



Correctifs automatisés pour les instances mutables dans le cloud hybride à l'aide de AWS Systems Manager

# AWS Directives prescriptives



# AWS Directives prescriptives: Correctifs automatisés pour les instances mutables dans le cloud hybride à l'aide de AWS Systems Manager

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
Présentation .....	3
Termes et concepts .....	4
Témoignages d'utilisateurs clés .....	5
Processus de correctifs .....	8
Conception pour instances EC2 mutables .....	11
Processus automatisé .....	11
Conception pour plusieurs AWS comptes et régions .....	14
Processus automatisé .....	14
Considérations sur l'architecture et restrictions .....	15
Quotas de fenêtre de maintenance par compte .....	15
Autres considérations .....	16
Conception pour les instances locales dans un environnement de cloud hybride .....	18
Processus automatisé .....	18
Considérations et restrictions sur l'architecture .....	20
Principales parties prenantes, rôles et responsabilités .....	22
Personas d'utilisateurs .....	22
Matrice RACI .....	23
Étapes suivantes .....	27
Ressources supplémentaires .....	28
Historique du document .....	29
Glossaire .....	30
# .....	30
A .....	31
B .....	34
C .....	36
D .....	39
E .....	44
F .....	46
G .....	47
H .....	48
I .....	50
L .....	52
M .....	53

---

O .....	58
P .....	60
Q .....	63
R .....	63
S .....	66
T .....	70
U .....	72
V .....	72
W .....	73
Z .....	74
.....	lxxv

# Application automatique de correctifs pour les instances mutables dans le cloud hybride à l'aide de AWS Systems Manager

Chandra Allaka, Amazon Web Services (AWS)

juin 2020([historique du document](#))

Ce guide prescriptif décrit une solution de mise à jour automatisée qui utilise Amazon Web Services (AWS) Systems Manager. Vous pouvez utiliser cette solution pour appliquer des correctifs à vos instances Amazon Elastic Compute Cloud (Amazon EC2) mutables (longue exécution) s'étendant sur plusieurs instances Amazon Elastic Compute Cloud AWScomptes etAWSLes régions et vos instances sur site.

Ce guide s'adresse aux utilisateurs impliqués dans la conception et le développement de capacités opérationnelles dans un environnement cloud hybride afin de permettre aux équipes chargées des applications de se conformer aux politiques de correctifs de leur entreprise. Il vous fournit un mécanisme en libre-service pour déployer des correctifs pré-approuvés sur vos serveurs d'applications.

Ce guide suppose une bonne compréhension des points suivantsAWSconcepts et services et concepts :

- [Systems Manager](#)— Fournit une interface utilisateur unifiée pour visualiser les données opérationnelles de plusieursAWSservices et automatisation des tâches opérationnelles sur votreAWSRessources.
- [Systems Manager Inventory](#)— Fournit une meilleure visibilité sur votre environnement informatique Amazon EC2 EC2 et sur site sur site. Vous pouvez utiliser l'inventaire pour collecter les métadonnées à partir de vos instances gérées.
- [Systems Manager Patch Manager](#)— Automatise le processus d'application de correctifs aux instances gérées avec des mises à jour liées à la sécurité et d'autres types de mises à jour
- [Fenêtres de maintenance de Systems Manager](#)— Vous permet de définir un planning d'exécution d'actions potentiellement perturbatrices sur vos instances, telles que l'application de correctifs à un système d'exploitation, la mise à jour de pilotes ou l'installation de logiciels ou de correctifs.
- [AWS Lambda](#) – Vous permet d'exécuter du code sans avoir à allouer ou gérer des serveurs.

- [Amazon QuickSight](#)— Vous permet de créer et de publier facilement des tableaux de bord interactifs, notamment des informations sur l'apprentissage automatique (ML). Vous pouvez accéder aux tableaux de bord depuis n'importe quel appareil et les intégrer à vos applications, portails et sites Web.
- [Balisage](#)— Vous permet d'attribuer des métadonnées à votre AWS Ressources sous la forme d'identifications. Chaque balise est une étiquette composée d'une clé définie par l'utilisateur et d'une valeur. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources.

# Présentation de la gestion des correctifs

Si vous êtes impliqué dans des opérations d'applications ou d'infrastructures, vous comprenez l'importance d'une solution de correction du système d'exploitation (OS) suffisamment flexible et évolutive pour répondre aux différentes exigences de vos équipes d'applications. Dans une organisation classique, certaines équipes d'applications utilisent une architecture qui implique des instances immuables tandis que d'autres déploient leurs applications sur des instances mutables.

L'application de correctifs aux instances immuables implique d'appliquer les correctifs aux Amazon Machine Images (AMI) qui sont utilisées pour provisionner les instances d'applications EC2 immuables. L'application de correctifs aux instances mutables implique le déploiement de correctifs sur place sur les instances en cours d'exécution pendant une fenêtre de maintenance planifiée.

Ce guide prescriptif explique comment utiliser le gestionnaire de correctifs de AWS Systems Manager pour appliquer des correctifs à des instances mutables qui couvrent plusieurs comptes et régions de manière automatisée, en fonction des fenêtres de maintenance et des groupes de correctifs définis par les équipes chargées des applications sur leurs serveurs à l'aide de balises.

Le guide décrit une solution d'application automatique des correctifs qui permet d'automatiser la configuration et la planification des correctifs à l'aide du gestionnaire de correctifs et de fenêtres de maintenance. Amazon QuickSight fournit les fonctionnalités de reporting et de tableau de bord nécessaires pour établir des rapports sur la conformité des correctifs.

