



Replateforme du COTS et des applications internes lors d'une migration vers le cloud AWS

# AWS Conseils prescriptifs



# AWS Conseils prescriptifs: Replateforme du COTS et des applications internes lors d'une migration vers le cloud AWS

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

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

---

# Table of Contents

Introduction .....	1
Résultats commerciaux ciblés .....	3
Choix de l'environnement de replatforme .....	4
Replateforme des composants d'application exécutés sur des systèmes d'exploitation non pris en charge .....	5
Remplacement des systèmes d'exploitation ou des serveurs d'applications non pris en charge .....	6
Mise à niveau du système d'exploitation pour les applications COTS .....	6
Mise à niveau du système d'exploitation pour les applications internes .....	7
Replateforme des bibliothèques d'applications et des logiciels dépendants .....	7
Replateforme de bases de données backend .....	8
Replateforme des bases de données backend pour les applications COTS .....	8
Replateforme des bases de données backend pour les applications internes .....	9
Replateforme de partages de fichiers .....	10
Mise à jour des composants de journalisation et de surveillance .....	11
Test et validation de vos applications .....	12
Automatisation du système d'exploitation .....	13
Utilisation des outils d'automatisation et de l'infrastructure en tant que code (iAC) .....	13
FAQ .....	15
Quand devrais-je choisir de reprogrammer plutôt que de le réhéberger ? .....	15
Puis-je refactionner mon application COTS vers une base de données open source ? .....	15
Mise d'AWS puis-je utiliser pour réhéberger rapidement mes serveurs sur le AWS Cloud ? .....	15
Mise d'AWS les outils que je peux utiliser pour replatformer mes applications ? .....	16
Ressources .....	17
Références .....	17
Outils .....	17
Historique du document .....	18
Glossaire .....	19
# .....	19
A .....	20
B .....	23
C .....	24
D .....	28
E .....	32

---

F .....	34
G .....	35
H .....	36
I .....	38
L .....	40
M .....	41
O .....	45
P .....	47
Q .....	50
R .....	50
S .....	53
T .....	56
U .....	58
V .....	59
W .....	59
Z .....	60
.....	lxii

# Replateforme du COTS et des applications internes lors d'une migration vers le cloud AWS

Anbu Selvan, Amazon Web Services () AWS

Mars 2021 ([historique du document](#))

Ce guide décrit sept domaines sur lesquels vous devez vous concentrer lorsque vous replateformez des applications commerciales off-the-shelf (COTS) et internes dans le cloud Amazon Web Services (AWS). Le guide fournit également des stratégies, des outils et des AWS services pour vous aider à reconfigurer les composants de l'application. Les applications COTS sont des applications tierces prêtes à l'emploi qui peuvent être achetées sur un marché commercial (par exemple, [AWS Marketplace](#)). Les applications internes sont développées et utilisées en interne par votre organisation.

Après avoir décidé de migrer votre COTS ou vos applications internes vers le AWS Cloud, vous devez évaluer laquelle des sept stratégies de migration courantes ([7 R](#)) utiliser. Ces stratégies sont le refactoring, la replateforme, le rachat, le réhébergement, la relocalisation, la rétention et le retrait. Nous vous recommandons de reconfigurer les applications qui utilisent des composants ou des bases de données qui ont atteint ou sont sur le point d'atteindre leur date end-of-support (EOS). EOS, c'est lorsqu'un fournisseur retire son support technique pour un produit. Si vous choisissez de reconfigurer une application dans le AWS cloud, vous pouvez bénéficier des fonctionnalités suivantes :

- Automatisez [les mises à niveau du système d'exploitation \(OS\)](#) sur place avec AWS Systems Manager.
- Utilisez les volumes de stockage de snapshots pour créer rapidement des Amazon Machine Images (AMI) à partir d'instances Amazon Elastic Compute Cloud (Amazon EC2).
- Créez un sous-réseau privé pour isoler les charges de travail exécutées sur des systèmes d'exploitation (OS) obsolètes.
- Utilisez le réseau haut débit pour répliquer rapidement les environnements de production afin de tester le replateformage.
- Configurez rapidement une pile d'applications distincte avec des instances EC2 à la demande, sans utiliser de matériel supplémentaire sur site.

Pour bénéficier de ces fonctionnalités et des autres fonctionnalités disponibles sur le AWS Cloud, nous vous recommandons de réhéberger d'abord votre application en utilisant [AWS Application Migration Service](#). Vous pouvez ensuite mettre à jour l'application dans le AWS cloud. La liste suivante fournit des exemples de cas dans lesquels une application doit être replatformée :

- Support n'est plus disponible pour le système d'exploitation, les environnements d'exécution (par exemple, [Apache Tomcat](#), [JBoss](#) ou [Oracle WebLogic Server](#)), les bases de données ou les composants d'exécution (par exemple, Java, Python ou Perl) de l'application.
- L'application doit devenir plus résiliente et se remettre automatiquement en cas de panne (bogues logiciels ou problèmes d'infrastructure, par exemple).
- De nouvelles fonctionnalités d'application sont nécessaires pour de nouveaux segments de clientèle ou pour prendre en charge des charges accrues.
- L'application est instable et doit être améliorée pour améliorer la stabilité opérationnelle.

