS.

Limites d'autorisations IAM

Dans AWS Identity and Access Management (IAM), une limite d'autorisations est utilisée pour définir le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateurs ou rôles). La limite des autorisations d'une entité lui permet d'effectuer uniquement les actions autorisées à la fois par ses politiques basées sur l'identité et ses limites des autorisations. Notez les points suivants en ce qui concerne l'utilisation des limites des autorisations :

- Vous pouvez utiliser une politique AWS gérée ou une politique gérée par le client pour définir les limites d'une entité IAM.
- Une limite d'autorisations restreint le nombre maximum d'autorisations, mais n'accorde pas seule l'accès. La politique de limite des autorisations limite les autorisations accordées à l'entité IAM.

Résultats métier

Gains de temps

- En ajoutant l’automatisation après avoir configuré les contrôles préventifs, vous pouvez réduire le besoin d’intervention manuelle et la fréquence des erreurs.
- L’utilisation des limites des autorisations comme contrôle préventif permet aux équipes de sécurité et IAM de se concentrer sur les tâches critiques, telles que la gouvernance et l’assistance.

Conformité aux réglementations

- Les entreprises peuvent avoir besoin de se conformer aux réglementations internes ou sectorielles. Il peut s’agir de restrictions régionales, de restrictions relatives aux utilisateurs et aux rôles ou de restrictions de service. Les SCP peuvent vous aider à rester en conformité et à éviter les sanctions en cas de violation.

Réduction des risques

- Avec la croissance, le nombre de demandes de création et de gestion de nouveaux rôles et de nouvelles politiques augmente. Il devient de plus en plus difficile de comprendre le contexte de ce qui est requis pour créer manuellement les autorisations pour chaque application. La mise en place de contrôles préventifs constitue une référence et permet d'empêcher les utilisateurs d'effectuer des actions involontaires, même s'ils y ont été accidentellement autorisés.
- L'application de contrôles préventifs aux politiques d'accès constitue une couche supplémentaire pour protéger les données et les actifs.

Contrôles proactifs

Les contrôles proactifs sont des contrôles de sécurité visant à empêcher la création de ressources non conformes. Ces contrôles peuvent réduire le nombre d’événements de sécurité gérés par des

contrôles réactifs et de détection. Ces contrôles garantissent la conformité des ressources déployées avant leur déploiement. Par conséquent, aucun événement de détection ne nécessite une réponse ou une correction.

Par exemple, vous pouvez avoir mis en place un contrôle de détection qui vous avertit si un compartiment Amazon Simple Storage Service (Amazon S3) devient accessible au public. Vous pouvez également disposer d'un contrôle réactif qui y apporte une solution. Bien que vous ayez déjà mis en place ces deux contrôles, vous pouvez ajouter une couche de protection supplémentaire en introduisant un contrôle proactif. Grâce à AWS CloudFormation ce contrôle proactif, vous pouvez empêcher la création ou la mise à jour de tout compartiment S3 dont l'accès public est activé. Les acteurs de la menace pourraient toujours contourner ce contrôle et déployer ou modifier des ressources en dehors de CloudFormation. Dans ce cas, les contrôles de détection et réactifs corrigeraient l'événement de sécurité.

Examinez les points suivants concernant ce type de contrôle :

- Objectifs
- Processus
- Cas d'utilisation
- Technologie
- Résultats métier

Objectifs

- Les contrôles proactifs vous aident à améliorer les opérations de sécurité et les processus de qualité.
- Les contrôles proactifs peuvent vous aider à respecter les politiques de sécurité, les normes et les obligations réglementaires ou de conformité.
- Les contrôles proactifs peuvent empêcher la création de ressources non conformes.
- Les contrôles proactifs peuvent réduire le nombre de résultats de sécurité.
- Les contrôles proactifs fournissent une couche de protection supplémentaire contre les acteurs malveillants qui contournent les contrôles préventifs et qui tentent de déployer des ressources non conformes.
- Associés à des contrôles préventifs, de détection et réactifs, les contrôles proactifs peuvent vous aider à faire face aux incidents de sécurité potentiels.