En outre, ce guide décrit une architecture de référence pour les environnements cloud hybrides. Les utilisateurs qui exécutent leurs applications dans une configuration de cloud hybride recherchent des opportunités de consolidation, de simplification, de standardisation et d'optimisation de leurs opérations de gestion des correctifs au sein de leur infrastructure sur site. Le guide explique comment la solution de correction automatique pour les instances mutables peut être étendue pour prendre en charge les scénarios de cloud hybride.

Ce guide décrit :

- Témoignages d'utilisateurs clés pour la gestion des correctifs
- Le processus de mise à jour
- Gestion des correctifs pour les instances mutables dans un seul compte et une seule région ; considérations et limites relatives à l'architecture

- Gestion des correctifs pour les instances mutables dans un environnement multi-comptes et multirégions ; considérations et limites relatives à l'architecture
- Gestion des correctifs pour les instances locales dans un environnement cloud hybride ; considérations et limites relatives à l'architecture
- Principales parties prenantes, rôles et responsabilités

### Note

Ce guide décrit l'architecture d'une solution automatisée (appelée solution de correction automatisée) que vous pouvez implémenter pour répondre à vos exigences en matière de gestion des correctifs pour les instances mutables. Il ne fournit pas le code pour créer la solution.

## Termes et concepts

Durée	Définition
Instances immuables	Les instances immuables sont des instances de serveur EC2 qui ne subissent aucune modification pendant leur exécution. Si des modifications sont nécessaires, vous créez une nouvelle instance avec l'image de serveur mise à jour, vous redéployez l'instance et vous détruisez l'image de serveur existante.
Base de référence du patch	Une ligne de base de correctifs est spécifique à un type de système d'exploitation et définit la liste des correctifs approuvés pour l'installation sur les instances. Pour plus d'informations, consultez la section <a href="#">À propos des bases de correctifs prédéfinies et personnalisées</a> dans la documentation de Systems Manager.
Groupe de patches	Un groupe de correctifs représente les serveurs d'un environnement d'applications qui sont



Durée	Définition
	<p>les cibles d'une ligne de base de correctifs spécifique. Les groupes de correctifs vous permettent de vous assurer que les lignes de correctifs sont mises en œuvre pour l'un d'instances adéquat. Ils permettent également d'éviter de déployer des correctifs avant qu'ils n'aient été correctement testés. Les groupes de correctifs sont représentés par la balise Patch Group. Pour plus d'informations, consultez la section <a href="#">À propos des groupes de correctifs</a> dans la documentation de Systems Manager.</p>
Fenêtre de maintenance	<p>Les fenêtres de maintenance vous permettent de définir une planification quant au moment où vous devez exécuter des actions potentiellement perturbatrices sur des instances, telles que l'application de correctifs à un système d'exploitation, la mise à jour de pilotes ou l'installation de logiciels ou de correctifs. Chaque fenêtre de maintenance dispose d'une planification, d'une durée maximale, d'une durée maximale, d'un un un un. Les fenêtres de maintenance sont représentées par la balise Maintenance Window. Pour plus d'informations, consultez la section <a href="#">À propos des calendriers de mise à jour à l'aide de fenêtres de maintenance</a> dans la documentation de Systems Manager.</p>

## Témoignages d'utilisateurs clés

Le processus classique de mise à jour du système d'exploitation comporte trois tâches :

1. Analyser des instances EC2 et des serveurs locaux pour rechercher les correctifs de système d'exploitation applicables.
2. Regrouper et corriger les instances au moment opportun.
3. Signaler la conformité des correctifs dans l'ensemble de l'environnement du serveur.

Le Le

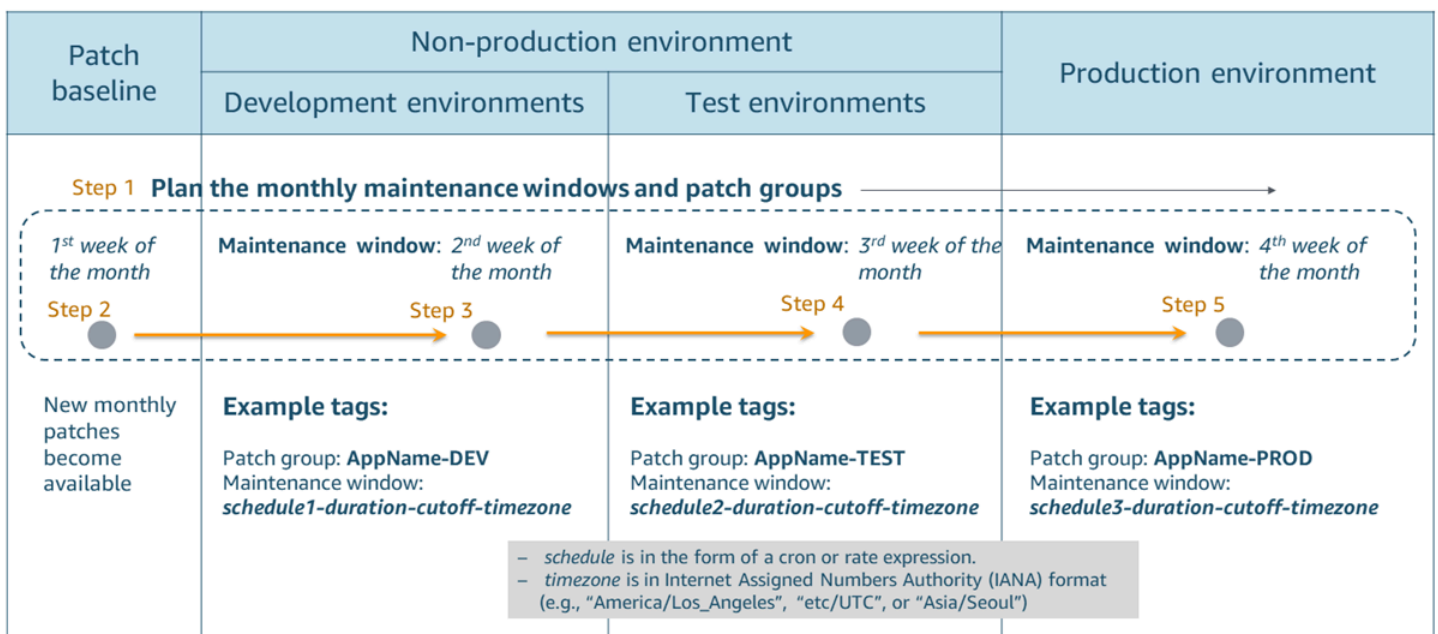
Scénario	Le rôle d'utilisateur	Description
Mécanisme de correction	Équipes de développement et de support d'applications	En tant que membre de l'équipe des applications responsable de l'application des correctifs du système d'exploitation, j'ai besoin d'un mécanisme pour corriger mes instances mutables ou de longue durée, afin de réduire les vulnérabilités de sécurité du système d'exploitation et de m'assurer que les instances sont conformes à la base de référence en matière de correctifs définie par l'équipe de sécurité.
Solution d'application de correctifs	Propriétaire du service cloud	En tant que propriétaire d'un service cloud chargé de fournir des services cloud aux équipes chargées des applications, je dois créer une solution de correctifs du système d'exploitation prenant en charge plusieurs AWS comptes et AWS régions ainsi que des serveurs sur site, afin que les équipes chargées

