



Appliquer le framework AWS Well-Architected aux applications Amazon WorkSpaces

AWS Conseils prescriptifs



AWS Conseils prescriptifs: Appliquer le framework AWS Well-Architected aux applications Amazon WorkSpaces

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Introduction	1
Public visé	1
Objectifs	2
Pilier d'excellence opérationnelle	3
Organisez les équipes en fonction des résultats commerciaux	3
Mettez en œuvre l'observabilité pour obtenir des informations exploitables	4
Automatisez en toute sécurité si possible	5
Effectuez des modifications fréquentes, mineures et réversibles	7
Affiner fréquemment les procédures opérationnelles	9
Anticipez les défaillances	9
Tirez les leçons de tous les événements opérationnels et de tous les indicateurs	11
Utiliser des services gérés	11
Pilier de sécurité	12
Mettre en place une base d'identité solide	12
Maintenir la traçabilité	13
Appliquer la sécurité à tous les niveaux	14
Automatisez les meilleures pratiques de sécurité	15
Éloignez les utilisateurs des données	16
Préparez-vous aux événements de sécurité	16
Pilier de fiabilité	18
Restauration automatique en cas de panne	18
Procédures de reprise des tests	19
Évoluez horizontalement pour augmenter la disponibilité globale de la charge de travail	20
Arrêtez de deviner la capacité	20
Gérez le changement grâce à l'automatisation	20
Pilier d'efficacité des performances	22
Démocratiser les technologies avancées	22
Passez à l'international en quelques minutes	23
Utiliser des architectures sans serveur	23
Expérimentez plus souvent	24
Pensez à la sympathie mécanique	24
Pilier d'optimisation des coûts	26
Mettre en œuvre la gestion financière dans le cloud	26
Ajouter un modèle de consommation	26

Mesurer l'efficacité globale	27
Arrêtez de dépenser de l'argent pour soulever des objets lourds de manière indifférenciée	27
Analyser et attribuer les dépenses	28
Pilier de durabilité	30
Comprenez votre impact	30
Fixer des objectifs de durabilité	30
Optimiser l'utilisation	31
Anticipez et adoptez de nouvelles offres matérielles et logicielles plus efficaces	31
Services gérés d'occasion	32
Réduisez l'impact en aval de vos charges de travail dans le cloud	32
Ressources	33
AWS documentation	33
AWS articles de blog	33
Historique du document	36
Glossaire	37
#	37
A	38
B	41
C	43
D	46
E	51
F	53
G	55
H	56
I	58
L	60
M	62
O	66
P	69
Q	72
R	72
S	75
T	79
U	81
V	82
W	82

Z	83
.....	lxxxv

Appliquer le framework AWS Well-Architected aux applications Amazon WorkSpaces

Mohamed Wali, Amazon Web Services

Juillet 2025 ([historique du document](#))

[Ce guide décrit les meilleures pratiques pour appliquer le AWS Well-Architected Framework lorsque vous utilisez Amazon Applications. WorkSpaces](#) WorkSpaces Applications est un service de streaming d'applications entièrement géré qui vous permet de diffuser des applications de bureau aux utilisateurs sans les réécrire.

Le AWS Well-Architected Framework aide les architectes du cloud à créer des infrastructures sécurisées, performantes, résilientes et efficaces pour une variété d'applications et de charges de travail. Il fournit également une approche cohérente aux utilisateurs et aux AWS partenaires pour évaluer les architectures et mettre en œuvre des conceptions évolutives.

Le AWS Well-Architected Framework repose sur six piliers :

- Excellence opérationnelle
- Sécurité
- Fiabilité
- Efficacité des performances
- Optimisation des coûts
- Durabilité

Ce guide explique comment ces piliers et meilleures pratiques s'appliquent à l'utilisation WorkSpaces des applications.

Public visé

Ce guide est destiné aux personnes suivantes :

- Architectes et ingénieurs du cloud qui conçoivent et mettent en œuvre des solutions d'WorkSpaces applications et doivent s'assurer que leurs architectures respectent les meilleures pratiques de AWS Well-Architected Framework.

- Les équipes des opérations informatiques qui gèrent et entretiennent les environnements d'WorkSpaces applications ; s'occupent de la gestion, de la mise à l'échelle et de la surveillance du parc ; et doivent optimiser les coûts et les performances.
- Organisations ou entreprises qui envisagent d'utiliser ou qui utilisent déjà WorkSpaces des applications, souhaitent diffuser des applications de bureau à leurs utilisateurs et doivent créer des infrastructures sécurisées, performantes, résilientes et efficaces.

Objectifs

Le respect des meilleures pratiques décrites dans ce guide vous permet de :

- Créez une infrastructure sécurisée, performante, résiliente et efficace pour diffuser des applications de bureau dans le AWS Cloud.
- Appliquez une approche cohérente lors de l'évaluation des architectures d'WorkSpaces applications et de la mise en œuvre de conceptions évolutives.

Pilier d'excellence opérationnelle

L'excellence opérationnelle (OE) représente un engagement à concevoir des solutions logicielles de haute qualité qui répondent et dépassent constamment les attentes des utilisateurs. Le [pilier de l'excellence opérationnelle](#) du AWS Well-Architected Framework englobe des stratégies éprouvées pour une organisation efficace des équipes, une conception robuste des charges de travail, des opérations efficaces à grande échelle et une adaptation fluide à l'évolution des exigences au fil du temps. En adhérant à ces principes, les entreprises peuvent s'assurer que leurs systèmes restent résilients, performants et adaptés à l'évolution des besoins de l'entreprise.

Principaux domaines d'intérêt pour appliquer ce pilier à votre environnement de streaming d'WorkSpaces applications :

- Surveillance et observabilité
- Automatisation et DevOps
- Procédures opérationnelles et documentation
- Support et gestion des incidents

Organisez les équipes en fonction des résultats commerciaux

Créez un modèle opérationnel aligné sur le cloud avec un engagement fort de la direction, dans lequel les objectifs commerciaux et les indicateurs de performance clés (KPIs) stimulent la transformation organisationnelle grâce à l'optimisation des personnes, des processus et des technologies.

- Structure de l'équipe. Constituez des équipes dédiées qui s'alignent sur les résultats du streaming des applications. Par exemple :
 - L'équipe de gestion des images est responsable du packaging des applications et de l'optimisation des images.
 - L'équipe des opérations de flotte gère la capacité, les performances et la mise à l'échelle.
 - L'équipe chargée de l'expérience utilisateur s'occupe du support et de la satisfaction des utilisateurs finaux.
- KPIs et métriques. Définissez et suivez des indicateurs adaptés à l'entreprise, tels que :
 - Taux de disponibilité des applications

- Il est temps de déployer de nouvelles applications
- Coût par heure de diffusion d'une application
- Modèle de fonctionnement. Créez des processus clairs pour :
 - Intégration et mises à jour des applications
 - Gestion de la capacité du parc
 - Provisionnement de l'accès utilisateur
 - Réponse et résolution des incidents

Mettez en œuvre l'observabilité pour obtenir des informations exploitables

Mettez en œuvre une surveillance et une observabilité complètes pour suivre l'état de KPIs la charge de travail. Ce principe permet de prendre des décisions basées sur les données et d'améliorer de manière proactive les performances, la fiabilité et les coûts.

- Mettez en œuvre le suivi des performances. Configurez [Amazon CloudWatch](#) pour :
 - Garantir une capacité suffisante pour répondre à la demande. Par exemple, vous pouvez utiliser les mesures suivantes :
 - `AvailableCapacity` pour surveiller les instances de streaming disponibles
 - `InUseCapacity` pour suivre les instances actuellement utilisées
 - `CapacityUtilization` pour surveiller le pourcentage d'utilisation de la flotte
 - Surveillez l'expérience utilisateur et les performances.
 - Identifiez et réglez rapidement les problèmes de service.
- Suivez et analysez les rapports d'utilisation des WorkSpaces applications.
- Capturez et analysez les journaux des applications. Pour plus d'informations, consultez les articles de AWS blog [Utilisation de Kinesis Agent pour Linux pour diffuser les journaux d' WorkSpaces applications dans Applications](#) et [Utilisation de Kinesis Agent pour Microsoft Windows pour stocker les journaux d'événements d' WorkSpaces Applications Windows](#).
- Surveillez WorkSpaces les métriques et les événements des applications par le biais de notifications par chat. Pour plus d'informations, consultez le billet de AWS blog [Surveiller et automatiser l'informatique des utilisateurs AWS finaux \(EUC\) avec AWS Chatbot](#).