Processus

Les contrôles proactifs complètent les contrôles préventifs. Les contrôles proactifs réduisent les risques de sécurité de votre organisation et appliquent le déploiement de ressources conformes. Ces contrôles évaluent la conformité des ressources avant leur création ou leur mise à jour. Les contrôles proactifs sont généralement mis en œuvre à l'aide de CloudFormation crochets. Si la ressource échoue à la validation du contrôle proactif, vous pouvez choisir de mettre en échec le déploiement de la ressource ou d'afficher un message d'avertissement. Voici quelques conseils et bonnes pratiques pour créer des contrôles proactifs :

- Assurez-vous que les contrôles proactifs sont mappés aux exigences de conformité de votre organisation.
- Assurez-vous que les contrôles proactifs respectent les bonnes pratiques de sécurité pour le service associé.
- Utilisez CloudFormation StackSets une autre solution pour déployer des contrôles proactifs sur plusieurs Régions AWS comptes.
- Assurez-vous que le message d'avertissement ou d'échec associé à un contrôle proactif est suffisamment clair et explicite. Cela permet aux développeurs de comprendre pourquoi la ressource n'a pas satisfait à l'évaluation.
- Lorsque vous créez des contrôles proactifs, commencez en mode observation. Cela signifie que vous envoyez un message d'avertissement au lieu de mettre en échec le déploiement des ressources. Vous pouvez ainsi mieux comprendre l'impact d'un contrôle proactif.
- Activez la connexion à Amazon CloudWatch Logs pour des contrôles proactifs.
- Si vous devez surveiller l'invocation d'un contrôle proactif spécifique, utilisez une EventBridge règle Amazon et abonnez-vous aux événements d'invocation pour le CloudFormation hook.

Cas d'utilisation

- Prévention du déploiement de ressources non conformes
- Respect des exigences en matière de conformité
- Amélioration de la qualité du code en appliquant la résolution d'un problème de sécurité avant le déploiement
- Réduction des interruptions de service associées à la résolution des problèmes de sécurité après le déploiement

Technologie

CloudFormation crochets

AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions. CloudFormation les hooks évaluent de manière proactive la configuration de vos CloudFormation ressources avant leur déploiement. Si des ressources non conformes sont détectées, ils renvoient un état d'échec. En fonction du mode de défaillance du hook, l'opération CloudFormation peut échouer ou présenter un avertissement permettant à l'utilisateur de poursuivre le déploiement. Vous pouvez utiliser les hooks disponibles ou développer les vôtres.

AWS Control Tower

AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives. AWS Control Tower propose des commandes proactives préconfigurées que vous pouvez activer dans votre zone d'atterrissage. Si votre zone de landing zone est configurée à l'aide de ces contrôles proactifs optionnels AWS Control Tower, vous pouvez utiliser ces contrôles proactifs optionnels comme point de départ pour votre organisation. Vous pouvez intégrer des contrôles proactifs personnalisés supplémentaires CloudFormation selon vos besoins.

Résultats métier

Moins d'efforts humains et d'erreurs humaines

Les contrôles proactifs réduisent le risque d'erreur humaine qui entraîne le déploiement de ressources non conformes. Ils réduisent également l'effort humain plus loin dans le cycle de développement, car ils obligent les développeurs à prendre en compte la sécurité des ressources avant le déploiement. Cela applique la pratique du décalage gauche à la création de ressources sécurisées, en imposant la conformité plus tôt dans le cycle de vie du développement.

Réduction des coûts

Il est généralement plus coûteux de corriger un problème de sécurité après le déploiement. L'identification et la résolution des problèmes plus tôt dans le cycle de développement réduisent les coûts de développement.

Gains de temps

Dans la mesure où les contrôles proactifs empêchent le déploiement de ressources non conformes, ils réduisent le temps que vous passez à trier et à corriger les problèmes de sécurité. Ils indiquent également le nombre de résultats de sécurité, que les contrôles de détection identifieraient plus tard dans le cycle de développement.

Conformité aux réglementations

Si votre organisation doit se conformer à des réglementations internes ou sectorielles, des contrôles proactifs peuvent vous aider à assurer votre conformité et à éviter les sanctions en cas de violation.

Réduction des risques

Les contrôles proactifs aident les développeurs à déployer des ressources conformes et plus sécurisées, de manière à réduire les risques de sécurité de votre organisation.

Contrôles de détection

Les contrôles de détection sont des contrôles de sécurité conçus pour détecter, journaliser et alerter après la survenue d'un événement. Les contrôles de détection constituent un élément fondamental des cadres de gouvernance. Ces barrières de protection constituent une deuxième ligne de défense, en vous signalant les problèmes de sécurité qui ont contourné les contrôles préventifs.