Scénario	Le rôle d'utilisateur	Description
		des applications puissent atténuer les vulnérabilités de sécurité du système d'exploitation et rester en conformité avec la base de référence en matière de correctifs définie par l'équipe de sécurité.
Rapports de conformité relatifs aux correctifs	Responsable des opérations de sécurité	En tant que responsable des opérations de sécurité chargé de garantir la conformité des correctifs, j'ai besoin de rapports détaillés sur la conformité des correctifs et d'informations sur l'ensemble du paysage cloud, afin de pouvoir identifier les serveurs non conformes à la base de référence des correctifs et d'alerter les équipes pour mettre en œuvre les mesures d'atténuation requises.
Définition des rôles et des responsabilités	Propriétaire du service cloud	En tant que propriétaire d'un service cloud, je dois créer une matrice de rôles et de responsabilités bien définie qui explique qui fait quoi dans la gestion de la solution de correctifs pour le cloud hybride que j'ai créée, afin que les obligations relatives aux opérations de mise à jour soient publiées et respectées.

## Processus de correctifs

Les principaux utilisateurs de la solution de correctifs sont les équipes de développement d'applications et d'exploitation. Chaque application est généralement déployée dans plusieurs environnements, tels que le développement, le test (intégration, acceptation des utilisateurs, etc.) et la production. Les équipes d'application doivent planifier les programmes de correctifs pour chaque environnement. Par conséquent, lorsqu'un correctif est appliqué à l'environnement de production, il a déjà été testé et déterminé qu'il n'a aucun effet négatif sur l'application.

Le flux de travail suivant illustre comment planifier les fenêtres de correctifs pour une application déployée dans plusieurs environnements et comment configurer les balises.



- Étape 1. Chaque équipe d'application planifie ses fenêtres de maintenance pour ses serveurs dans différents environnements et configure les balises qui représentent les groupes de correctifs et les fenêtres de maintenance des serveurs en conséquence :
  - Le Groupe de correctifs représente les serveurs d'un environnement d'application qui sont les cibles d'une ligne de base de correctifs spécifique. Les groupes de correctifs vous permettent de vous assurer que les lignes de référence de correctifs appropriées sont déployées sur l'ensemble d'instances adéquat. Les groupes de correctifs vous permettent également d'éviter le déploiement de correctifs dans l'environnement de production avant qu'ils aient été testés correctement.

- Si les serveurs d'applications comprennent plusieurs systèmes d'exploitation, l'équipe d'application crée des groupes de correctifs basés sur la combinaison de l'environnement et du système d'exploitation. Un groupe de correctifs peut être enregistré avec une seule ligne de base de correctifs, et une instance ne peut faire partie d'un seul groupe de correctifs.

Par exemple: *appname*-DEV-WINet*appname*-DEV-RHEL

- LeMaintenance Windowreprésente le calendrier de correction des serveurs. Tous les serveurs d'un groupe de correctifs doivent se trouver dans la même fenêtre de maintenance. La balise de fenêtre de maintenance doit suivre un format cohérent pour les expressions cron et rate afin qu'une fonction Lambda que vous définissez puisse analyser facilement les expressions. (Dans ce guide, nous allons faire référence à cette fonction Lambda sous le nomautomate-patch.)

Par exemple : *schedule-duration-cutoff-timezone*

`cron(0 2 ? * SAT#3 *)`représente 2 h 00 le troisième samedi de chaque mois. Pour plus d'informations sur les expressions de type cron et rate, consultez le[Documentation Systems Manager](#).