Avant de commencer le processus de replatforme, vous devez explorer des alternatives aux fonctionnalités de votre application ; par exemple, évaluez si vous pouvez les remplacer par une solution SaaS (Software as a Service) d'un éditeur de logiciels indépendant (ISV). [Vous pouvez également être en mesure de reconstruire les fonctionnalités de l'application en utilisant AWS des services tels qu'AWS Lambda Amazon Cognito, Amazon MQ AWS Glue, Amazon ou QuickSight Amazon Aurora.](#)

Ce guide s'adresse aux administrateurs informatiques, aux propriétaires d'applications, aux architectes, aux responsables techniques et aux chefs de projet. Le guide fournit les sept domaines suivants sur lesquels vous devez vous concentrer lorsque vous replatformez le COTS et des applications internes dans le AWS cloud :

- [Choix de l'environnement de replatforme](#)
- [Replateforme des composants d'application exécutés sur des systèmes d'exploitation non pris en charge](#)
- [Replateforme de bases de données backend](#)
- [Replateforme de partages de fichiers](#)
- [Mise à jour des composants de journalisation et de surveillance](#)
- [Test et validation de vos applications](#)
- [Automatisation du système d'exploitation](#)

## Résultats commerciaux ciblés

Vous devez vous attendre aux quatre résultats suivants après la replateforme du COTS et des applications internes dans le cloud : AWS

- Réduisez les risques de sécurité liés aux applications existantes qui exécutent des logiciels ou des systèmes d'exploitation non pris en charge.
- Réduisez le coût global de propriété de vos applications en supprimant les éditions de base de données coûteuses et non essentielles ou en adoptant des bases de données open source.
- Réduisez les frais opérationnels en utilisant des bases de données AWS gérées (par exemple, [Amazon Relational Database Service \(Amazon RDS\)](#) ou Aurora) pour améliorer la disponibilité et la fiabilité de vos applications.
- Rendez les applications existantes plus résilientes en adoptant des fonctionnalités d'automatisation et de surveillance natives du cloud, telles que la CloudWatch surveillance [Amazon](#) ou l'application de correctifs de système d'exploitation basés sur Systems Manager.

## Choix de l'environnement de replateforme

Nous vous recommandons de replateformer une application dans le AWS Cloud pour utiliser des fonctionnalités telles que [Instantanés Amazon Elastic Block Store \(Amazon EBS\)](#) ou le clonage d'un [Instance EC2 pour créer une AMI](#). Ces fonctionnalités facilitent votre processus de mise à niveau et de test.

Généralement, vous commencez par réhéberger l'application sur le AWS Cloud, puis commencez le processus de replateforme. Toutefois, vous devez être prudent si vous migrez des applications présentant des vulnérabilités ou si vous exécutez des logiciels et des systèmes d'exploitation non pris en charge. Ces applications peuvent exposer des vulnérabilités de sécurité dangereuses pour votre migration et vos opérations future. A la place, nous vous recommandons d'utiliser [Application Migration Service](#) pour répliquer les composants de l'application sur un sous-réseau privé avec une sortie limitée. Cette approche isole vos charges de travail, et vous pouvez ensuite les replateformes et les tester en toute sécurité avant qu'elles ne soient déployées dans un environnement de production.

Votre organisation a peut-être acheté une prise en charge étendue du système d'exploitation auprès d'un ISV, ce qui prolonge le correctif du système d'exploitation au-delà de la date officielle d'EOS pour une période de trois à cinq ans. Il s'agit d'une mesure temporaire qui donne plus de temps pour refactionner ou aligner les délais de mise à niveau ou de migration de votre produit avec le calendrier de lancement du produit d'un fournisseur d'applications COTS. Cependant, nous vous recommandons d'utiliser les outils et expertise de [AWS Services professionnels](#) ou [Partenaires de compétences en migration AWS](#) pour replateformer ces charges de travail vers des systèmes d'exploitation plus récents. Cela permet d'éviter les contrats de licence étendus coûteux et vous permet de terminer votre migration plus rapidement.



# Replateforme des composants d'application exécutés sur des systèmes d'exploitation non pris en charge

L'approche de replatforme pour les composants d'application exécutés sur des systèmes d'exploitation non pris en charge est différente pour chaque composant d'application. Le tableau suivant récapitule les options de replatforme disponibles pour les composants d'application ayant atteint EOS.

Composant d'application	Solution pour applications COTS	Solution pour applications internes
Serveur d'application	Effectuez la mise à niveau vers la version recommandée par le fournisseur de l'application.	Identifiez la version la plus récente du serveur d'applications. Créez et validez-le dans un environnement de développement avant de procéder à la mise à niveau.
SE	Effectuez la mise à niveau vers la version recommandée par le fournisseur de l'application.	Identifiez la dernière version du système d'exploitation. Créez et validez-le dans un environnement de développement avant de procéder à la mise à niveau.
bibliothèques d'exécution	Effectuez la mise à niveau vers la version recommandée par le fournisseur de l'application.	Mettez à niveau et validez par rapport à la dernière version.
Autres composants d'application	Demandez de nouveaux binaires d'applications au fournisseur de l'application.	Construisez avec les versions les plus récentes du système d'exploitation, du moteur d'exécution et du serveur d'applications.

Les sections suivantes fournissent de plus amples informations sur les approches de replateforme pour vos composants d'application.