- Activez la gestion proactive des sessions grâce à des repères visuels. Pour plus d'informations, consultez le billet de AWS blog [Afficher l'expiration de la session et le compte à rebours dans Amazon WorkSpaces Applications](#).
- Créez des visualisations des modèles et des tendances d'utilisation. Pour plus d'informations, consultez le billet de AWS blog [Ingérez et visualisez les rapports d'utilisation WorkSpaces des applications Amazon dans Amazon OpenSearch Service](#).
- Utilisez le kit d'outils EUC pour surveiller les sessions actives, suivre l'inventaire de la flotte et générer des rapports de session (exportation CSV). Pour plus d'informations, consultez le billet de AWS blog [Utiliser le kit EUC pour gérer Amazon WorkSpaces Applications et Amazon WorkSpaces](#).

Automatisez en toute sécurité si possible

Appliquez les principes de l'infrastructure sous forme de code (IaC) pour automatiser tous les aspects de vos opérations de charge de travail. Utilisez des glissières de sécurité pour garantir une exécution sûre et cohérente tout en réduisant les interventions manuelles.

- Automatisez la création et la configuration des images d' WorkSpaces applications à l'aide de l'interface de ligne de commande Image Assistant. Pour plus d'informations, consultez [Créer votre image Amazon WorkSpaces Applications par programmation à l'aide des opérations de la CLI Image Assistant dans la documentation des WorkSpaces applications](#).
- Installation des applications : utilisez la CLI Image Assistant pour automatiser l'installation des applications lors de la création d'images.
- Création d'images : créez des images d' WorkSpaces applications par programmation à l'aide des commandes de la CLI Image Assistant.
- Gestion de la configuration : automatisez la configuration des paramètres par défaut de l'application et des paramètres de lancement.
- Automatisez la personnalisation des images des WorkSpaces applications. Pour plus d'informations, consultez le billet de AWS blog [Créer automatiquement des images Windows WorkSpaces d'applications personnalisées](#).
- Appliquez IaC pour déployer l'infrastructure et les composants d'application pour les WorkSpaces applications. Pour plus d'informations, consultez le billet de AWS blog [Automatisation de l'infrastructure et du déploiement d'applications pour Amazon WorkSpaces Applications avec Terraform](#).

- Mettez en œuvre des processus automatisés pour la gestion de flotte, notamment :
 - Évolution de la flotte en fonction de la demande. Configurez des politiques de dimensionnement automatique pour ajuster automatiquement la capacité du parc en fonction des indicateurs d'utilisation. Pour plus d'informations, consultez le billet de AWS blog [Utiliser AWS Lambda pour ajuster les étapes de dimensionnement et les seuils pour Amazon WorkSpaces Applications](#).
 - Mises à jour des images de base. Bénéficiez des mises à jour automatiques de l'image de base des WorkSpaces applications fournie par AWS.
 - Optimisation des capacités. Définissez des seuils de dimensionnement automatisés pour optimiser l'utilisation des ressources en fonction des modèles de demande.
- Configurez les garde-corps pour automatiser les contrôles de sécurité :
 - Limites de taille maximale du parc. Fixez des limites supérieures à la capacité du parc afin d'éviter le surprovisionnement.
 - Configuration de la politique de dimensionnement. Mettez en œuvre des politiques de dimensionnement par étapes ou de suivi des cibles avec des seuils appropriés.
 - Quotas de service. Utilisez les quotas de AWS service comme limites intégrées pour éviter une allocation de ressources excessive.
 - Protection évolutive. Configurez la protection évolutive pour empêcher la suppression d'instances actives lors d'événements de dimensionnement.
- Effectuez des tests et des validations, notamment des tests de création d'images, de flotte et d'intégration.
 - Test du générateur d'images :
 - Testez les applications directement dans l'interface du générateur d'images.
 - Vérifiez le lancement et le fonctionnement de l'application.
 - Testez les paramètres et les configurations utilisateur.
 - Validez la compatibilité des applications.
 - Tests de flotte :
 - Testez les sessions de streaming à partir de différents appareils clients.
 - Vérifiez les droits et les accès des utilisateurs.
 - Validez les performances des applications.
 - Testez l'expérience utilisateur pour les éléments et les opérations tels que le presse-papiers, le transfert de fichiers et l'impression.

- Testez l'authentification basée sur Active Directory ou SAML 2.0.
- Testez les dossiers personnels et le stockage persistant.
- Testez les droits des applications.
- Testez la redirection du périphérique USB (si elle est configurée).
- Utilisez le gestionnaire WorkSpaces d'applications pour automatiser le packaging et le déploiement des applications. Pour plus d'informations, consultez le billet de AWS blog [Simplifiez l'intégration des applications avec le gestionnaire d'applications pour Amazon WorkSpaces Applications](#).
- Automatisez le déploiement de nouvelles versions d'applications en utilisant des pipelines d'intégration continue et de livraison continue (CI/CD). Pour plus d'informations, consultez le billet de AWS blog [Screening Eagle : Optimize CI/CD and end user experience in Amazon WorkSpaces Applications](#).

Effectuez des modifications fréquentes, mineures et réversibles

Créez des charges de travail évolutives et faiblement couplées qui permettent des déploiements automatisés fréquents et à petite échelle avec un minimum de risques et des fonctionnalités de restauration faciles.

- Pour les mises à jour d'images, utilisez la création d'images versionnées et les mises à jour incrémentielles.
 - Création d'images versionnées :
 - Créez de nouvelles images pour chaque ensemble de modifications à l'aide d'un générateur d'images.
 - Gérez plusieurs versions d'image pour prendre en charge les scénarios de restauration.
 - Utilisez des [stratégies AWS de balisage](#) pour suivre les versions et les attributs des images.
 - Mises à jour incrémentielles :
 - Apportez de petites modifications incrémentielles aux applications ou aux configurations.
 - Testez soigneusement les mises à jour dans le générateur d'images avant de créer une nouvelle image.
 - Documentez toutes les modifications que vous avez apportées dans chaque nouvelle version d'image.
- Pour les mises à jour du parc de contrôle :
 - Créez de nouvelles flottes avec des images mises à jour à des fins de test.

- Modifiez les attributs de flotte existants sans perturber les sessions actives.
- Établissez des procédures de gestion des modifications pour la documentation, les protocoles de test, les flux de travail d'approbation et les processus de surveillance.
 - Documentation :
 - Conservez des journaux de modifications détaillés pour toutes les mises à jour d'images et de flotte.
 - Documentez les procédures de test et les résultats pour chaque modification.
 - [AWS CloudTrail](#) à utiliser pour suivre et auditer les modifications de configuration.
 - Protocoles de test :
 - Établissez un processus de test complet pour tous les changements.
 - Incluez des tests de fonctionnalité, de performance et d'expérience utilisateur des applications.
 - Effectuez des tests dans le générateur d'images avant de créer de nouvelles images.
 - Effectuez des tests supplémentaires sur des flottes non destinées à la production avant le déploiement complet.
 - Flux de travail d'approbation :
 - Mettez en œuvre un processus d'approbation pour les modifications apportées aux environnements de production.
 - Définissez des critères pour les modifications nécessitant une approbation par rapport aux mises à jour standard.
 - Définissez les rôles et les responsabilités pour l'approbation des modifications.
 - Surveillance et validation :
 - Utilisez [Amazon CloudWatch](#) pour surveiller les performances du parc et des applications après les modifications.
 - Configurez des alertes pour les indicateurs clés afin d'identifier rapidement les problèmes après les mises à jour.
 - Réalisez des examens après la mise en œuvre pour valider le succès du changement et en tirer des enseignements.

Affiner fréquemment les procédures opérationnelles

Améliorez continuellement les procédures opérationnelles grâce à des révisions régulières, à des mises à jour et à l'engagement de l'équipe afin de tenir toutes les parties prenantes informées et conformes aux meilleures pratiques.