- Étape 2. Systems Manager Patch Manager rend les nouveaux correctifs disponibles régulièrement via des lignes de base de correctifs spécifiques au système d'exploitation basées sur les configurations définies.
  - Pour chaque système d'exploitation, vous pouvez définir une ligne de base de correctifs personnalisée qui inclut les règles d'approbation et les correctifs devant être appliqués aux instances dans l'environnement cloud.
- Étape 3. Votre code d'automatisation personnalisé configure Patch Manager pour configurer les correctifs en fonction de laGroupe de correctifsetMaintenance Windowet applique les correctifs à l'environnement de développement.
  - Une fois le correctif terminé, les équipes de développement d'applications et de support testent l'application et vérifient que tout fonctionne correctement.
  - Si l'application rencontre des problèmes avec le nouveau correctif, les équipes d'application demandent à l'équipe des services cloud d'arrêter le traitement des correctifs vers d'autres groupes de correctifs et autres environnements, soit en désactivant les fenêtres de maintenance, soit en désenregistrant l'exécution de la tâche de correctif.
- Étape 4. Une fois que l'environnement de développement a été correctement corrigé, les correctifs sont déployés dans tous les autres environnements autres que la production. Comme pour l'environnement de développement, l'application est testée et vérifiée qu'elle fonctionne

correctement dans tous les environnements hors production. En cas de problème, les équipes d'applications demandent à l'équipe des services cloud d'arrêter le traitement des correctifs vers l'environnement de production.

- Étape 5. Une fois que tous les environnements hors production ont été corrigés avec succès, le correctif est appliqué à l'environnement de production.

# Conception de solutions de correctifs pour les instances EC2 mutables

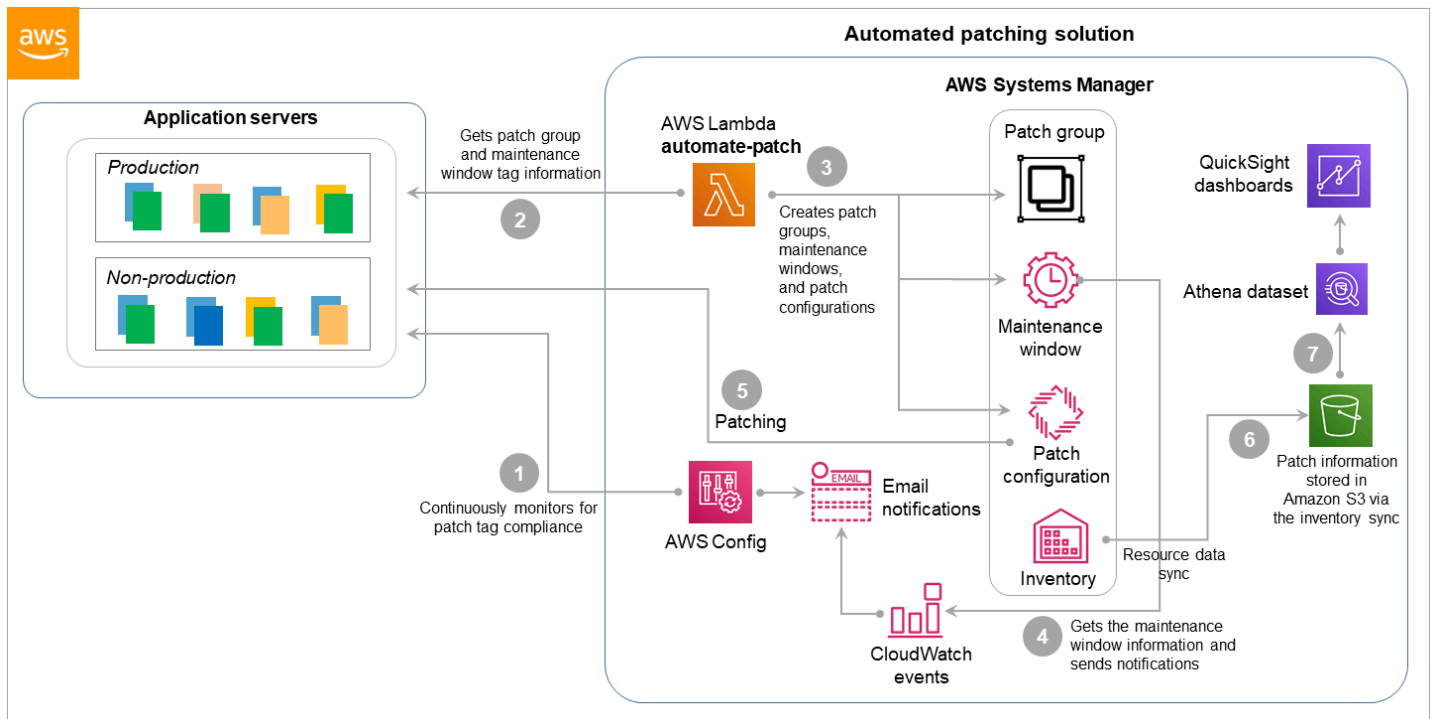
Le processus de correctif pour les instances mutables implique les équipes et actions suivantes :

- Les équipes d'application (DevOps) définissent les groupes de correctifs pour leurs serveurs en fonction de l'environnement d'application, du type de système d'exploitation ou d'autres critères. Ils définissent également les fenêtres de maintenance spécifiques à chaque groupe de correctifs. Ces informations sont stockées sur le Groupe de correctif et Maintenance Window balises des instances d'application EC2. Au cours de chaque cycle de correctifs, les équipes d'application se préparent au correctif, testent l'application après le correctif et résolvent tout problème lié à leurs applications et à leur système d'exploitation pendant le correctif.
- L'équipe d'opérations de sécurité définit les lignes de base de correctifs pour les différents types de systèmes d'exploitation utilisés par les équipes d'application, approuve les correctifs et rend les correctifs disponibles via Systems Manager Patch Manager.
- La solution de correctifs automatisés s'exécute régulièrement et déploie les correctifs définis dans les lignes de base de correctifs en fonction des groupes de correctifs définis par l'utilisateur et des fenêtres de maintenance. Les informations de conformité des correctifs sont obtenues via une synchronisation des données de ressources dans Systems Manager Inventory et sont utilisées pour les rapports de conformité des correctifs via les tableaux de bord Amazon QuickSight.
- Les équipes de gouvernance et de conformité définissent les directives de correctifs, définissent les processus et mécanismes d'exception et obtiennent les rapports de conformité auprès d'Amazon QuickSight.