## Remplacement des systèmes d'exploitation ou des serveurs d'applications non pris en charge

Si vous remplacez des serveurs d'applications non pris en charge (par exemple, Apache Tomcat 6.0, Apache 2.2 ou IIS 7.x), les nouvelles versions de votre serveur d'applications peuvent nécessiter une mise à niveau du système d'exploitation sous-jacente. La plupart des systèmes d'exploitation non pris en charge sont Red Hat Enterprise Linux (RHEL) versions 5 et 6, CentOS versions 5 et 6 ou Windows 2008 R2. Vous devez déployer les étapes suivantes pour les applications exécutant ces systèmes d'exploitation :

1. Lancer une instance EC2 avec la version du système d'exploitation requise.
2. Installez la version requise du serveur d'applications.
3. Il existe deux approches distinctes pour les applications internes et COTS :
  - Applications internes: redéployer l'application vers l'instance EC2.
  - Applications COTS— Contactez le fournisseur de l'application et demandez des binaires d'applications certifiés pour les versions requises du système d'exploitation ou du serveur d'applications.

## Mise à niveau du système d'exploitation pour les applications COTS

La plupart des fournisseurs d'applications COTS prennent en charge Windows 2016 ou RHEL 7. Si votre ancienne application COTS ne prend pas en charge Windows 2016, nous recommandons une mise à niveau sur place depuis Windows 2008 R2 vers Windows 2012 R2 à l'aide du [option de mise à niveau sur place fournie par Microsoft](#). Vous pouvez également utiliser [AWS Systems Manager Runbooks Automation](#) pour mettre à niveau automatiquement Windows Server exécuté sur des instances EC2. Nous vous recommandons de contacter le fournisseur de l'application et de lui demander de certifier son logiciel pour la dernière version du système d'exploitation.

Pour les applications COTS héritées qui exécutent Windows Server et ne fonctionnent pas avec le système d'exploitation le plus récent, nous vous recommandons d'utiliser le [Programme de migration](#)

---

[de fin de support AWS \(EMP\) pour Windows Server](#) pour emballer l'application et l'exécuter sur la dernière version Windows dans un environnement EC2.

## Mise à niveau du système d'exploitation pour les applications internes

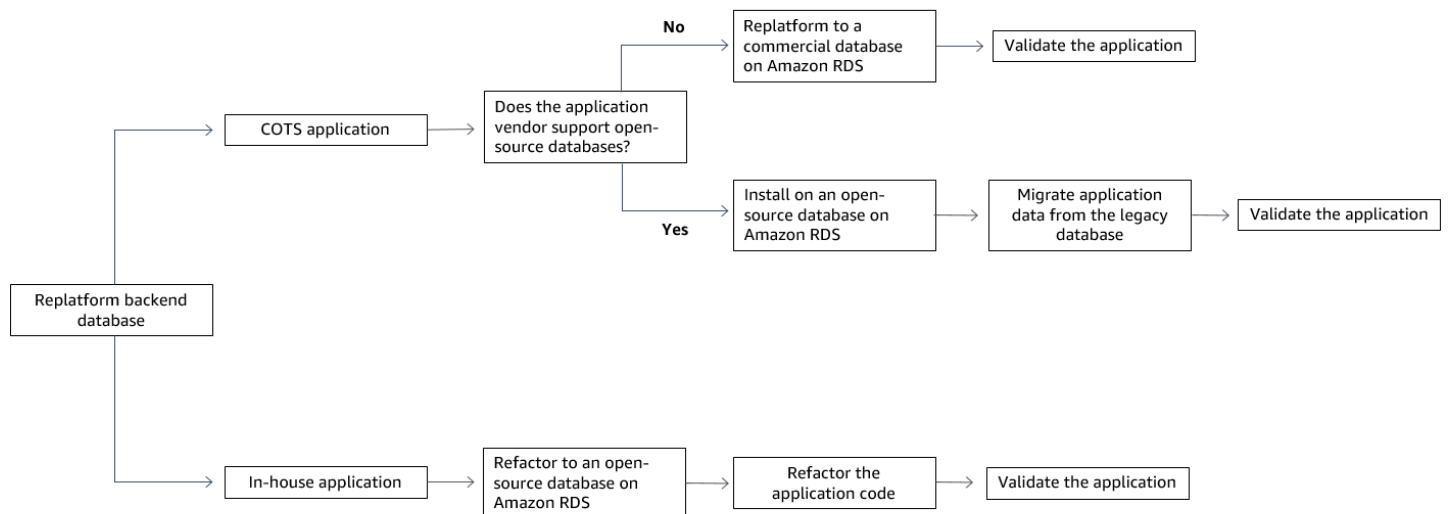
Nous vous recommandons de compiler et de reconstruire le logiciel de votre application interne à l'aide des versions les plus récentes du système d'exploitation et de l'exécution logicielle (par exemple, Java, C++, .NET ou Python). Vous pouvez ensuite cloner l'environnement d'application existant, déployer et valider manuellement la fonctionnalité, et mettre à jour votre environnement de génération vers le système d'exploitation, les composants logiciels d'exécution et les bibliothèques les plus récents avant de passer à votre environnement de production.

## Replateforme des bibliothèques d'applications et des logiciels dépendants

L'approche de replatforme des bibliothèques d'applications et des logiciels dépendants est similaire à celle des systèmes d'exploitation, mais vous ne mettez à niveau que les bibliothèques. Vous testez ensuite la fonctionnalité de l'application et répliquez les bibliothèques requises dans vos serveurs de préproduction et de production. En règle générale, le fournisseur de l'application COTS gère les mises à jour requises pour les composants de l'application via leurs versions logicielles en cours.