- **Gestion de la documentation** Conservez la documentation actualisée et contrôlée par version des procédures relatives aux WorkSpaces applications dans un emplacement central afin de garantir la cohérence opérationnelle et le partage des connaissances entre les équipes.
 - **Documentation requise** : Conservez up-to-date la documentation relative aux opérations critiques des WorkSpaces applications pour la création et la gestion d'images, les opérations de flotte et le dépannage.
 - **Examens opérationnels** : surveillez et passez en revue les principaux aspects opérationnels, notamment les indicateurs de performance et la gestion des incidents.
- **Amélioration continue**. Améliorez systématiquement le fonctionnement des WorkSpaces applications en incorporant Service AWS des mises à jour, des mesures opérationnelles et les meilleures pratiques apprises dans les procédures standard.
 - **Mises à jour du service** : surveillez WorkSpaces les notes de mise à jour des applications pour connaître les nouvelles fonctionnalités, les améliorations de service, les mises à jour de sécurité et la disponibilité régionale.
 - **Meilleures pratiques** : passez en revue et intégrez les mises à jour de AWS Well-Architected Framework, les meilleures pratiques en matière d'applications WorkSpaces , les architectures de référence AWS et les recommandations de sécurité. AWS
 - **Gestion des connaissances** : Maintenir et mettre à jour les procédures opérationnelles standard, les manuels d'exécution, les guides de dépannage et la documentation d'assistance aux utilisateurs.

Anticipez les défaillances

Procédez régulièrement à des tests de scénarios de défaillance pour comprendre les risques, valider les procédures de réponse et améliorer la préparation de l'équipe à la gestion des incidents réels.

- **Tests de défaillance**. Simulez et testez régulièrement les défaillances telles que l'épuisement de la capacité du parc, les échecs de lancement d'applications et les problèmes de connectivité réseau.
 - **Épuisement de la capacité du parc** :

- Surveillez et testez le comportement de mise à l'échelle de la flotte à l'approche des limites de capacité.
- Configurez les CloudWatch alarmes `CapacityUtilization` et `AvailableCapacity` les métriques.
- Mettre en œuvre des procédures pour gérer les contraintes de capacité pendant les pics d'utilisation.
- Échec du lancement de l'application :
 - Testez le comportement de lancement de l'application sur les instances de streaming.
 - Validez l'accès aux applications et les performances des différentes configurations de flotte.
- Problèmes de connectivité réseau :
 - Testez les performances des sessions de streaming dans différentes conditions de réseau.
 - Surveillez `StreamingSessionLatency` les problèmes de qualité de connexion.
 - Assurez-vous que les paramètres VPC et les groupes de sécurité sont correctement configurés.
- Procédures de rétablissement. Élaborer et tester des procédures pour :
 - Basculement de flotte entre AWS Zones de disponibilité. En outre, documentez les procédures pour augmenter la capacité de la flotte, gérer les mises à jour de la flotte et répondre aux problèmes de santé des instances.
 - Gestion des données utilisateur :
 - Configurez et testez les solutions de [persistance et de stockage des paramètres d'application](#) pour les dossiers personnels dans Amazon Simple Storage Service (Amazon S3) pour les flottes Windows et les systèmes de fichiers partagés dans Amazon Elastic File System (Amazon EFS) pour les flottes Linux.
 - Validez la synchronisation des données entre les sessions.
 - Continuité du service. Maintenez les procédures de création de nouvelles instances de flotte, de gestion des mises à jour des images et de gestion des déconnexions de sessions.
- Gestion des risques Identifiez et atténuez :
 - Contraintes de capacité en définissant une capacité minimale de flotte appropriée, en configurant des politiques de dimensionnement automatique en fonction des modèles de demande et en surveillant les tendances d'utilisation de la flotte à l'aide de CloudWatch métriques telles que `CapacityUtilizationInUseCapacity`, et `AvailableCapacity`.

- Des problèmes de performance liés au suivi des indicateurs clés tels que la configuration des alarmes appropriées `StreamingSessionLatency` et à la configuration des alarmes appropriées. CloudWatch

Tirez les leçons de tous les événements opérationnels et de tous les indicateurs

Favorisez une culture d'amélioration continue en partageant les leçons tirées des événements opérationnels et des défaillances au sein de l'organisation. Soulignez leur impact sur les résultats commerciaux.

- Analyse des événements. Documentez et analysez les interruptions de service, la dégradation des performances, les plaintes des utilisateurs et les problèmes de capacité.
- Examen des métriques. Analysez régulièrement les modèles d'utilisation, les tendances de performance, les indicateurs de coûts et les données de satisfaction des utilisateurs.
- Partage des connaissances. Établissez des processus pour les sessions d'apprentissage en équipe, la documentation des meilleures pratiques, le transfert de connaissances entre les équipes et les rétrospectives des incidents.

Utiliser des services gérés

Minimisez les frais d'exploitation en utilisant des services AWS gérés et en élaborant des procédures normalisées autour de ceux-ci. Intégrez les services AWS gérés suivants :

- [AWS Systems Manager](#) pour l'automatisation
- [Amazon CloudWatch](#) pour la surveillance
- [Gestion des identités et des accès AWS \(IAM\)](#) pour le contrôle d'accès
- [Amazon S3](#) pour le stockage utilisateur pour les flottes Windows
- [Amazon EFS](#) pour le stockage utilisateur pour les flottes Linux
- [AWS Directory Service](#) pour l'authentification des utilisateurs

Pilier de sécurité

Le [pilier de sécurité](#) du AWS Well-Architected Framework vise à tirer parti des fonctionnalités du cloud pour aider à établir des mécanismes de protection robustes pour vos informations, votre infrastructure et vos ressources. Ces principes contribuent à améliorer votre posture globale en matière de sécurité tout en favorisant l'innovation.

Principaux domaines d'intérêt pour appliquer ce pilier à votre environnement de streaming d'WorkSpaces applications :

- Intégrité et confidentialité des données
- Gestion des autorisations utilisateur
- Mise en place de contrôles pour détecter les événements de sécurité

Mettre en place une base d'identité solide

Utilisez les autorisations minimales requises pour accéder aux AWS ressources tout en centralisant la gestion des identités et en évitant les identifiants à long terme.

- Accordez les autorisations les moins privilégiées pour WorkSpaces les ressources des applications :
 - Créez des rôles IAM spécifiques pour les flottes WorkSpaces d'applications avec les autorisations minimales requises.
 - Configurez des autorisations IAM limitées pour les générateurs d'images.
 - Limitez l'accès administratif aux fonctions de gestion des WorkSpaces applications.
 - Définissez des autorisations granulaires pour la gestion des stocks et des flottes.
- Mettez en œuvre des mécanismes d'authentification utilisateur appropriés :
 - Configurez la fédération SAML 2.0 pour l'intégration des fournisseurs d'identité d'entreprise.
 - Configuration [AWS IAM Identity Center](#) pour la gestion des utilisateurs.
 - Utilisez des courtiers d'identité personnalisés uniquement lorsque cela est nécessaire pour des scénarios d'authentification spécifiques.
 - Mettez en œuvre l'authentification multifactorielle (MFA) lorsqu'elle est prise en charge.
- Contrôlez l'accès des utilisateurs aux applications :
 - Configurez les droits des applications pour restreindre l'accès à des applications spécifiques.

- Créez des groupes d'attribution d'applications en fonction des rôles des utilisateurs.
- Gérez l'accès aux applications via des autorisations de pile.
- Mettez en œuvre des politiques de session pour contrôler le comportement des applications.
- Sécurisez les sessions utilisateur avec des contrôles appropriés :
 - Configurez les politiques de temporisation des sessions.
 - Définissez les actions de temporisation de déconnexion.
 - Implémentez les exigences de persistance des sessions.
 - Contrôlez les autorisations de redirection du système de fichiers.
- Configurez l'authentification basée sur des certificats pour les applications WorkSpaces . Pour plus d'informations, consultez le billet de AWS blog [Simplifier l'authentification basée sur les certificats pour les WorkSpaces applications et WorkSpaces avec Autorité de certification privée AWS Connector for Active Directory](#).
- Utilisez des balises de session pour mettre en œuvre un contrôle d'accès précis. Pour plus d'informations, consultez le billet de AWS blog [Utiliser les balises de session pour simplifier WorkSpaces les autorisations des applications](#).

Maintenir la traçabilité

Mettez en œuvre une surveillance en temps réel et des systèmes de réponse automatisés pour tous les changements et activités liés à l'environnement.