Par exemple, vous pouvez appliquer un contrôle de détection qui détecte et vous avertit si un compartiment Amazon Simple Storage Service (Amazon S3) devient accessible au public. Bien que vous ayez mis en place des contrôles préventifs qui empêchent l'accès public aux compartiments S3 au niveau du compte, puis désactivent l'accès via des SCP, un acteur malveillant peut contourner ces contrôles préventifs en se connectant en tant qu'utilisateur administratif. Dans ces situations, un contrôle de détection peut vous avertir de la mauvaise configuration et de la menace potentielle.

Examinez les points suivants concernant ce type de contrôle :

- Objectifs
- Processus
- Cas d’utilisation
- Technologie
- Résultats métier

Objectifs

- Les contrôles de détection vous aident à améliorer les processus opérationnels de sécurité et les processus de qualité.
- Les contrôles de détection vous aident à respecter les obligations réglementaires, légales ou de conformité.
- Les contrôles de détection offrent aux équipes chargées des opérations de sécurité la visibilité nécessaire pour répondre aux problèmes de sécurité, notamment aux menaces avancées qui contournent les contrôles préventifs.
- Les contrôles de détection peuvent vous aider à identifier la réponse appropriée aux problèmes de sécurité et aux menaces potentielles.

Processus

Vous implémentez des contrôles de détection mis en œuvre en deux phases. Tout d'abord, vous configurez le système pour enregistrer les événements et les états des ressources dans un emplacement centralisé, tel qu'Amazon CloudWatch Logs. Une fois la journalisation centralisée en place, vous analysez ces journaux pour détecter les anomalies susceptibles d'indiquer une menace. Chaque analyse est un contrôle qui est mappé à vos exigences et politiques d'origine. Par exemple, vous pouvez créer un contrôle de détection qui recherche dans les journaux un modèle spécifique et génère une alerte en cas de correspondance. Les contrôles de détection sont utilisés par les équipes de sécurité pour améliorer leur visibilité globale sur les menaces et les risques auxquels leur système peut être exposé.

Cas d’utilisation

Détection de comportements suspects

Les contrôles de détection permettent d'identifier toute activité anormale, telle que la compromission des informations d'identification d'un utilisateur privilégié ou l'accès à des données sensibles ou leur exfiltration. Ces contrôles sont des facteurs réactifs importants qui peuvent aider votre entreprise à identifier et à comprendre l'ampleur des activités anormales.

Détection de la fraude

Ces contrôles permettent de détecter et d'identifier une menace au sein de votre entreprise, telle qu'un utilisateur qui contourne les politiques et qui effectue des transactions non autorisées.

Conformité d'

Les contrôles de détection vous aident à respecter des exigences de conformité, telles que la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), et peuvent contribuer à prévenir des usurpations d'identité. Ces contrôles peuvent vous aider à découvrir et à protéger les informations sensibles soumises à la conformité réglementaire, telles que les informations personnelles identifiables.

Analyse automatisée

Les contrôles de détection peuvent analyser automatiquement les journaux pour détecter les anomalies et autres indicateurs d'activité non autorisée.

Vous pouvez analyser automatiquement les journaux provenant de différentes sources telles que les journaux AWS CloudTrail , le journal de flux VPC et des journaux de système de nom de domaine (DNS), pour détecter des activités potentiellement malveillantes. Pour faciliter l'organisation, regroupez les alertes de sécurité ou les résultats de plusieurs Services AWS sites vers un emplacement centralisé.

Technologie

Un contrôle de détection courant consiste à implémenter un ou plusieurs services de surveillance capables d'analyser les sources de données, telles que les journaux, afin d'identifier les menaces de sécurité. Vous pouvez y analyser des AWS Cloud sources telles que les AWS CloudTrail journaux, les journaux d'accès Amazon S3 et les journaux de flux Amazon Virtual Private Cloud pour détecter les activités inhabituelles. AWS les services de sécurité tels qu'Amazon GuardDuty, Amazon Detective et Amazon Macie disposent de fonctionnalités de surveillance intégrées. AWS Security Hub

GuardDuty et Security Hub

Amazon GuardDuty utilise des techniques de renseignement sur les menaces, d'apprentissage automatique et de détection d'anomalies pour surveiller en permanence les sources de vos journaux afin de détecter toute activité malveillante ou non autorisée. Le tableau de bord fournit des informations sur l'état en temps réel de votre charge de travail Comptes AWS et de votre charge de travail. Vous pouvez intégrer un service GuardDuty de AWS Security Hubgestion de la posture de sécurité dans le cloud qui vérifie le respect des meilleures pratiques, regroupe les alertes et permet des mesures correctives automatisées. GuardDuty envoie les résultats à Security Hub afin de centraliser les informations. Vous pouvez intégrer davantage Security Hub aux solutions de gestion

des informations et des événements de sécurité (SIEM) afin d'étendre les capacités de surveillance et d'alerte de votre entreprise.