# Replateforme de bases de données backend

L'approche de replatforme des bases de données backend est différente pour les applications COTS et internes. En effet, le code source n'est généralement disponible que pour les applications internes. L'illustration suivante montre les options de replatforme disponibles pour les bases de données backend de votre application.



Les sections suivantes expliquent les approches de replatforme des bases de données backend appartenant à COTS ou à des applications internes.

## Replateforme des bases de données backend pour les applications COTS

Nous vous recommandons d'utiliser une base de données Aurora si votre application COTS prend en charge des bases de données open source. L'utilisation d'une base de données open source permet de réduire les coûts de licence, et vous pouvez également utiliser des outils tels que [AWS Schema Conversion Tool\(AWS SCT\)](#) et [AWS Database Migration Service\(AWS DMS\)](#) pour réaliser une coupure avec un temps d'arrêt minimal pendant votre migration.

Si votre application COTS ne prend pas en charge les bases de données open source, nous vous recommandons de le replacer en une base de données commerciale sur Amazon Relational Database Service (Amazon RDS) telle que [Amazon RDS pour Oracle](#) ou [Amazon RDS pour Microsoft SQL Server](#). Vous devez évaluer les fonctionnalités de base de données utilisées par votre

application et vous assurer qu'elles sont prises en charge dans Amazon RDS avant de commencer votre migration. Pour de plus amples informations, veuillez consulter [Limites propres aux instances de bases de données Microsoft SQL Server](#) dans la documentation Amazon RDS.

Vous pouvez également utiliser vos licences de base de données restantes et exécuter des bases de données commerciales autogérées sur des instances EC2. Si vous choisissez cette approche, nous vous recommandons de commencer le processus de vérification des licences avec le fournisseur de votre base de données. Une fois le processus de vérification des licences terminé, vous devez concevoir une solution de base de données autogérée sur Amazon EC2 pour l'objectif de temps de récupération (RTO) ou l'objectif de point de récupération (RPO) requis par votre application.

Enfin, nous recommandons de replacer les applications COTS hautes performances sensibles à la sécurité qui utilisent des bases de données SQL Server vers SQL Server exécutées sur des instances Linux Amazon EC2. Pour plus d'informations à ce sujet, veuillez consulter [Migration de vos charges de travail SQL Server Windows locales vers Amazon EC2 Linux](#).

## Replateforme des bases de données backend pour les applications internes

Vous pouvez réduire les coûts de licence de votre base de données et augmenter l'évolutivité en replatform les bases de données backend de votre application interne pour AWS bases de données gérées (par exemple, [Amazon RDS pour PostgreSQL](#), [Amazon RDS pour MySQL](#), [Aurora](#), ou [Amazon DynamoDB](#)).

Les bases de données gérées AWS vous aident à réduire les tâches administratives récurrentes pour vos bases de données (par exemple, effectuer des sauvegardes ou appliquer des correctifs aux bases de données et aux systèmes d'exploitation). Si vous utilisez des déploiements Amazon RDS Multi-AZ, vous pouvez également augmenter la disponibilité de votre application en évitant les pannes dues à des défaillances matérielles de base de données. Les bases de données multi-AZ sont répliquées en continu vers une autre zone de disponibilité et l'application bascule de manière transparente vers la base de données répliquée pendant les pannes.

Vous pouvez utiliser AWS DMS et AWS SCT pour convertir des bases de données commerciales en Aurora et Amazon RDS. AWS SCT automatise le processus de conversion du schéma de base de données, et AWS DMS permet la répllication des données depuis des bases de données locales vers Amazon RDS. AWS DMS permet également de réduire les temps d'arrêt minimes lorsque vous migrez des applications locales vers le AWS cloud.

## Replateforme de partages de fichiers

Si vos applications internes utilisent des partages de fichiers externes locaux, tels que Network File Systems (NFS) ou Server Message Block (SMB), nous vous recommandons de modifier le code de l'application pour utiliser Amazon Simple Storage Service (Amazon S3) et [Amazon CloudFront](#). Toutefois, si un accès basé sur des blocs est requis, vous pouvez utiliser [Amazon Elastic File System \(Amazon EFS\)](#) ou [Amazon FSx for Lustre](#). Amazon EFS et Amazon FSx sont AWS Options pour les applications nécessitant un stockage de fichiers partagés.

Pour les applications COTS, nous recommandons de migrer les données des partages de fichiers locaux vers Amazon EFS sous Linux ou [FSx for Windows File Server](#). Vous devez exposer les partages de fichiers basés sur des blocs à l'application de la même manière que les partages de fichiers locaux sont exposés. Amazon EFS et Amazon FSx fournissent des partages de fichiers basés sur NFS et SMB avec les mêmes fonctionnalités que les partages de fichiers locaux fournis. Pour utiliser Amazon EFS ou Amazon FSx pour les partages de fichiers, seules les modifications de configuration sont nécessaires pour les applications COTS.

# Mise à jour des composants de journalisation et de surveillance

Certains environnements hérités utilisent des outils de journalisation et de surveillance centralisés (par exemple, [Splunk](#), [Vents solaires](#), ou [Zabbix](#)) pour la surveillance de l'infrastructure et des applications. Les équipes de support des applications peuvent également utiliser le protocole Secure Shell (SSH) ou le protocole RDP (Remote Desktop Protocol) pour surveiller et déboguer. Pour éviter ce processus manuel et répétitif, vous pouvez utiliser [CloudWatch](#) pour automatiser la surveillance sur le AWScloud.