- Configurez la [CloudWatch journalisation](#) des journaux des applications afin de surveiller les événements spécifiques aux applications, notamment les lancements d'applications, les pannes et les erreurs. Configurez les journaux de session pour suivre les informations des sessions de streaming, notamment les démarrages, les arrêts et les événements de connexion utilisateur.
- [Activez cette option CloudTrail pour enregistrer tous les appels d'API des WorkSpaces applications](#) et pour suivre les événements de gestion tels que la création et la modification de flottes, les opérations de création d'images, les configurations de stack et les activités de gestion des utilisateurs.
- Surveillez l'activité WorkSpaces des instances d'applications :
 - Configurez la journalisation des instances pour capturer les événements au niveau du système.
 - Suivez les lancements et les échecs des applications.
 - Surveillez l'utilisation des ressources et les performances du système.

- Suivez l'activité des utilisateurs :
 - Surveillez les tentatives et les échecs d'authentification des utilisateurs. Utilisez CloudWatch les métriques et les CloudWatch journaux pour suivre les tentatives de connexion des utilisateurs, les heures de début et de fin de session et les événements de déconnexion de session.
 - Suivez les habitudes d'utilisation des applications. [Activez WorkSpaces les rapports d'utilisation des applications](#) pour récupérer des informations telles que la durée des sessions, les heures de début et de fin, les types d'instances utilisés et les applications consultées.
 - Enregistrez les activités du système de fichiers via les dossiers de base activés.
 - Configurez les paramètres du presse-papiers et les opérations d'impression pour atteindre vos objectifs de prévention des pertes de données.
- Configurez des [CloudWatch alarmes](#) pour les mesures liées à la sécurité, telles que les échecs d'authentification des utilisateurs, les modèles de session inhabituels et les violations d'accès aux ressources.
- Utilisez le kit d'outils EUC pour suivre les sessions et les états actifs, surveiller les adresses IP pour les sessions actives en cours d'utilisation et exporter les données de session à des fins d'audit. Pour plus d'informations, consultez le billet de AWS blog [Utiliser le kit d'outils EUC pour gérer Amazon WorkSpaces Applications et Amazon WorkSpaces](#).

Appliquer la sécurité à tous les niveaux

Mettez en œuvre plusieurs niveaux de contrôles de sécurité sur tous les composants de votre infrastructure, de la périphérie du réseau au code d'application.

- Configurer la sécurité de la couche réseau :
 - Mettez en œuvre des règles strictes relatives aux groupes de sécurité.
 - Placez WorkSpaces les instances du parc d'applications dans des sous-réseaux privés qui n'ont pas d'accès direct à Internet. Contrôlez l'accès à Internet via des appareils NAT.
 - Utilisez les points de terminaison de cloud privé virtuel (VPC) pour accéder aux services pris en charge Services AWS (comme Amazon S3).
 - Implémentez des listes de contrôle d'accès réseau (ACLs) en tant que couche de sécurité réseau supplémentaire.
 - Limitez l'accès au port de streaming (TCP 8443 pour HTTPS et WebSocket Secure) à des plages d'adresses IP spécifiques.
- Configurer la sécurité de la couche d'accès :

- Mettez en œuvre des politiques de temporisation de session pour déconnecter automatiquement les utilisateurs inactifs.
- Mettez en œuvre un contrôle d'accès basé sur les attributs à l'aide de balises de session. Pour plus d'informations, consultez le billet de AWS blog [Utiliser les balises de session pour simplifier WorkSpaces les autorisations des applications](#).
- Configurer la sécurité de la couche applicative :
 - Configurez les droits des applications pour contrôler quels utilisateurs peuvent accéder à des applications spécifiques.
 - Activez les contrôles de redirection du système de fichiers pour restreindre l'accès aux lecteurs locaux.
 - Configurez le presse-papiers, le transfert de fichiers et les autorisations d'impression en fonction des exigences de sécurité.
 - Configurez les contrôles d'accès aux périphériques USB conformément aux politiques de sécurité.
- Configurer la sécurité de la couche d'image :
 - Créez et gérez des images de base renforcées qui répondent aux exigences de sécurité.
 - Maintenez les images de base à jour avec les derniers correctifs de sécurité.
 - Configurez les paramètres de sécurité Windows dans les images de base.
 - Désactivez les services et fonctionnalités Windows inutiles dans les images de base.

Automatisez les meilleures pratiques de sécurité

Utilisez des contrôles de sécurité automatisés définis par code dans des modèles contrôlés par version pour permettre un déploiement d'infrastructure sécurisé et évolutif.

- Utilisez l'infrastructure en tant que code (IaC) en utilisant des services tels que la mise AWS CloudFormation en œuvre de configurations de sécurité cohérentes dans tous les déploiements de flotte. Pour plus d'informations, consultez le billet de AWS blog [Attacher automatiquement des groupes de sécurité supplémentaires à Amazon WorkSpaces Applications et Amazon WorkSpaces](#).
- Automatisez les processus de sécurité liés à la création d'images à l'aide de l'interface de ligne de commande Image Assistant.

- Configurez des réponses automatisées en cas de dépassement des seuils d'utilisation des capacités, de tentatives d'accès non autorisées et de modifications du groupe de sécurité en utilisant les CloudWatch alarmes Amazon, EventBridge les règles Amazon et les AWS Lambda fonctions de réponses automatisées.

Éloignez les utilisateurs des données

Automatisez les processus de traitement des données afin de minimiser l'accès humain direct et de réduire le risque d'erreurs ou de mauvaise gestion.

- Configurez les droits des applications pour contrôler quels utilisateurs peuvent accéder à des applications spécifiques.
- Utilisez le [framework d'applications dynamiques](#) pour créer un fournisseur d'applications dynamiques afin de rendre les applications disponibles de manière dynamique en fonction des attributs utilisateur.
- Configurez la redirection du système de fichiers pour contrôler les lecteurs locaux auxquels les utilisateurs peuvent accéder, pour restreindre l'accès à des dossiers spécifiques et pour gérer les autorisations de transfert de fichiers entre les sessions locales et les sessions de streaming.
- Implémentez des restrictions relatives au presse-papiers pour désactiver le partage du presse-papiers entre les sessions locales et les sessions de streaming, activer le flux unidirectionnel dans le presse-papiers si nécessaire et empêcher la copie non autorisée des données.
- Configurez la persistance des paramètres des applications pour enregistrer et restaurer automatiquement les configurations des applications, éliminer les besoins de configuration manuelle et garantir une expérience utilisateur cohérente.

Préparez-vous aux événements de sécurité

Développez et mettez en pratique des plans de réponse aux incidents en utilisant des outils automatisés pour permettre une détection, une investigation et une reprise rapides après des événements de sécurité.

- Configurez des CloudWatch alarmes en cas d'échec des tentatives d'authentification, de modification des groupes de sécurité du parc, de modification des configurations d'image et de modèles de session de streaming inhabituels.

- Documentez les procédures de réponse pour les scénarios de sécurité des WorkSpaces applications courants tels que :
 - Tentatives d'accès non autorisées
 - Détection : surveillez les échecs d'authentification.
 - Réponse : révoquez les droits des utilisateurs, consultez les journaux de session et mettez à jour les politiques d'accès.
 - Instances de streaming compromises
 - Détection : surveillez le comportement de l'instance.
 - Réponse : mettez fin aux sessions concernées, remplacez les instances de flotte et passez en revue les configurations des groupes de sécurité.
 - Tentatives d'exfiltration de données
 - Détection : surveillez les activités de transfert de fichiers.
 - Réponse : passez en revue le presse-papiers et les journaux de transfert de fichiers, ajustez les autorisations de transfert de fichiers et mettez à jour les politiques de protection des données.
- Mettez en œuvre des processus de restauration automatisés pour le remplacement des instances du parc, la restauration des groupes de sécurité, la reconfiguration des accès utilisateurs et la restauration des paramètres des applications.
- Services AWS À utiliser pour la gestion de la sécurité, par exemple AWS Security Hub CSPM pour les résultats de sécurité et Amazon GuardDuty pour la détection des menaces.