Macie

Amazon Macie est un service totalement géré de sécurité et de confidentialité des données qui utilise le machine learning et la correspondance de modèles pour détecter et protéger les données sensibles dans AWS. Vous trouverez ci-dessous certaines des commandes et des fonctionnalités de détection disponibles dans Macie :

- Macie inspecte l'inventaire des compartiments et tous les objets stockés dans Amazon S3. Ces informations peuvent être présentées dans une vue de tableau de bord unique, pour ainsi vous offrir de la visibilité et vous aider à évaluer la sécurité des compartiments.
- Pour découvrir les données sensibles, Macie utilise des identifiants de données intégrés et gérés et prend également en charge les identifiants de données personnalisés.
- Macie s'intègre nativement aux autres outils Services AWS et outils. Par exemple, Macie publie ses résultats sous forme d' EventBridge événements Amazon, qui sont automatiquement envoyés à Security Hub.

Les bonnes pratiques pour configurer des contrôles de détection dans Macie sont les suivantes :

- Activez Macie sur tous les comptes. En utilisant la fonctionnalité de gestion déléguée, activez Macie sur plusieurs comptes avec AWS Organizations.
- Utilisez Macie pour évaluer la sécurité des compartiments S3 de vos comptes. Cela permet d'éviter les pertes de données en fournissant une visibilité sur l'emplacement des données et l'accès aux données. Pour plus d'informations, veuillez consulter Analyzing your Amazon S3 security posture (documentation Macie).
- Automatisez la découverte des données sensibles dans vos compartiments S3 en exécutant et en planifiant des tâches de traitement et de découverte de données automatisées. Cela permet d'inspecter régulièrement les compartiments S3 pour détecter la présence de données sensibles.

AWS Config

AWS Configvérifie et enregistre la conformité des AWS ressources. AWS Config découvre les AWS ressources existantes et génère un inventaire complet, ainsi que les détails de configuration de chaque ressource. En cas de modifications de la configuration, il les enregistre et envoie une

notification. Cela peut vous aider à détecter et à annuler les modifications non autorisées de l'infrastructure. Vous pouvez utiliser des règles AWS gérées et créer des règles personnalisées.

Les bonnes pratiques pour configurer des contrôles de détection dans AWS Config sont les suivantes :

- Activez Région AWS cette option AWS Config pour chaque compte membre de l'organisation et pour chaque compte contenant des ressources que vous souhaitez protéger.
- Configurez des alertes Amazon Simple Notification Service (Amazon SNS) pour toute modification de la configuration.
- Stockez des données de configuration dans un compartiment S3 et utilisez Amazon Athena pour les analyser.
- Automatisez la correction des ressources non conformes en utilisant Automation, une fonctionnalité d' AWS Systems Manager.
- Utilisez EventBridge Amazon SNS pour configurer les notifications relatives aux ressources non AWS conformes.

Trusted Advisor

AWS Trusted Advisor peut être utilisé comme service pour les contrôles de détection. Grâce à un ensemble de contrôles, Trusted Advisor identifie les domaines dans lesquels vous pouvez optimiser votre infrastructure, améliorer les performances et la sécurité ou réduire les coûts. Trusted Advisor fournit des recommandations basées sur les AWS meilleures pratiques que vous pouvez suivre pour améliorer vos services et vos ressources. Les plans Business et Enterprise Support donnent accès à tous les chèques disponibles pour les piliers du AWS Well-Architected Framework.

Les bonnes pratiques pour configurer des contrôles de détection dans Trusted Advisor sont les suivantes :

- Consulter le résumé au niveau des contrôles
- Implémentez des recommandations propres aux ressources pour les états d'avertissement et d'erreur.
- Vérifiez Trusted Advisor fréquemment pour examiner activement et mettre en œuvre ses recommandations.