Nous vous recommandons d'utiliser CloudWatch des métriques pour surveiller votre infrastructure et CloudWatch pour envoyer les journaux d'applications vers CloudWatch. Une fois les journaux d'applications reçus par CloudWatch, vous pouvez créer [Filtres de métriques CloudWatch](#) et utiliser [Alarmes CloudWatch](#) pour surveiller les erreurs d'application et notifier automatiquement les équipes d'assistance.

CloudWatch fournit également des outils permettant de créer des tableaux de bord opérationnels pour les examens continus des opérations de production de vos applications. Les outils de surveillance centralisés tiers peuvent être intégrés à CloudWatch et autres AWS et cela permet d'étendre vos pratiques opérationnelles existantes à l'infrastructure et aux applications sur le AWScloud. Toutefois, vous devrez peut-être recycler vos équipes d'assistance ou d'exploitation si vous choisissez d'utiliser des applications dans le AWScloud. Pour de plus amples informations à ce sujet, consultez le [Perspective des opérations : Gérer et faire évoluer](#) Section du AWS Cadre d'adoption du cloud (AWS Livre blanc CAF).

# Test et validation de vos applications

Les tests fonctionnels et de performances constituent un élément important du processus de replateforme d'une application. En règle générale, les applications héritées reposent sur les connaissances d'un propriétaire d'application pour les tests, car les détails fonctionnels ne sont pas correctement ou entièrement documentés. Cependant, nous vous déconseillons d'enregistrer les cas d'utilisation d'applications à l'aide de tests comportementaux et automatisés. Cette approche permet de valider rapidement et de manière fiable les fonctionnalités d'une application avant et après la replateforme. Vous pouvez utiliser des outils de test automatisés (par exemple, [Sélénium](#), [Tricestis](#), ou [Gatling](#)) pour créer des tests fonctionnels et de performance. Un résultat de référence doit être généré en exécutant des tests fonctionnels et de performances sur votre environnement applicatif actuel. Les résultats des tests entre l'environnement d'application actuel et l'environnement cible peuvent être comparés et utilisés comme critères d'acceptation.

Nous recommandons d'utiliser les tests Canary pour les applications orientées client. Le test Canary teste périodiquement les flux de travail applicatifs critiques dans l'environnement de production et notifie les erreurs aux équipes de support. Pour plus d'informations, consultez le [Déploiement Canary](#) Section du AWS Cadre Well-Architected.



## Automatisation du système d'exploitation

Les applications héritées des centres de données locaux reposent souvent sur des processus opérationnels manuels pour les correctifs continus du système d'exploitation et les mises à jour logicielles. Au cours de votre processus de replateforme, nous vous recommandons d'automatiser le correctif du système d'exploitation en utilisant [Gestionnaire de correctifs pour Systems Manager](#) ou d'autres processus de correctifs automatisés. Patch Manager fournit un processus centralisé et cohérent permettant de recueillir des informations opérationnelles et de mettre en œuvre des tâches opérationnelles de routine sur le [AWS Ressources cloud](#) et sur site.

Nous recommandons de corriger les environnements de développement avant la fenêtre de temps de correction utilisée pour les environnements de production. Pour de plus amples informations à ce sujet, veuillez consulter le [Runbook du Gestionnaire de correctifs](#) pour automatiser le correctif du système d'exploitation. Vous devez également déployer des tests Canary pour tester périodiquement les principales fonctionnalités des applications dans des environnements de préproduction ou de production, et alerter les équipes de support en cas d'échec des tests. Cela permet d'éviter les pannes imprévues de votre application.

## Utilisation des outils d'automatisation et de l'infrastructure en tant que code (iAC)

Dans le cadre du processus de replateforme de votre application, vous devez automatiser les constructions de plateformes à l'aide d'outils de gestion de la configuration tels que [Chef](#), [Puppet](#), ou [Ansible](#). Ces outils permettent une génération répétable de la pile d'applications et formalisent les étapes de génération d'une instance d'application, y compris la configuration de la pile.

Nous vous recommandons de provisionner votre infrastructure en utilisant les meilleures pratiques iAC. Plusieurs options sont disponibles pour cela, notamment [AWS Cloud Development Kit \(AWS CDK\)](#), [AWS CloudFormation](#) et [Terraform](#). Chef, Ansible et Puppet ont également des capacités limitées qui peuvent fournir suffisamment d'automatisation pour votre cas d'utilisation.

Les versions répétables qui utilisent iAC et le code de gestion de la configuration vous aident à tester l'infrastructure sans les frais généraux ni les risques liés à la reconstruction de ces ressources. Le correctif et la mise à jour d'une instance existante peuvent entraîner un état qui rend difficile la reproduction et l'identification des problèmes.

---

Si une application COTS ne prend pas en charge l'installation automatisée, nous vous recommandons de consulter le [Réseau de partenaires AWS \(APN\)](#). Pour de plus amples informations à ce sujet, veuillez consulter le [Perspective de la plateforme Applications et infrastructure](#) Section du AWS Livre blanc des FAC.

# FAQ sur la replateforme des COTS et des applications internes

Cette section fournit des réponses aux questions fréquemment posées sur la replateforme COTS et les applications internes.