Pilier de fiabilité

Le [pilier de fiabilité](#) du AWS Well-Architected Framework porte sur la capacité d'un système à maintenir les fonctionnalités et les niveaux de performance prévus pendant les périodes opérationnelles prévues tout au long de sa durée de vie. Il fournit des directives complètes pour la création et la maintenance de systèmes fiables AWS, y compris des stratégies de test et de validation à toutes les étapes du cycle de vie des charges de travail.

Principaux domaines d'intérêt pour appliquer ce pilier à votre environnement de streaming d'WorkSpaces applications :

- Gestion et mise à l'échelle de la flotte
- Fiabilité des sessions
- Disponibilité des applications
- Procédures de rétablissement

Restauration automatique en cas de panne

Surveillez KPIs la valeur commerciale afin de déclencher des réponses automatisées capables de prévoir, de prévenir ou de corriger les défaillances avant qu'elles n'aient un impact sur les opérations.

- Assurez-vous que l'allocation de votre sous-réseau IP tient compte de l'extension et de la disponibilité.
- Surveillez CloudWatch les indicateurs critiques pour garantir la disponibilité et les performances des services, y compris les indicateurs de capacité du parc tels que `AvailableCapacity` et `InUseCapacity`, et les indicateurs de qualité du streaming tels que `StreamingSessionLatency`.
- Configurez des alertes pour les seuils de capacité, les indicateurs de santé des sessions, la dégradation des performances et les modifications de l'état de santé du parc.
- Utilisez les fonctionnalités de mise à l'échelle automatique des WorkSpaces applications intégrées pour :
 - Configurez la capacité minimale et maximale du parc.
 - Définissez des politiques de dimensionnement basées sur l'utilisation des capacités.

- Définissez des seuils de scale-out et de scale-in en fonction des indicateurs de l'expérience utilisateur et des exigences commerciales plutôt que de simples indicateurs techniques.
- Créez un environnement de reprise après sinistre pour votre environnement WorkSpaces d'applications. Pour plus d'informations, consultez le billet de AWS blog [Considérations relatives à la reprise après sinistre avec Amazon WorkSpaces Applications](#).

Procédures de reprise des tests

Les environnements cloud permettent de tester automatiquement les scénarios de défaillance et les procédures de restauration. Ces fonctionnalités vous aident à identifier et à corriger les vulnérabilités avant que de véritables défaillances ne se produisent.

- Tests de reprise de flotte. Mettez en œuvre des tests complets de reprise de flotte dans le cadre de plusieurs scénarios :
 - Simulez la terminaison d'une instance pour vérifier la réponse automatique du dimensionnement.
 - Validez le maintien de la capacité minimale de la flotte.
 - Testez le calendrier de remplacement des instances et la redirection des utilisateurs.
 - Validez l'efficacité des politiques de dimensionnement.
 - Testez les limites de capacité du parc et la gestion des débordements.
- Test de restauration de session. Mettre en œuvre des procédures de validation de restauration de session :
 - Testez les scénarios de déconnexion et de reconnexion.
 - Vérifiez la préservation de l'état de l'application.
 - Testez différents scénarios d'interruption du réseau.
 - Validez les comportements d'expiration de session.
 - Vérifiez la persistance de l'authentification utilisateur.
 - Vérifiez la gestion du stockage temporaire.

Évoluez horizontalement pour augmenter la disponibilité globale de la charge de travail

Répartissez votre charge de travail sur plusieurs ressources plus petites afin de minimiser l'impact des défaillances individuelles et d'éliminer les points de défaillance uniques.

- Déployez des instances de flotte dans plusieurs zones de disponibilité.
- Configurez la capacité minimale de flotte appropriée.
- Configurez le dimensionnement automatique pour les flottes et définissez des seuils de dimensionnement appropriés.
- Surveillez l'utilisation des capacités dans l'ensemble du parc.
- Déployez WorkSpaces des piles d'applications dans plusieurs régions. Pour plus d'informations, consultez le billet de AWS blog [Optimize user experience with latency based routing for Amazon Applications](#). WorkSpaces

Arrêtez de deviner la capacité

Utilisez les fonctionnalités de dimensionnement automatique du cloud pour ajuster dynamiquement les ressources en fonction de la demande. Cela permet d'éviter la saturation des ressources tout en maintenant une efficacité optimale.

- Surveillez les indicateurs clés tels que `CapacityUtilizationAvailableCapacity`, et `InUseCapacity` pour comprendre les besoins en capacité.
- Suivez les tendances d'utilisation de la flotte sur différentes périodes. Surveillez les tendances quotidiennes, les variations hebdomadaires, les tendances mensuelles et les pics saisonniers.
- Définissez des politiques de dimensionnement et configurez des seuils de dimensionnement.
- Assurez-vous qu'il existe un écart suffisant entre les quotas actuels et l'utilisation maximale pour permettre le basculement.
- Adaptez les quotas et les contraintes de service fixes au sein de votre architecture.

Gérez le changement grâce à l'automatisation

Mettez en œuvre les modifications de l'infrastructure par le biais de l'automatisation, y compris des modifications contrôlées par version du code d'automatisation lui-même.

- Utilisez iAc pour la configuration de la flotte.
- Mettez en œuvre des politiques de dimensionnement cohérentes.
- Utilisez la [CLI Image Assistant](#) pour créer des images de manière cohérente.

Pilier d'efficacité des performances

Le [pilier de l'efficacité des performances](#) du AWS Well-Architected Framework se concentre sur l'optimisation de l'utilisation des ressources du cloud pour atteindre ou dépasser les objectifs de performance tout en garantissant l'adaptabilité aux demandes fluctuantes et aux technologies émergentes. Il souligne l'importance de peaufiner en permanence les systèmes afin de maintenir une efficacité maximale dans un environnement cloud dynamique.

Principaux domaines d'intérêt pour appliquer ce pilier à votre environnement de streaming d'WorkSpaces applications :

- Sélection et optimisation du type d'instance
- Optimisation des performances de streaming
- Gestion de la capacité du parc

Démocratiser les technologies avancées

Tirez parti des services gérés par les fournisseurs de cloud pour les technologies complexes afin que votre équipe puisse se concentrer sur le développement de produits plutôt que sur la gestion de l'infrastructure.

- Configurez les types d'instances appropriés en fonction des exigences de l'application :
 - Sélectionnez des instances compatibles GPU pour les applications gourmandes en ressources graphiques.
 - Choisissez [les familles de GPU](#) appropriées (telles que Graphics G4dn ou Graphics G5) en fonction des besoins de l'application.
- Choisissez et configurez l'une des méthodes d'authentification suivantes :
 - Configurez l'intégration avec un fournisseur d'identité basé sur SAML 2.0.
 - Configurez les paramètres du groupe d'utilisateurs.
 - Intégrez avec [AWS Directory Service](#).
- Activez et configurez les options de stockage en fonction des besoins des utilisateurs :
 - Configurez des dossiers personnels dans [Amazon S3](#) pour les flottes basées sur Windows.
 - Configurez des systèmes de fichiers partagés dans [Amazon EFS pour les flottes](#) basées sur Linux.

- Configurez les autorisations de stockage persistantes.
- Activez la persistance des paramètres de l'application.

Passez à l'international en quelques minutes

Utilisez le déploiement multirégional pour améliorer l'expérience utilisateur globale grâce à une latence réduite.

- Configurez plusieurs flottes en Régions AWS déployant des flottes dans les régions les plus proches de vos utilisateurs tout en créant des piles distinctes pour chaque région.
- Mettez en œuvre la redirection entre régions pour rediriger automatiquement les utilisateurs des WorkSpaces applications vers les AppStream piles les plus proches de leur emplacement actuel.
- Si vous utilisez l'une des fonctionnalités facultatives des WorkSpaces applications, telles que la persistance des paramètres des applications, les dossiers personnels ou les flottes élastiques, vous devez configurer la réplication entre régions d'Amazon S3 pour les données utilisateur pour les flottes Windows et la réplication entre régions pour les flottes basées sur Linux.
- Répliquez les images d'une région à l'autre. Pour plus d'informations, consultez la section [Copier une image que vous possédez vers une autre image Région AWS dans Amazon WorkSpaces Applications](#) dans la AWS documentation.
- Pour les flottes jointes à un domaine, assurez-vous qu'une infrastructure Active Directory, y compris Active Directory Federation Services (AD FS) (sauf si vous utilisez SAML 2.0 et Amazon Cognito comme alternative), est correctement configurée dans les autres régions et que vous l'utilisez pour les fonctionnalités de réplication multirégionale. [AWS Directory Service for Microsoft Active Directory](#)
- Dirigez les utilisateurs vers les points de terminaison des WorkSpaces applications avec le moins de latence. Pour plus d'informations, consultez le billet de AWS blog [Optimize user experience with latency based routing for Amazon Applications](#). WorkSpaces

Utiliser des architectures sans serveur

Les architectures sans serveur éliminent les frais de gestion des serveurs et réduisent les coûts en utilisant des services gérés dans le cloud pour les fonctions de calcul.