Pour obtenir des informations détaillées sur les principales parties prenantes impliquées dans une solution de gestion des correctifs du système d'exploitation réussie et leurs responsabilités, consultez le [Principales parties prenantes, rôles et responsabilités](#) dans la suite de ce guide.

## Processus automatisé

La solution de correctifs automatisés utilise plusieurs AWS services fonctionnant en tandem pour déployer les correctifs sur les instances EC2. Ce processus implique AWS Config, AWS Lambda, Systems Manager, Amazon Simple Storage Service (Amazon S3) et Amazon QuickSight. Le schéma suivant illustre l'architecture de référence et le flux de travail.



Le flux de travail inclut ces étapes, où les numéros de pas correspondent aux légendes du diagramme :

1. AWS Config surveille en permanence les éléments suivants et envoie des notifications avec les détails des instances non conformes et des configurations nécessaires :
  - Conformité au balisage des correctifs sur les instances EC2. AWS Config vérifie les instances qui n'ont pas de groupe de correctif et de Maintenance Window étiquettes.
  - Le AWS Identity and Access Management (IAM) avec le rôle Systems Manager, qui permet à Systems Manager de gérer les instances.
2. La fonction Lambda (on l'appellera `automate-patch`) s'exécute selon un calendrier prédéfini et recueille le Groupe de correctif et Maintenance Window informations pour tous les serveurs.
3. Le `automate-patch` crée ou met à jour les groupes de correctifs et les fenêtres de maintenance appropriés, associe les groupes de correctifs aux lignes de base de correctifs, configure l'analyse des correctifs et déploie la tâche de correction. Le cas échéant, le `automate-patch` crée également des événements dans Amazon CloudWatch Events pour informer les utilisateurs des correctifs imminents.
4. Sur la base des fenêtres de maintenance, les événements envoient des notifications de correctifs aux équipes d'application avec les détails de l'opération de correctif imminente.



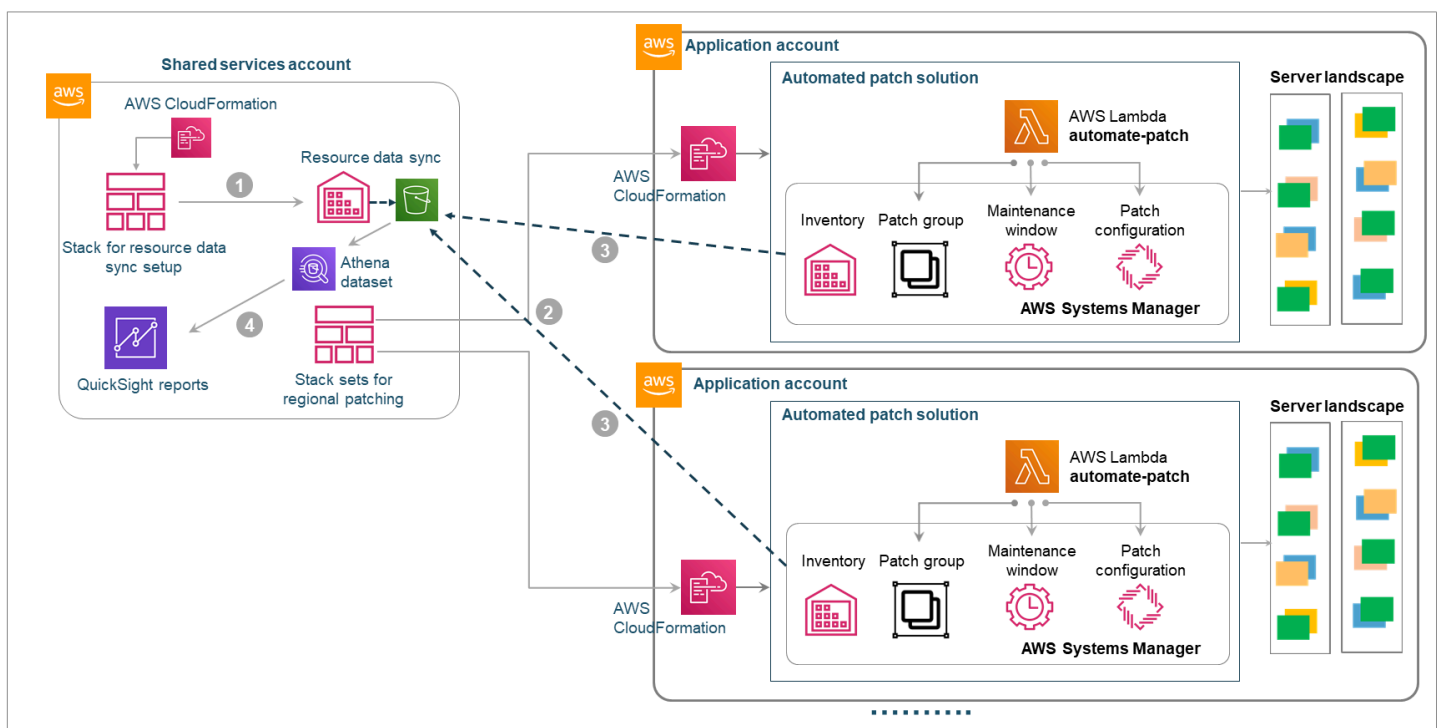
5. Patch Manager effectue des correctifs système en fonction de la planification définie et des groupes de correctifs.
6. Une synchronisation des données de ressources dans Systems Manager Inventory rassemble les détails des correctifs et les publie dans un compartiment S3.
7. Les rapports de conformité des correctifs et les tableaux de bord sont intégrés à Amazon QuickSight à partir des informations du compartiment S3.