Amazon Inspector

Amazon Inspector est un service automatisé de gestion des vulnérabilités qui, après avoir été activé, analyse continuellement vos charges de travail pour détecter les vulnérabilités logicielles et l'exposition involontaire du réseau. Il contextualise les résultats sous forme d'un score de risque qui peut vous aider à déterminer les prochaines étapes, telles que la correction ou la confirmation de l'état de conformité.

Les bonnes pratiques pour configurer des contrôles de détection dans Amazon Inspector sont les suivantes :

- Activez Amazon Inspector sur tous les comptes EventBridge et intégrez-le à Security Hub pour configurer les rapports et les notifications en cas de failles de sécurité.
- Priorisez les mesures correctives et les autres actions en fonction du score de risque d'Amazon Inspector.

Résultats métier

Moins d'efforts humains et d'erreurs humaines

Vous pouvez parvenir à l'automatisation en utilisant l'infrastructure en tant que code (IaC). L'automatisation du déploiement, ainsi que de la configuration des services et des outils de surveillance et de correction réduit le risque d'erreurs manuelles, mais aussi le temps et les efforts nécessaires pour mettre à l'échelle ces contrôles de détection. L'automatisation facilite le développement de runbooks de sécurité et réduit les opérations manuelles pour les analystes de sécurité. Des examens réguliers permettent d'ajuster les outils d'automatisation, mais aussi d'itérer et d'améliorer en permanence les contrôles de détection.

Mesures appropriées contre les menaces potentielles

La capture et l'analyse des événements à partir des journaux et des métriques sont cruciales pour gagner en visibilité. Cela permet aux analystes de prendre des mesures en cas d'événements de sécurité et de menaces potentielles afin de sécuriser vos charges de travail. La capacité d'identifier rapidement les vulnérabilités existantes aide les analystes à prendre les mesures appropriées pour y remédier.

Meilleure réponse aux incidents et meilleure gestion des enquêtes

L'automatisation des outils de contrôle de détection peut augmenter la vitesse de détection, d'investigation et de restauration. Les alertes et notifications automatisées basées sur des conditions définies permettent aux analystes de sécurité d'enquêter et de réagir de manière appropriée. Ces facteurs réactifs peuvent vous aider à identifier et à comprendre l'ampleur d'une activité anormale.

Contrôles réactifs

Les contrôles réactifs sont des contrôles de sécurité conçus pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Des exemples de contrôles réactifs techniques incluent l'application de correctifs à un système, la mise en quarantaine d'un virus, l'arrêt d'un processus ou le redémarrage d'un système.

Examinez les points suivants concernant ce type de contrôle :

- Objectifs
- Processus
- Cas d’utilisation
- Technologie
- Résultats métier

Objectifs

- Les contrôles réactifs peuvent vous aider à créer des runbooks pour les types d'attaque les plus courants, tels que l'hameçonnage ou la force brute.
- Les contrôles réactifs peuvent implémenter des réponses automatisées aux problèmes de sécurité potentiels.
- Les contrôles réactifs peuvent corriger automatiquement les actions involontaires ou non approuvées sur les AWS ressources, telles que la suppression de compartiments S3 non chiffrés.
- Les contrôles réactifs peuvent être orchestrés pour fonctionner avec des contrôles préventifs et de détection en vue de créer une approche globale et proactive visant à corriger les incidents de sécurité potentiels.

Processus

Les contrôles de détection sont indispensables à la mise en place de contrôles réactifs. Vous devez être en mesure de détecter le problème de sécurité avant de pouvoir le résoudre. Vous pouvez ensuite établir une politique ou une réponse au problème de sécurité. Par exemple, en cas d'attaque par force brute, un processus de correction serait implémenté. Une fois le processus de correction terminé, il peut être automatisé et exécuté sous forme de script à l'aide d'un langage de programmation, tel qu'un script shell.

Déterminez si le contrôle réactif risque d'interrompre une charge de travail de production existante. Par exemple, si le contrôle de sécurité de détection est Les compartiments S3 ne doivent pas être accessibles au public et si la remédiation consiste à désactiver l'accès public à Amazon S3, cela peut avoir des conséquences importantes pour votre entreprise et ses clients. Si le compartiment S3 dessert un site Web public, la désactivation de l'accès public peut provoquer une panne. Les bases de données sont un exemple similaire. Si une base de données ne doit pas être accessible au public via Internet, la désactivation de l'accès public peut affecter la connectivité à l'application.