Utilisez des services AWS sans serveur tels que les suivants :

- [AWS Lambda](#) pour automatiser les tâches et intégrer une logique personnalisée grâce à des fonctions pilotées par des événements
- [Amazon S3](#) fournira un stockage évolutif pour les WorkSpaces applications, les données utilisateur, les fichiers d'applications et les artefacts de session
- [Amazon va CloudWatch](#) fournir des services de surveillance, de journalisation et d'alerte pour les indicateurs de performance et d'utilisation des WorkSpaces applications
- [Amazon Cognito va](#) faciliter l'authentification des utilisateurs et le contrôle d'accès pour WorkSpaces les applications et les applications
- [Amazon API Gateway](#) pour RESTful APIs créer une interface entre les WorkSpaces applications et d'autres services ou applications personnalisées

Expérimentez plus souvent

L'infrastructure cloud permet de tester rapidement différentes configurations de ressources afin d'optimiser les performances et les coûts.

- Testez différents types d'instances pour optimiser les performances et les coûts :
 - Comparez les performances des flux entre différentes familles d'instances.
 - Évaluez les instances GPU par rapport aux instances non GPU pour les applications graphiques.
 - Testez des instances optimisées pour la mémoire pour les applications gourmandes en mémoire.
- Testez les configurations des applications à l'aide d'Image Builder :
 - Créez des images de test avec différentes configurations d'applications.
 - Validez les performances de l'application avant le déploiement.
 - Testez la compatibilité des applications avec différents types d'instances.
- Testez les paramètres du parc en utilisant des configurations de capacité du parc telles que la capacité minimale et maximale, les politiques de dimensionnement, les paramètres de session tels que la durée maximale des sessions et les paramètres de délai de déconnexion.

Pensez à la sympathie mécanique

Choisissez des services cloud en fonction des exigences et des modèles d'utilisation spécifiques de votre charge de travail afin de garantir des performances et une efficacité optimales.

- Choisissez les instances Graphics G5 pour les applications gourmandes en ressources graphiques, les applications qui nécessitent un logiciel de visualisation DirectX, OpenGL, OpenCL ou 3D.
- Sélectionnez `stream.standard` des instances pour les applications professionnelles, les navigateurs Web et les applications graphiques légères
- Surveillez et ajustez le protocole de streaming en fonction de CloudWatch métriques telles que `StreamingSessionLatency`.
- Configurez VPCs les WorkSpaces applications les plus proches de vos utilisateurs et utilisez la bande passante réseau appropriée en fonction des exigences de votre application.
- Choisissez le type de flotte approprié en fonction du comportement de l'application. Par exemple, choisissez des flottes mono-session pour les applications qui nécessitent des ressources dédiées et des flottes multisessions pour les applications capables de partager des ressources efficacement.
- Tenez compte de la compatibilité des applications avec les environnements multisessions.
- Utilisez la [fonctionnalité de redirection du système de fichiers](#) pour gérer les interactions entre les applications distantes et locales. Pour plus d'informations, consultez le billet de AWS blog [Lancer des applications locales à partir d'une session de streaming Amazon WorkSpaces Applications](#).

Pilier d'optimisation des coûts

Le [pilier d'optimisation des coûts](#) du AWS Well-Architected Framework vise à maximiser la valeur commerciale tout en minimisant les dépenses. Cela permet de garantir que chaque dollar que vous dépensez en ressources cloud contribue efficacement à la réalisation des objectifs de votre organisation.

Principaux domaines d'intérêt pour appliquer ce pilier à votre environnement de streaming d'WorkSpaces applications :

- Gestion de la capacité du parc et sélection du type d'instance
- Optimisation du dimensionnement et de la planification
- Surveillance et analyse des modèles d'utilisation
- Répartition et suivi des coûts

Mettre en œuvre la gestion financière dans le cloud

Développez des capacités organisationnelles dédiées à la gestion financière du cloud et à l'optimisation des coûts grâce à des programmes et processus structurés afin de maximiser la valeur et l'efficacité du cloud.

- Surveillez les coûts WorkSpaces des applications en utilisant [AWS Cost Explorer](#) des rapports d'utilisation pour suivre l'utilisation des heures de streaming, analyser les coûts des instances du parc et surveiller la répartition des coûts au niveau régional.
- Planifiez et définissez le contrôle des coûts en définissant des alertes [AWS Budgets](#) concernant les coûts globaux WorkSpaces des services des applications, en créant des seuils budgétaires pour le service et en surveillant les dépenses réelles par rapport aux montants budgétisés. Pour plus d'informations, consultez le billet de AWS blog [How to use automation to optimize and control cost of Amazon WorkSpaces Applications](#).

Ajouter un modèle de consommation

Adaptez les ressources informatiques et les coûts en fonction des modèles d'utilisation réels. Par exemple, vous pouvez fermer les environnements hors production en dehors des heures de bureau pour optimiser les dépenses.

- Choisissez le modèle de tarification approprié. Par exemple, utilisez des flottes permanentes pour une utilisation cohérente et des flottes à la demande pour des charges de travail variables.
- Sélectionnez les types d'instances optimaux. Par exemple, utilisez `stream.standard` des instances pour des applications générales et utilisez des instances graphiques (G4dn) uniquement lorsque cela est nécessaire.

Mesurer l'efficacité globale

Calculez et suivez les résultats cost-per-unit de l'entreprise pour quantifier les améliorations d'efficacité et orienter les efforts d'optimisation.

- Suivez l'efficacité des sessions.
- Surveillez l'utilisation de la flotte à l'aide CloudWatch des indicateurs suivants :
 - `AvailableCapacity` pour suivre la capacité inutilisée
 - `InUseCapacity` pour mesurer l'utilisation réelle
- Calculez et suivez les coûts par session tels que le coût par heure de diffusion, le coût par utilisateur et le coût par application.
- Mettez en œuvre l'[optimiseur de coûts pour les WorkSpaces applications](#) afin de surveiller vos constructeurs.
- Comparez les coûts entre les types de flotte. Par exemple, comparez :
 - Coûts de licence pour les sessions uniques et multisessions
 - Taux d'utilisation des ressources
 - Densité d'utilisateurs par instance
- Utilisez les données de suivi des processus pour identifier les applications sous-utilisées ou inutiles. Pour plus d'informations, consultez le billet de AWS blog [Track user process in Amazon WorkSpaces Applications sessions](#).

Arrêtez de dépenser de l'argent pour soulever des objets lourds de manière indifférenciée

AWS gère les opérations d'infrastructure et propose des services gérés afin que votre organisation puisse se concentrer sur les objectifs commerciaux plutôt que sur la maintenance informatique.

- Créez et gérez des images d'applications à l'aide d'Image Builder pour emballer vos applications, configurer les paramètres des applications et tester la compatibilité des applications.
- Configurez les spécifications du parc en sélectionnant les types d'instances appropriés, en définissant des seuils de dimensionnement et en définissant les limites de capacité souhaitées.
- Configurez des options de stockage persistant en configurant des dossiers personnels dans [Amazon S3](#) pour les flottes basées sur Windows et des systèmes de fichiers partagés dans Amazon [EFS](#) pour les flottes basées sur Linux. Définissez les autorisations de stockage et les politiques de rétention.

Analyser et attribuer les dépenses

Le cloud permet un suivi précis de l'utilisation des ressources et des coûts par charge de travail, ce qui permet de mesurer avec précision le retour sur investissement (ROI) et de cibler les opportunités d'optimisation.