## Quand devrais-je choisir de reprogrammer plutôt que de le réhéberger ?

Vous devez replateformer les composants autres que la base de données si le fournisseur du système d'exploitation a interrompu les mises à jour de sécurité (par exemple, RHEL 5 et Windows 2008). Pour les systèmes d'exploitation non pris en charge, vous pouvez réhéberger les composants sur un sous-réseau privé isolé et les mettre à niveau avant de les déployer dans un environnement de production.

Pour les composants de base de données, vous devez évaluer si la replateforme vers une base de données commerciale sur Amazon RDS constitue un choix approprié. Vous pouvez également utiliser une base de données autogérée exécutée sur Amazon EC2 si le fournisseur de la base de données vous autorise à utiliser votre licence actuelle sur leAWScloud.

## Puis-je refactionner mon application COTS vers une base de données open source ?

Il est possible de refactionner une application COTS vers une base de données open source si le fournisseur de votre application prend en charge les bases de données open source. Nous ne recommandons pas d'utiliser des bases de données open source pour les applications COTS sans obtenir le support du fournisseur.

## Mise d'AWS puis-je utiliser pour réhéberger rapidement mes serveurs sur leAWSCloud ?

Vous pouvez utiliser [Application Migration Service](#) en tant que service de migration principal pour soulever et déplacer vos applications versAWS.

# Mise d'AWSles outils que je peux utiliser pour replateformer mes applications ?

Plusieurs outils sont disponibles sur leAWScloud, y compris :

- [Mises à niveau automatisées Systems Manager](#)— Mettez à niveau Windows 2008 et SQL Server 2008 sur leAWScloud.
- [AWS SCT](#)— Convertissez le schéma de base de données des bases de données commerciales en bases de données open source
- [AWS DMS](#)— Répliquer les données des bases de données locales vers leAWScloud, soit sur des bases de données Amazon RDS ou des bases de données exécutées sur Amazon EC2.

# Ressources

## Références

- [AWS Cloud Adoption Framework](#) à partir des [AWS Livre blanc sur la migration](#)
- [Création d'un tableau de bord CloudWatch](#)
- [Limites propres aux instances de bases de données Microsoft SQL Server](#)
- [Migrer une base de données Microsoft SQL Server autogérée vers une base de données entièrement gérée sur Amazon RDS](#)
- [AWS Atelier : Instance de cluster de basculement Microsoft SQL Server sur Amazon FSx](#)
- [Mise à niveau du système d'exploitation Amazon EC2 Windows Server](#)

## Outils

- [AWS CodeBuild](#) et [AWS CodePipeline](#) vous aide à créer des pipelines d'intégration et de développement en continu (CI/CD) sur le cloud AWS.
- [AWS DataSync](#) – DataSync aide à répliquer les magasins de fichiers locaux sur le AWS Cloud.
- [AWS DMS](#) – AWS Database Migration Service (AWS DMS) permet de répliquer les données des bases de données locales vers des bases de données Amazon RDS ou des bases de données Amazon EC2.
- [AWS Systems Manager](#) mises à niveau automatisées basées sur aide à mettre à niveau Windows 2008 et SQL Server 2008 sur le AWS Cloud.
- [AWS SCT](#) – AWS Schema Conversion Tool permet de convertir le schéma de base de données des bases de données commerciales en bases de données open source.
- [Application Migration Service](#) – AWS Application Migration Service est une solution hautement automatisée lift-and-shift solution (réhéberger) qui simplifie, accélère et réduit le coût de la migration des applications vers AWS.
- [Assistant de recréation de plateformes Windows vers Linux pour les bases de données Microsoft SQL Server](#) est un outil de recréation de plateformes.

## Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Si vous souhaitez être alerté des mises à jour à future, abonnez-vous à [Flux RSS](#).

Modification	Description	Date
<a href="#">Nom du service AWS mis à jour</a>	Mis à jourCloudEndure MigrerpourApplication Migration Service	12 mai 2022
<a href="#">=</a>	Publication initiale	12 mars 2021

# Glossaire des recommandations AWS

Les termes suivants sont couramment utilisés dans les politiques, les guides et les modèles fournis par les recommandations AWS. 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 Amazon Aurora Édition compatible avec 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) for Oracle dans le Cloud AWS.
- **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 Cloud AWS.
- **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. Ce scénario de migration est propre à VMware Cloud on AWS, qui prend en charge la compatibilité des machines virtuelles (VM) et la portabilité de la charge de travail entre votre environnement sur site et AWS. Vous pouvez utiliser les technologies VMware Cloud Foundation à partir de vos centres de données sur site lorsque vous migrez votre infrastructure vers VMware Cloud on AWS. Exemple : relocalisez l'hyperviseur hébergeant votre base de données Oracle vers VMware Cloud on AWS.

- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.
- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

## A

### ABAC

Voir contrôle [d'accès basé sur les attributs](#).

services abstraits

Consultez la section [Services gérés](#).

### ACIDE

Voir [atomicité, consistance, isolation, durabilité](#).

migration active-active

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

migration active-passive

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

fonction d'agrégation

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



## AI

Voir [intelligence artificielle](#).