Cas d’utilisation

- Réponse automatique aux événements de sécurité détectés
- Correction automatique des vulnérabilités de sécurité détectées
- Contrôle de récupération automatisé pour réduire les temps d'arrêt opérationnels

Technologie

Security Hub

AWS Security Hubenvoie automatiquement tous les nouveaux résultats et toutes les mises à jour des résultats existants EventBridge sous forme d'événements. Vous pouvez également créer des actions personnalisées qui envoient des résultats sélectionnés et des informations sur les résultats à EventBridge. Vous pouvez configurer EventBridge pour répondre à chaque type d'événement. L'événement peut lancer une AWS Lambda fonction qui exécute l'action de correction.

AWS Config

AWS Configutilise des règles pour évaluer vos AWS ressources et vous aide à remédier aux ressources non conformes. AWS Config applique la correction à l'aide de l'AWS Systems Manager automatisation. Dans les documents d'automatisation, vous définissez les actions que vous souhaitez

effectuer sur les ressources AWS Config considérées comme non conformes. Après avoir créé des documents d'automatisation, vous pouvez les utiliser dans Systems Manager via AWS Management Console ou à l'aide d'API. Vous pouvez choisir de corriger manuellement ou automatiquement les ressources non conformes.

Résultats métier

Réduire les pertes de données

Après un incident de cybersécurité, l'utilisation de contrôles de sécurité réactifs peut aider à réduire les pertes de données et les dommages au niveau du système ou du réseau. Les contrôles réactifs peuvent également aider à restaurer les systèmes et processus métier critiques le plus rapidement possible, renforçant ainsi la résilience de vos charges de travail.

Réduire les coûts

L'automatisation réduit les coûts associés aux ressources humaines, car les membres de l'équipe n'ont pas à répondre manuellement aux incidents ou à les gérer d'une autre manière sur une case-by-case base.

Étapes suivantes

Après avoir lu ce guide, vous devriez être familiarisé avec les quatre types de contrôle de sécurité, comprendre en quoi ils font partie de votre cadre de gouvernance de la sécurité et être prêt à commencer à implémenter et à automatiser les contrôles de sécurité dans l'AWS Cloud. Pour en savoir plus, nous vous recommandons d'examiner les références incluses dans la section Ressources.

Nous vous recommandons également de procéder comme suit pour évaluer la sécurité de votre infrastructure cloud et commencer l'implémentation des contrôles de sécurité :

1. Activez et configurez AWS Security Hub. En tant que bonne pratique, nous vous recommandons d'activer les contrôles des normes disponibles. Pour plus d'informations, veuillez consulter Security standards and controls (documentation Security Hub).
2. Activez et configurez AWS Config. Pour plus d'informations, veuillez consulter Getting started (documentation AWS Config).
3. À l'aide d'Services AWS comme Security Hub, Amazon Macie, AWS Config, AWS Trusted Advisor et Amazon Inspector, évaluez votre organisation et votre infrastructure de compte, identifiez les domaines à améliorer, puis examinez les recommandations dans ces services. Utilisez la fonctionnalité de contrôle de sécurité de Security Hub pour générer un score de sécurité pour une norme de sécurité. Pour plus d'informations, consultez Determining security scores (documentation Security Hub).
4. Implémentez des contrôles de sécurité préventifs, proactifs, de détection et réactifs en fonction des améliorations identifiées.
5. Procédez à une évaluation de sécurité de suivi pour évaluer l'efficacité des contrôles de sécurité implémentés. Dans Security Hub, déterminez si le score de sécurité s'est amélioré. Effectuez une itération pour améliorer ou ajouter de nouveaux contrôles de sécurité.
6. Établissez une cadence régulière pour effectuer des évaluations de sécurité, par exemple une fois par an.

FAQ

Sur quoi dois-je me concentrer si je dispose de peu de temps et de ressources et si je ne peux pas implémenter tous ces types de contrôle ?