- Mettez en œuvre une stratégie de balisage complète pour les flottes pour la répartition des coûts, les images pour le suivi des actifs, les générateurs d'images pour la désignation de l'environnement et les piles pour le regroupement organisationnel.
- Utilisez les [rapports sur les AWS coûts et l'utilisation \(AWS CUR\)](#) pour WorkSpaces ventiler les coûts des applications par ressource balisée et analyser les coûts par parc, par pile et par image.
- Utilisez-le [AWS Cost Explorer](#) pour visualiser WorkSpaces les tendances des dépenses liées aux applications et comparer les coûts selon différentes dimensions, telles que les régions et les types d'instances.
- Surveillez et analysez les taux d'utilisation du parc, l'efficacité des types d'instances et les heures de streaming par application.
- Suivez la capacité réservée inutilisée, les flottes ou les piles sous-utilisées et les périodes d'inactivité liées à l'utilisation du parc.
- Calculez et suivez le coût par utilisateur pour chaque application, les heures de streaming par application et les taux d'adoption des applications diffusées par les utilisateurs.
- Configurez une analyse détaillée de l'utilisation en configurant les rapports d'utilisation des WorkSpaces applications, en utilisant [Amazon Athena](#) pour interroger les données d'utilisation et en créant des visualisations dans [Amazon Quick](#) pour obtenir des informations sur les coûts et l'utilisation.

- Évaluez les considérations relatives au coût total, telles que les licences Windows Server, les modèles de licences d'applications et les licences par utilisateur par rapport aux licences par appareil.
- Utilisez Amazon Athena pour interroger et analyser les coûts de stockage des dossiers personnels et les modèles d'utilisation par utilisateur. Pour plus d'informations, consultez le billet de AWS blog [Comment signaler l'utilisation du dossier d'accueil d'Amazon WorkSpaces Applications avec Amazon Athena](#).

Pilier de durabilité

Le [pilier du développement durable](#) du AWS Well-Architected Framework met l'accent sur la réduction de votre empreinte environnementale et sur l'optimisation de la consommation et de l'efficacité énergétiques. Il aide les architectes à prendre des décisions respectueuses de l'environnement dans le cadre de la conception de leurs systèmes et de leurs stratégies d'allocation des ressources.

Principaux domaines d'intérêt pour appliquer ce pilier à votre environnement de streaming d'WorkSpaces applications :

- Comprendre et optimiser l'allocation des ressources pour répondre à la demande réelle et minimiser le gaspillage dans les environnements de streaming
- Analyser les habitudes de consommation des utilisateurs et s'y adapter afin d'améliorer l'efficacité de la diffusion des applications et des sessions de streaming
- Sélection et utilisation de configurations matérielles appropriées pour optimiser l'efficacité énergétique tout en répondant aux exigences de performance
- Utilisation des fonctionnalités de services AWS gérés pour bénéficier des économies d'échelle et des fonctionnalités d'efficacité intégrées offertes par ces services

Comprenez votre impact

Surveillez et optimisez l'impact environnemental de votre charge de travail en mesurant l'efficacité des ressources et les émissions par unité de production. Utilisez ces données pour établir KPIs et orienter les améliorations en matière de durabilité.

- Surveillez les modèles d'utilisation de la flotte.
- Suivez les heures de streaming par utilisateur.
- Analysez les tendances d'utilisation de la capacité du parc.

Fixer des objectifs de durabilité

Définissez des objectifs de durabilité mesurables pour chaque charge de travail, conformément aux objectifs de l'organisation. Concentrez-vous sur la réduction de l'intensité des ressources par transaction à mesure que vous évoluez.

- Définissez des objectifs en matière de taux d'utilisation de la flotte, d'efficacité des types d'instances et d'optimisation des heures de streaming.
- Planifiez la capacité en fonction des modèles d'utilisation réels.

Optimiser l'utilisation

Optimisez l'efficacité de la charge de travail en dimensionnant correctement les ressources et en maximisant l'utilisation. Réduisez la capacité d'inactivité pour minimiser la consommation d'énergie et améliorer la durabilité.

- Configurez le dimensionnement automatique pour répondre à la demande réelle.
- Dimensionnez correctement la capacité du parc en fonction des modèles d'utilisation.
- Mettez en œuvre des limites de capacité minimale et maximale appropriées.
- Choisissez les types d'instances appropriés pour les charges de travail.
- Surveillez et optimisez la densité des sessions de streaming.
- Réduisez la capacité d'inactivité pendant les heures creuses.

Anticipez et adoptez de nouvelles offres matérielles et logicielles plus efficaces

Tenez-vous au courant des nouvelles technologies efficaces proposées par les partenaires et fournisseurs et adoptez-les rapidement afin d'améliorer en permanence l'impact environnemental de votre charge de travail.

- Utilisez les types d'instances de la génération actuelle.
- Effectuez une mise à niveau vers de nouveaux types d'instances lorsqu'ils sont disponibles.
- Optimisez les paramètres de diffusion des applications.
- Configurez les protocoles de diffusion appropriés.
- Mise à jour vers les dernières fonctionnalités WorkSpaces des applications.

Services gérés d'occasion

Tirez parti des services cloud partagés et des solutions gérées pour optimiser l'efficacité de l'utilisation des ressources tout en minimisant l'impact environnemental grâce à une mise à l'échelle et à une gestion du cycle de vie automatisées.

- Utilisez [Amazon S3](#) pour le stockage utilisateur pour les flottes basées sur Windows et Amazon [EFS](#) pour les systèmes de fichiers partagés pour les flottes basées sur Linux.
- Implémenter [CloudWatch](#) pour la surveillance.
- Configurez [IAM](#) pour la gestion des accès.

Réduisez l'impact en aval de vos charges de travail dans le cloud

Concevez des services visant à minimiser les besoins en ressources côté client, à réduire la consommation d'énergie et à prolonger la durée de vie des appareils pour les utilisateurs.

- Ajustez la durée maximale des sessions pour éviter toute consommation inutile de ressources.
- Configurez les délais d'expiration de session appropriés.
- Définissez des politiques de délai de déconnexion.
- Mettez en œuvre des politiques de persistance des sessions si nécessaire.

Ressources

AWS documentation

- [AWS Framework Well-Architected](#)
- [Guide d'administration WorkSpaces des applications Amazon](#)
- [Guide de CloudWatch l'utilisateur Amazon](#)
- [Guide de l'utilisateur Amazon EFSS](#)
- [Guide de l'utilisateur Amazon S3](#)
- [Guide de l'utilisateur IAM](#)

AWS articles de blog

- [WorkSpaces Applications basées sur l'appartenance à un groupe Active Directory Ciblage des applications](#)
- [Créez un fournisseur d'identité unique pour tous vos Amazon WorkSpaces Applications Stacks avec Azure AD](#)
- [Configuration de l'assistance à distance Windows pour Amazon WorkSpaces et Amazon WorkSpaces Applications](#)
- [Création d'un enregistrement AS2 TrustedDomains DNS TXT pour rediriger le client natif d'Amazon WorkSpaces Applications vers un fournisseur d'identité tiers](#)
- [Création d'une journalisation personnalisée et d' CloudWatch alertes Amazon dans Amazon Applications WorkSpaces](#)
- [Redirection entre régions avec Geo Targetly et Amazon Applications WorkSpaces](#)
- [Ressources multi-comptes et applications Amazon WorkSpaces](#)
- [Activez la fédération avec BIO-key PortalGuard et Amazon Applications WorkSpaces](#)
- [Activer la fédération avec les WorkSpaces applications Simple SAMLphp et Amazon](#)
- [Activer la fédération des identités avec Duo Single Sign-On et Amazon Applications WorkSpaces](#)
- [Activer la fédération des identités avec les applications Shibboleth et Amazon WorkSpaces](#)
- [Stratégies de basculement pour le VDI sur site avec Amazon End User Computing](#)