# Conception de solutions de correctifs pour plusieurs AWS comptes et régions

Vous pouvez étendre la solution de correctifs automatisés pour prendre en charge des serveurs couvrant plusieurs serveurs AWS comptes et plusieurs AWS Régions. La solution étendue implique la configuration de la solution d'automatisation des correctifs dans chaque AWS compte via AWS CloudFormation StackSets dans un compte de services partagés et configuration d'une synchronisation des données de ressources entre les comptes avec le compte Shared Services.

## Processus automatisé

Le diagramme suivant illustre l'architecture pour ce scénario. Cette architecture comprend AWS CloudFormation StackSets et un AWS compte de service partagé.



Le flux de travail est similaire au processus décrit dans la section précédente, mais implique les étapes supplémentaires suivantes, où les numéros d'étape correspondent aux légendes du diagramme :

1. Dans le compte Shared Services, unAWS CloudFormationLe jeu de piles permet de configurer le compartiment S3 pour la synchronisation de données de ressource via Systems Manager Inventory.
2. Le jeu de piles CloudFormation crée la pile avec le automate-patch Fonction Lambda, configure les lignes de base des correctifs et configure la synchronisation des données de ressources d'inventaire Systems Manager sur les comptes d'application, pour synchroniser les ressources du compte de services partagés.
3. Les informations sur les ressources des comptes d'application sont synchronisées avec celles du compte de services partagés.
4. Amazon QuickSight génère des rapports de conformité des correctifs, en utilisant le jeu de données Amazon Athena pour les informations sur les ressources synchronisées.

## Considérations sur l'architecture et restrictions

### Quotas de fenêtre de maintenance par compte

L'architecture illustrée et décrite dans la section précédente crée une fenêtre de maintenance pour chaque groupe de correctifs. Toutefois, le quota pour le nombre de fenêtres de maintenance parAWScompte 50 (en supposant que vous n'avez pas demandé d'augmentation du quota de service). Si vous prévoyez que le nombre de groupes de correctifs dépasse 50 groupes en un seulAWS, cette architecture ne sera pas évolutive pour répondre à vos besoins.

Si une augmentation du quota de service n'est pas suffisante pour répondre à vos besoins, il existe deux options pour gérer ce défi : l'utilisation de fenêtres de maintenance prédéfinies et l'utilisation de CloudWatch Events. Voici les avantages et les inconvénients de chaque approche.

#### Option 1. Utiliser des fenêtres de maintenance prédéfinies

- Définissez une liste de fenêtres de maintenance avec différentes fenêtres horaires (par exemple, 15 à 20 fenêtres de maintenance par compte).
- Les équipes d'application choisissent les fenêtres de maintenance qui leur conviennent dans la liste prédéfinie et marquent les instances en conséquence.
- Mettez à jour la solution de correctifs automatisés pour mapper les groupes de correctifs aux fenêtres de maintenance sélectionnées au lieu de créer de nouvelles fenêtres de maintenance.

Avantages :

- Gestion simplifiée.

Les inconvénients :

- Moins de flexibilité pour définir des fenêtres de maintenance personnalisées.
- Lorsque plusieurs groupes de correctifs partagent des fenêtres de maintenance et des tâches de correctif, l'annulation d'une tâche de correctif spécifique pour un groupe de correctifs spécifique nécessite un effort manuel supplémentaire.

Option 2. Utiliser CloudWatch Events pour déclencher des tâches de correctif au lieu d'utiliser des fenêtres de maintenance

- Au lieu de créer des fenêtres de maintenance, utilisez CloudWatch Events pour déclencher des tâches de correctif basées sur la planification et les groupes de correctifs.
- Dans ce scénario, chaque groupe de correctifs est associé à un événement CloudWatch Events au lieu d'une fenêtre de maintenance.
- Mettez à jour la solution de correctifs automatisés pour créer des événements plutôt que des fenêtres de maintenance.

Avantages :

- Design évolutif.
- Offre une flexibilité pour définir des fenêtres de maintenance personnalisées.

Les inconvénients :

- Les fenêtres de maintenance fournissent des fonctionnalités supplémentaires (telles que la durée et les heures limites) qui ne sont pas disponibles avec CloudWatch Events.

## Autres considérations

- La solution de correctifs automatisés décrite dans cette section ne prend pas en charge les instances EC2 arrêtées.

- Ce processus prend en charge les instances EC2 dans des sous-réseaux publics. Pour corriger des instances dans des sous-réseaux privés, vous devez déployer un [référentiel local de correctifs tel que Windows Server Update Services \(WSUS\)](#).
- Vous devez ajuster la fréquence d'exécution de la fonction Lambda pour que les groupes de correctifs et les fenêtres de maintenance soient mis à jour en fonction de la planification requise.

# Conception de solutions de correctifs pour les instances locales dans un environnement cloud hybride

Vous pouvez également étendre la solution décrite dans ce guide pour corriger les instances de serveur locales dans un environnement de cloud hybride.