## AIOps

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

## anonymisation

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

## anti-motif

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

## contrôle des applications

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

## portefeuille d'applications

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

## intelligence artificielle (IA)

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

## opérations d'intelligence artificielle (AIOps)

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

## chiffrement asymétrique

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

## atomicité, cohérence, isolement, durabilité (ACID)

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

## contrôle d'accès par attributs (ABAC)

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

## source de données faisant autorité

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

## Zone de disponibilité

Emplacement distinct au sein d'une Région AWS qui est à l'abri des dysfonctionnements d'autres zones de disponibilité et offre une connectivité réseau peu coûteuse et de faible latence par rapport aux autres zones de disponibilité de la même région.

## Framework d'adoption du Cloud AWS (AWS CAF)

Un cadre de directives et de bonnes pratiques d'AWS pour aider les entreprises à élaborer un plan efficient et efficace pour réussir leur migration vers le Cloud AWS. Le CAF organise ses conseils en six domaines prioritaires appelés perspectives : l'entreprise, les personnes, la gouvernance, la plateforme, 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, 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 Workload Qualification Framework (AWS WQF)

Outil qui évalue les charges de travail de migration de base de données, recommande des politiques de migration et fournit des estimations de travail. AWS 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

### 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.

### 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-ArchitectedAWS.

#### 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](#).

## CCoE

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 en local, avant que le Service AWS cible ne les reçoive.

## Centre d'excellence cloud (CCoE)

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

## 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 organisations traversent généralement lorsqu'elles migrent vers le Cloud AWS :

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

Ces étapes ont été définies par Stephen Orban dans le billet de blog [The Journey Toward Cloud-First & the Stages of Adoption](#) sur le blog AWS Cloud Enterprise Strategy. Pour en savoir plus sur la façon dont elles sont liées à stratégie de migration AWS, veuillez consulter 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 AWS CodeCommit. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

## cache passif

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

## données gelées

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

## vision par ordinateur

Domaine de l'IA utilisé par les machines pour identifier des personnes, des lieux et des objets sur des images avec une précision égale ou supérieure à celle de l'être humain. Souvent conçu à partir de modèles d'apprentissage profond, il automatise l'extraction, l'analyse, la classification et la compréhension des informations utiles à partir d'une seule image ou d'une séquence d'images.

## 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

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

## intégration continue et livraison continue (CI/CD)

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

## 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 cadre AWS Well-Architected. 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.

### 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 de 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 sur AWS, vous ajoutez plusieurs contrôles à différentes couches de

la structure AWS Organizations afin de protéger 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 membre AWS 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](#).

### informatique de périphérie

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

### chiffrement

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

### clé de chiffrement

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

### endianisme

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

### point de terminaison

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

### service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et

accorder des autorisations à d'autres Comptes AWS ou aux principaux AWS Identity and Access Management (IAM). 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).

## chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, veuillez consulter la rubrique [Envelope encryption](#) 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 pipeline CI/CD, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

## épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les épopées AWS CAF en matière de sécurité comprennent la gestion des identités et des accès, les contrôles de détection, la sécurité de l'infrastructure, 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](#).

## 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.

## 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.

## G

### blocage géographique

Voir les [restrictions géographiques](#).

### restrictions géographiques (blocage géographique)

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

## Flux de travail Gitflow

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

### stratégie inédite

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

### barrière de protection

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

## H

### HA

Découvrez [la haute disponibilité](#).

### migration de base de données hétérogène

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

### haute disponibilité (HA)

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



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

#### modernisation des historiens

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

#### 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 replatforme. 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 transactionnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

#### correctif

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

#### période de soins intensifs

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

I

IaC

Considérez [l'infrastructure comme un code](#).

politique basée sur l'identité

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

application inactive

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

IIoT

Voir [Internet industriel des objets](#).

infrastructure immuable

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

VPC entrant (d'entrée)

Dans une architecture à comptes multiples AWS, VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'[architecture de référence de sécurité AWS](#) recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

migration incrémentielle

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

I

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.

## infrastructure

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

## infrastructure en tant que code (IaC)

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

## internet industriel des objets (IIoT)

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

## VPC d'inspection

Dans une architecture AWS à comptes multiples, VPC centralisé qui gère les inspections du trafic réseau entre des VPC (dans des Régions AWS identiques ou différentes), Internet et les réseaux sur site. L'[architecture de référence de sécurité AWS](#) recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

## Internet des objets (IoT)

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

## interprétabilité

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

## IoT

Voir [Internet des objets](#).

## Bibliothèque d'informations informatiques (ITIL)

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

## gestion des services informatiques (ITSM)

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

## ITIL

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

## ITSM

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

## migration de grande envergure

Migration de 300 serveurs ou plus.

## LBAC

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

principe de moindre privilège

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

lift and shift

Voir [7 Rs](#).

système de poids faible

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

environnements inférieurs

Voir [environnement](#).

## M

machine learning (ML)

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

branche principale

Voir [succursale](#).

services gérés

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

MAP

Voir [Migration Acceleration Program](#).

## mécanisme

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

## compte membre

Tous les Comptes AWS autres que le 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.

## microservice

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

## architecture de microservices

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

## Programme d'accélération des migrations (MAP)

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

## migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague.

Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la [stratégie de migration AWS](#).

#### usine de migration

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

#### métadonnées de migration

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

#### 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 : réhéberger la migration vers Amazon EC2 avec AWS Application Migration Service.

#### 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 Cloud AWS. 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 mis gratuitement à la disposition de tous les consultants AWS et consultants partenaires APN.

## Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation au cloud d'une entreprise, à identifier les forces et les faiblesses, ainsi qu'à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide d'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

Approche utilisée pour migrer une charge de travail vers le Cloud AWS. 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](#).

### MPA

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

### 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, veuillez consulter [Strategy for modernizing applications in the 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, veuillez consulter [Evaluating modernization readiness for applications in the 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](#).

#### classification multi-classes

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

#### infrastructure mutable

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

## O

### OAC

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

### OAI

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

### OCM

Voir [gestion du changement organisationnel](#).

#### migration hors ligne

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

### OI

Voir [Intégration des opérations](#).

### OLA

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

## migration en ligne

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

## 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.

## 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

Journal de suivi créé par AWS CloudTrail qui journalise tous les événements pour tous les Comptes AWS dans 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 migration AWS, ce cadre s'appelle accélération des personnes, 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). OAC prend en charge tous les compartiments S3 dans toutes les Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS), ainsi que les demandes PUT et DELETE dynamiques adressées au compartiment S3.

## identité d'accès d'origine (OAI)

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

## OU

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

## VPC sortant (de sortie)

Dans une architecture AWS à comptes multiples, VPC qui gère les connexions réseau initiées depuis une application. L'[architecture de référence de sécurité AWS](#) recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

## P

### limite des autorisations

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

### informations personnelles identifiables (PII)

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

## PII

Voir les [informations personnelles identifiables](#).

### manuel stratégique

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

### politique

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

### persistance polyglotte

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

### évaluation du portefeuille

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

### predicate

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

### prédicat pushdown

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

## contrôle préventif

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

## principal

Une entité d'AWS qui peut exécuter des actions et accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS, un rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans [Termes et concepts relatifs aux rôles](#), dans la documentation IAM.

## Confidentialité dès la conception

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

## zones hébergées privées

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

## contrôle proactif

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

## environnement de production

Voir [environnement](#).

## 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.

## Q

### plan de requête

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

### régression du plan de requêtes

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

## R

### Matrice RACI

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

### rançongiciel

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

### Matrice RASCI

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

### RCAC

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

### réplica en lecture

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

### réarchitecte

Voir [7 Rs](#).

## objectif de point de récupération (RPO)

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

## objectif de temps de récupération (RTO)

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

## refactoriser

Voir [7 Rs.](#)

## Région

Ensemble de ressources AWS dans une zone géographique. Chaque Région AWS est isolée et indépendante des autres pour assurer la tolérance aux pannes, la stabilité et la résilience. Pour plus d'informations, veuillez consulter [Managing Régions AWS](#) dans Références générales AWS.

## 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.](#)

## politique basée sur les ressources

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

## matrice responsable, redevable, consulté et informé (RACI)

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

## contrôle réactif

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

## retain

Voir [7 Rs](#).

## se retirer

Voir [7 Rs](#).

## rotation

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

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

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

## RPO

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

## RTO

Voir l'[objectif relatif au temps de rétablissement](#).



## runbook

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

## S

### SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité active l'authentification unique (SSO) fédérée, permettant aux utilisateurs de se connecter à AWS Management Console ou d'appeler les opérations d'API AWS sans qu'il soit nécessaire de créer un utilisateur dans IAM pour chaque membre de l'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.

### 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, consultez la section [Secret](#) dans la documentation de Secrets Manager.

### contrôle de sécurité

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

### renforcement de la sécurité

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

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

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

## automatisation des réponses de sécurité

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

## chiffrement côté serveur

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

## Politique de contrôle des services (SCP)

Politique qui propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. Les SCP définissent des barrières de protection ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer les services ou les actions autorisés ou interdits. Pour plus d'informations, veuillez consulter la rubrique [Politiques de contrôle de service](#) dans la documentation AWS Organizations.

## 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

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

## SIEM

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

## point de défaillance unique (SPOF)

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

## SLA

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

## SLI

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

## SLO

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

## split-and-seed modèle

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

## SPOF

Voir [point de défaillance unique](#).

## schéma en étoile

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

## modèle de figuier étrangleur

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

## sous-réseau

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

## chiffrement symétrique

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

## tests synthétiques

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

# T

## balises

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

## variable cible

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

## liste de tâches

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

## environnement de test

Voir [environnement](#).

## entraînement

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

## passerelle de transit

Hub de transit de réseau que vous pouvez utiliser pour relier vos VPC et vos réseaux sur site. Pour plus d'informations, veuillez consulter la rubrique [Qu'est-ce qu'une passerelle de transit ?](#) dans la documentation AWS Transit Gateway.

## 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

Octroi d'autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation dans 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, veuillez consulter la rubrique [Utilisation d'AWS Organizations avec d'autres services AWS](#) dans la documentation AWS Organizations.

## réglage

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

## équipe de deux pizzas

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

# U

## incertitude

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

## tâches indifférenciées

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

## environnements supérieurs

Voir [environnement](#).

## V

### mise à vide

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

### contrôle de version

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

### Appairage de VPC

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

### vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

## W

### cache actif

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

### données chaudes

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

### fonction de fenêtre

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

## charge de travail

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

## flux de travail

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

## VER

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

## WQF

Consultez le [cadre de qualification des charges de travail AWS](#).

## écrire une fois, lire plusieurs (WORM)

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

## Z

### exploit Zero-Day

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

### vulnérabilité « jour zéro »

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



## application zombie

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

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