- [Comment Amazon utilise les WorkSpaces applications Amazon pour permettre aux data scientists et aux analystes d'accéder à des données sensibles](#)
- [Comment configurer l'authentification basée sur des certificats pour Amazon Applications WorkSpaces](#)
- [Comment utiliser les demandes Okta avec les droits d'application pour Amazon Applications WorkSpaces](#)
- [Gestion des laboratoires informatiques sur les WorkSpaces applications Amazon avec la gestion des applications virtuelles open source](#)
- [Méthodes d'allocation des coûts de vos WorkSpaces applications à vos unités commerciales](#)
- [Surveillance des WorkSpaces applications Amazon avec Amazon OpenSearch Service et Amazon Kinesis Data Firehose](#)
- [Séparation du réseau et désinfection des données à l'aide d'Amazon WorkSpaces, d'Amazon WorkSpaces Applications et d'Amazon Macie](#)
- [OneLogin SSO avec Amazon Applications WorkSpaces](#)
- [Optimisez le chemin audio de vos appels Amazon Connect avec Amazon WorkSpaces Applications](#)
- [Stockage permanent pour les flottes Amazon WorkSpaces Applications Linux sur Amazon Elastic File System](#)
- [Rediriger une application Okta SAML vers le client natif Amazon WorkSpaces Applications](#)
- [Simplifiez la gestion WorkSpaces des images Amazon Applications grâce au masquage des applications](#)
- [Diffusez des applications à moindre coût grâce à Amazon WorkSpaces Applications, aux flottes élastiques et à la compatibilité avec Linux.](#)
- [Streaming depuis les points de terminaison VPC de l'interface pour les environnements réglementés avec applications WorkSpaces](#)
- [Utiliser les droits WorkSpaces des applications Amazon Applications avec Azure AD](#)
- [Signalateur de problèmes utilisateur pour Amazon WorkSpaces Applications](#)
- [Utilisation des droits WorkSpaces d'application Amazon Applications avec Google Workspace](#)
- [Utilisation d'Auth0 avec Microsoft Active Directory sur Amazon Applications WorkSpaces](#)
- [Utilisation AppLocker de Microsoft pour gérer l'expérience applicative sur Amazon WorkSpaces Applications](#)

- [Utilisation de Python pour alimenter une interface utilisateur graphique d' WorkSpaces Applications Linux Imaging Assistant](#)
- [Options de redirection d'applications Web pour le client WorkSpaces Applications](#)

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un [fil RSS](#).

Modification	Description	Date
Publication initiale	—	23 juillet 2025

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 réplique bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration [active-passive](#).

migration active-passive

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

fonction d'agrégation

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

AI

Voir [intelligence artificielle](#).

AIOps

Voir les [opérations d'intelligence artificielle](#).

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez [ABAC pour AWS](#) dans la documentation Gestion des identités et des accès AWS (IAM).

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

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

B

mauvais bot

Un [bot](#) destiné à perturber ou à nuire à des individus ou à des organisations.

BCP

Consultez la section [Planification de la continuité des activités](#).

graphique de comportement

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

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi [endianité](#).

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

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

planification de la continuité des activités (BCP)

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

C

CAF

Voir le [cadre d'adoption du AWS cloud](#).

déploiement de Canary

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

CCo E

Voir [le Centre d'excellence du cloud](#).

CDC

Voir [capture des données de modification](#).

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez [l'intégration continue et la livraison continue](#).

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

Consultez la base de [données de gestion des configurations](#).

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir [vision par ordinateur](#).

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir [langage de définition de base](#) de données.

ensemble profond

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

deep learning

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

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de

la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une défense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

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

déploiement

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

environnement de développement

Voir [environnement](#).

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

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

reprise après sinistre (DR)

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

DML

Voir [langage de manipulation de base](#) de données.

conception axée sur le domaine

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

DR

Voir [reprise après sinistre](#).

détection de dérive

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

pour [détecter les modifications de votre zone d'atterrissage](#) susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la [cartographie de la chaîne de valeur du développement](#).

E

EDA

Voir [analyse exploratoire des données](#).

EDI

Voir échange [de données informatisé](#).

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir [point de terminaison de service](#).

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environnement

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

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

environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

épopée

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

ERP

Voir [Planification des ressources d'entreprise](#).

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des

charges de travail. Pour plus d'informations, consultez la section [Limites d'isolation des AWS pannes](#).

branche de fonctionnalités

Voir [succursale](#).

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

Découvrez le [contrôle d'accès détaillé](#).

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le [modèle de fondation](#).

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les [restrictions géographiques](#).

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez [la haute disponibilité](#).

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiques

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

laC

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.

Ilo T

Voir [Internet industriel des objets](#).

infrastructure immuable

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

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'[architecture AWS de référence de sécurité](#) recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes

I

et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

migration incrémentielle

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

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

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

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. [L'architecture AWS de référence de sécurité](#) recommande de configurer votre compte réseau

avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir [Internet des objets](#).

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la [bibliothèque d'informations informatiques](#).

ITSM

Voir [Gestion des services informatiques](#).

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection

entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'[accès basé sur des étiquettes](#).

principe de moindre privilège

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

lift and shift

Voir [7 Rs](#).

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi [endianité](#).

LLM

Voir le [grand modèle de langage](#).

environnements inférieurs

Voir [environnement](#).

M

machine learning (ML)

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

branche principale

Voir [succursale](#).

malware

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

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir [Migration Acceleration Program](#).

mécanisme

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

compte membre

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

MAILLES

Voir le [système d'exécution de la fabrication](#).

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

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

microservice

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

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir [apprentissage automatique](#).

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir [Évaluation du portefeuille de migration](#).

MQTT

Voir [Message Queuing Telemetry Transport](#).

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir [Contrôle d'accès à l'origine](#).

OAI

Voir [l'identité d'accès à l'origine](#).

OCM

Voir [gestion du changement organisationnel](#).

migration hors ligne

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

OI

Consultez la section [Intégration des opérations](#).

OLA

Voir l'accord [au niveau opérationnel](#).

migration en ligne

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

OPC-UA

Voir [Open Process Communications - Architecture unifiée](#).

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

Voir l'[examen de l'état de préparation opérationnelle](#).

DE

Voir [technologie opérationnelle](#).

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les [informations personnelles identifiables](#).

manuel stratégique

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

PLC

Voir [contrôleur logique programmable](#).

PLM

Consultez la section [Gestion du cycle de vie des produits](#).

policy

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

Entité AWS capable d'effectuer des actions et d'accéder aux ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus

d'informations, veuillez consulter la rubrique Principal dans [Termes et concepts relatifs aux rôles](#), dans la documentation IAM.

confidentialité dès la conception

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

zones hébergées privées

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

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir [environnement](#).

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

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

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

Voir [responsable, responsable, consulté, informé \(RACI\)](#).

RAG

Voir [Retrieval Augmented Generation](#).

rançongiciel

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

Matrice RASCI

Voir [responsable, responsable, consulté, informé \(RACI\)](#).

RCAC

Voir [contrôle d'accès aux lignes et aux colonnes](#).

réplica en lecture

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

réarchitecte

Voir [7 Rs](#).

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir [7 Rs](#).

Région

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

régression

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

réhéberger

Voir [7 Rs](#).

version

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

déplacer

Voir [7 Rs](#).

replateforme

Voir [7 Rs](#).

rachat

Voir [7 Rs](#).

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir [7 Rs](#).

se retirer

Voir [7 Rs](#).

Génération augmentée de récupération (RAG)

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

rotation

Processus de mise à jour périodique d'un [secret](#) pour empêcher un attaquant d'accéder aux informations d'identification.

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

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

RPO

Voir l'[objectif du point de récupération](#).

RTO

Voir l'[objectif en matière de temps de rétablissement](#).

runbook

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

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter

AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter [À propos de la fédération SAML 2.0](#) dans la documentation IAM.

SCADA

Voir [Contrôle de supervision et acquisition de données](#).

SCP

Voir la [politique de contrôle des services](#).

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les

données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de [niveau de service](#).

modèle de responsabilité partagée

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

SIEM

Consultez les [informations de sécurité et le système de gestion des événements](#).

point de défaillance unique (SPOF)

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

SLA

Voir le contrat [de niveau de service](#).

SLI

Voir l'indicateur de [niveau de service](#).

SLO

Voir l'objectif de [niveau de service](#).

split-and-seed modèle

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

SPOF

Voir [point de défaillance unique](#).

schéma en étoile

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

modèle de figuier étrangleur

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

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

tags

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

variable cible

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

liste de tâches

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

environnement de test

Voir [environnement](#).

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de

confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section [Utilisation AWS Organizations avec d'autres AWS services](#) dans la AWS Organizations documentation.

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir [environnement](#).

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

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

VER

Voir [écrire une fois, lire plusieurs](#).

WQF

Voir le [cadre AWS de qualification de la charge](#) de travail.

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité « jour zéro »

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

invite Zero-Shot

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

application zombie

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

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