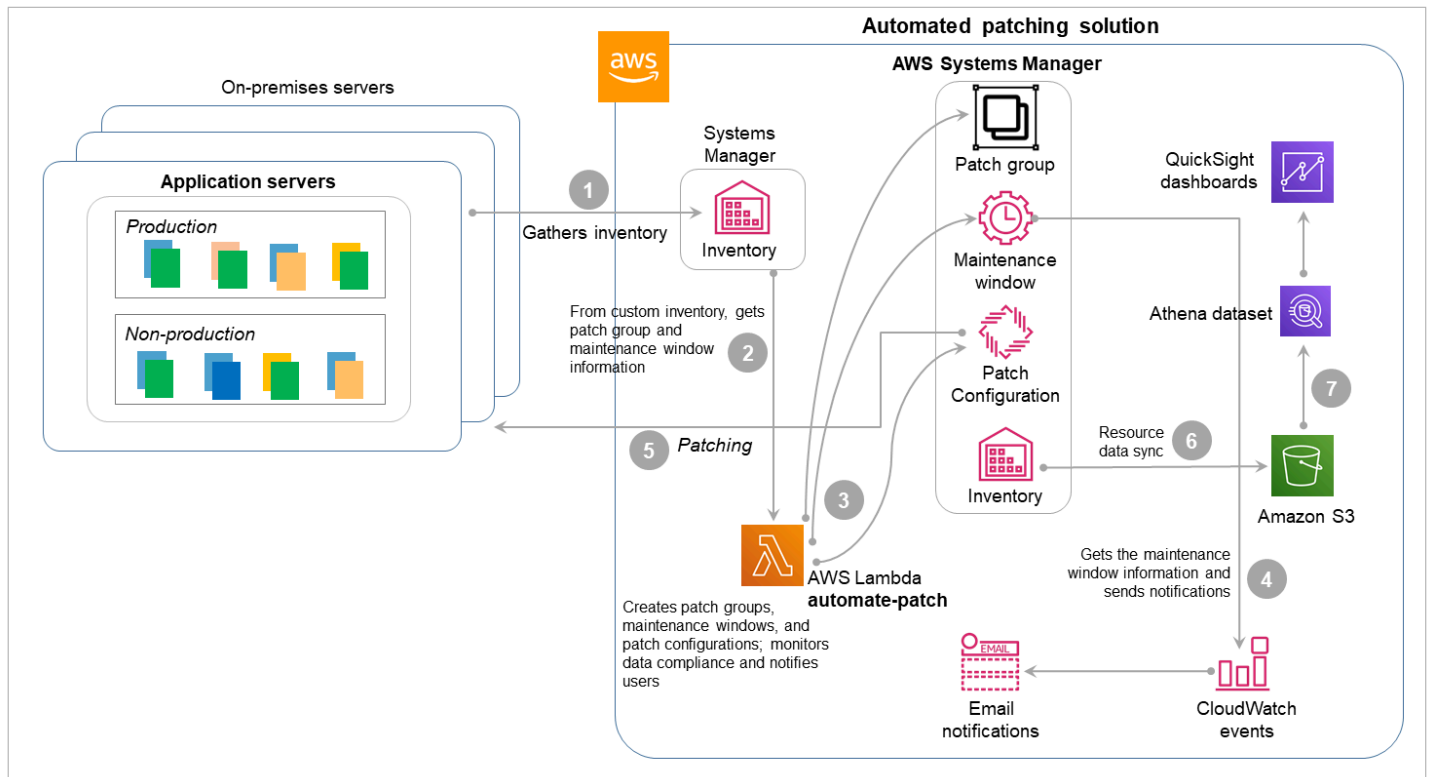
Le processus de correctif standard pour les instances locales comprend deux étapes :

- Vous configurez vos serveurs locaux pour qu'ils soient gérés par Systems Manager. Pour de plus amples informations sur ce processus, veuillez consulter [Configuration de Systems Manager pour les environnements hybrides](#) dans la documentation Systems Manager.
- Vous configurez la configuration appropriée Groupe de correctif et Maintenance Window balises pour ces instances gérées sur site à l'aide du AWS Command Line Interface (AWS CLI) [commande add-tags-to-resource](#).

Toutefois, cette approche nécessite que l'équipe d'application ou l'équipe cloud exécute manuellement le AWS CLI chaque fois qu'ils veulent modifier les groupes de correctifs ou les fenêtres de maintenance.

## Processus automatisé

L'illustration suivante décrit une autre approche pour appliquer des correctifs aux instances locales utilisant l'option d'inventaire personnalisé Systems Manager. Ce processus est une extension de la solution de correctifs automatisés que nous avons décrite précédemment pour les instances EC2 mutables.



1. Au lieu d'utiliser des balises, Systems Manager capture les informations sur les correctifs (groupes de correctifs et fenêtres de maintenance) à partir des instances gérées sur site via une collection d'inventaire personnalisée.

Sample custom inventory JSON file

```
{
  "SchemaVersion": "1.0",
  "TypeName": "Custom:PatchInformation",
  "Content": {
    "Patch Group": "<APP-PROD>",
    "Maintenance Window": "XXX"
  }
}
```

2. Le Lambda automate-patch s'exécute tous les jours, recueille les informations du groupe de correctifs et de la fenêtre de maintenance à partir de l'inventaire personnalisé du serveur local, et crée le Groupe de correctif et Maintenance Window balises sur les instances gérées.
3. Le Lambda automate-patch crée ou met à jour les groupes de correctifs et les fenêtres de maintenance appropriés, associe les groupes de correctifs aux lignes de base de correctifs, configure les analyses de correctifs et déploie la tâche de correctif, en fonction de l'inventaire

- personnalisé qui a été collecté. En option, le `automate-patch` crée également des événements dans CloudWatch Events pour informer les utilisateurs des correctifs imminents.
4. Sur la base des fenêtres de maintenance, les événements envoient des notifications de correctifs aux équipes d'application avec les détails de l'opération de correctif imminente.
  5. Patch Manager effectue des correctifs système en fonction de la planification définie et des groupes de correctifs.
  6. Une synchronisation des données de ressources dans Systems Manager Inventory rassemble les détails des correctifs et les publie dans un compartiment S3.
  7. Les rapports de conformité des correctifs et les tableaux de bord sont intégrés à Amazon QuickSight à partir des informations du compartiment S3.