Nous recommandons d'implémenter AWS Security Hub. Security Hub utilise également un ensemble de contrôles de sécurité automatisés appelés norme Pratiques exemplaires en matière de sécurité de base AWS (documentation Security Hub). Il s'agit d'un ensemble de bonnes pratiques de sécurité soigneusement sélectionnées, géré par des experts en sécurité AWS. Vous pouvez exécuter ces contrôles standard soit en continu, chaque fois que des modifications sont apportées aux ressources associées, soit périodiquement, selon un calendrier régulier. Chaque contrôle possède un score de gravité spécifique pour vous aider à prioriser vos efforts de remédiation. Pour plus d'informations, veuillez consulter Running security checks (documentation Security Hub). Si vous utilisez AWS Control Tower, vous pouvez également consulter et choisir d’activer ses contrôles préventifs, de détection et proactifs.

Ressources

Documentation AWS

- AWS Security Reference Architecture (AWS SRA)
- Perspective Sécurité AWS CAF
- Bonnes pratiques pour la sécurité, l'identité et la conformité
- Automated Security Response sur AWS (Solution AWS)
  - Page d'accueil de la solution
  - Guide d'implémentation

Billets de blogs AWS

- Identity Guide – Preventive controls with AWS Identity – SCPs
- How to implement a read-only service control policy (SCP) for accounts in AWS Organizations
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment
- Maintain compliance using Service Control Policies and ensure they are always applied
- When and where to use IAM permissions boundaries
- Garantie de la sécurité et de la conformité des ressources de manière proactive grâce à des hooks AWS CloudFormation

Autres ressources

- Cloud Controls Matrix (CCM) (Cloud Security Alliance)
- Example permissions boundaries (GitHub)

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
Contrôles proactifs	Nous avons ajouté des informations sur les contrôles proactifs à ce guide, y compris la section Contrôles proactifs.	4 décembre 2023
Publication initiale	—	12 décembre 2022

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

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

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

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

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

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCoE

Voir le Centre d'excellence du cloud.

CDC

Consultez la section Capture des données de modification.

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant un modèle opérationnel)
- Migration : migration d'applications individuelles

- Réinvention : optimisation des produits et services et innovation dans le cloud

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

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, AWS Panorama propose des appareils qui ajoutent des CV aux réseaux de caméras locaux, et Amazon SageMaker fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes source, de génération, de test, intermédiaire et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

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

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte AWS membre pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est

appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique Services qui fonctionnent avec AWS Organizations dans la documentation AWS Organizations .

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Consultez la section Reprise après sinistre.

détection de dérive

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

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

informatique de périphérie

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

épopée

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

branche de fonctionnalités

Voir la succursale.

fonctionnalités

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

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes

techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec :AWS.

transformation de fonctionnalité

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

G

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation de l'historien

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

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

application inactive

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

IIoT

Voir Internet industriel des objets.

infrastructure immuable

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

VPC entrant (d'entrée)

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

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

internet industriel des objets (IIoT)

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

VPC d'inspection

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

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Consultez la section Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

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

zone de destination

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

lift and shift

Voir 7 Rs.

système de poids faible

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

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

Voir la succursale.

malware

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

services gérés

Services AWS qui AWS gère la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données.

Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également connus sous le nom de services abstraits.

système d'exécution de la fabrication (MES)

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

MAP

Voir Migration Acceleration Program.

mécanisme

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

compte membre

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

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

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

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une

interface bien définie à l'aide d'API légères. Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement les opérations, les analystes commerciaux et les propriétaires, les ingénieurs de migration, les développeurs et les DevOps professionnels travaillant dans le cadre de sprints. Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat

de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, consultez la section Évaluation de l'état de préparation à la modernisation des applications dans le AWS Cloud.

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés ne peuvent accéder au contenu d'un compartiment

S3 que par le biais d'une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

OU

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute

modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter Preventative controls dans Implementing security controls on AWS.

principal

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

Confidentialité dès la conception

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

zones hébergées privées

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

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

pseudonymisation

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

publier/souscrire (pub/sub)

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

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Cela permet de déterminer ce qui est considéré comme une perte de données acceptable entre le dernier point de restauration et l'interruption du service.

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

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

S

SAML 2.0

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

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

Politique qui propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. Les SCP définissent des barrières de protection ou des

limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

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

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

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

réglage

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

équipe de deux pizzas

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

U

incertitude

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

Pour plus d'informations, veuillez consulter le guide Quantifying uncertainty in deep learning systems.

tâches indifférenciées

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

environnements supérieurs

Voir environnement.

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

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

VER

Voir écrire une fois, lire plusieurs.

WQF

Consultez le cadre de qualification des charges de travail AWS.

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité de type « jour zéro »

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

application zombie

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

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