## Considérations et restrictions sur l'architecture

Comme indiqué dans les sections précédentes, il existe deux approches pour appliquer des correctifs aux instances locales : via un inventaire personnalisé ou en utilisant des balises. Voici les avantages et désavantages de chaque approche.

### Option 1. Utiliser un inventaire personnalisé pour des informations sur les correctifs

- Les équipes d'applications travaillant avec des serveurs locaux configurent les informations de correctif dans le fichier d'inventaire personnalisé, et Systems Manager sélectionne ces informations.
- Les informations de correctif d'inventaire personnalisées sont ensuite utilisées pour créer les tâches de correctif.

#### Avantages :

- Il est beaucoup plus simple à configurer car il ne s'agit que d'une mise à jour de fichier.

#### Les inconvénients :

- Les modifications apportées à la configuration des correctifs sont limitées au calendrier de collecte des stocks.

### Option 2. Utiliser des balises pour les instances gérées sur site



- Les équipes d'application travaillant avec des serveurs sur site créent un groupe de correctifs et utilisent les balises AWS CLI avec les informations appropriées sur les correctifs.
- Les informations de balise sont utilisées pour créer les tâches de correctif.

#### Avantages :

- Approche cohérente sur site pour piloter la normalisation et l'automatisation des correctifs.

#### Les inconvénients :

- Les équipes d'applications travaillant avec des instances locales doivent apprendre et utiliser AWS CLI pour créer ou mettre à jour les balises.

# Principales parties prenantes, rôles et responsabilités dans la gestion des correctifs

La gestion réussie des correctifs du système d'exploitation nécessite de disposer de rôles et de responsabilités bien définis pour prendre en charge votre solution de correctifs automatisés et l'optimiser continuellement. Cette section décrit les rôles et responsabilités suggérés que vous pouvez modifier en fonction de vos besoins et de votre structure organisationnelle.

## Personas d'utilisateurs

Le tableau suivant décrit les personnes utilisateur impliquées dans la solution de correctifs automatisés.

Persona utilisateur	Description
Consommateurs (C)	<p>La solution de gestion des correctifs pour les instances de longue durée est utilisée par différentes équipes impliquées dans la gestion du système d'exploitation, notamment :</p> <ul style="list-style-type: none"> <li>• Les équipes de développement qui gèrent les environnements applicatifs complets.</li> <li>• Les équipes opérationnelles qui gèrent le système d'exploitation du serveur d'applications.</li> </ul>
Ingénierie Cloud (CE)	<p>L'équipe responsable de :</p> <ul style="list-style-type: none"> <li>• Optimisation continue de la solution de gestion des correctifs.</li> <li>• Création d'automatisation des services cloud.</li> <li>• Soutien à l'automatisation.</li> </ul>
Bureau d'affaires Cloud (CBO)	L'équipe impliquée dans :

Persona utilisateur	Description
	<ul style="list-style-type: none"> <li>• Gestion de l'expérience consommateur pour la solution.</li> <li>• Activation et engagement des utilisateurs.</li> <li>• S'assurer que la solution corrective répond aux besoins des consommateurs.</li> </ul>
Propriétaire du service cloud et du produit (CPO)	<p>La personne qui est responsable de :</p> <ul style="list-style-type: none"> <li>• Fournir des services cloud aux consommateurs.</li> <li>• Travailler en étroite collaboration avec l'équipe de direction pour aligner la prestation des services sur les attentes et les lignes directrices.</li> <li>• Gérer toutes les attentes des clients et les escalades liées à la plateforme.</li> <li>• Posséder la feuille de route de la plateforme.</li> </ul>
Opérations de sécurité (SO)	L'équipe qui gère les lignes de base et les approbations des correctifs.
Gestionnaire des opérations de sécurité (SOM)	Le responsable responsable de la conformité des correctifs.

## Matrice RACI

La matrice RACI (responsable, responsable, consultée, informée) suivante spécifie les activités impliquées dans la solution de gestion des correctifs. Pour chaque étape du processus, il répertorie les parties prenantes et leur implication :

- R— responsable de la réalisation de l'étape
- UN— responsable de l'approbation et de la signature des travaux
- C— consultés pour fournir une contribution à une tâche
- JE— informés des progrès réalisés, mais pas directement impliqués dans la tâche

Solution de gestion des correctifs	CPO	CBO	DE NOTRE ÈRE	DONC	SOM	C
Exécution de la feuille de route des produits de gestion	A	C	R	C	C	I
Architecture et conception de gestion des correctifs	A	I	R	C	I	
Développement et configuration de la gestion des correctifs	A		R	C		
Validation et test de la gestion des	A	I	R	I	I	
NouvelleAWSintégration de comptes, d'applications et de serveurs	A	C	R	I		

Solution de gestion des correctifs	CPO	CBO	DE NOTRE ÈRE	DONC	SOM	C
pour les correctifs						
Engagement et activation des utilisateurs	A	R	I	I	I	
Gestion des commentaires des utilisateurs et de l'escalade	A	R		I	I	
Gestion des modifications de produits	A	R	C	I		
Gestion et résolution des problèmes	A		R	C		
Correctifs serveur et conformité des correctifs			C	C		AR

Solution de gestion des correctifs	CPO	CBO	DE NOTRE ÈRE	DONC	SOM	C
Configuration de référence de correctif			C	R	A	C
Reporting et conformité des correctifs			C	R	AR	I

## Étapes suivantes

Ce guide décrit une solution de correctifs automatisés pour les instances mutables sur AWS et des instances sur site dans un environnement cloud hybride. Pour créer la solution, nous vous recommandons de consulter la documentation relative aux services AWS décrits dans ce guide. Si vous avez des questions, contactez votre équipe AWS de compte pour obtenir de l'aide.

Pour plus d'informations, consultez le [.Ressources supplémentaires](#) Section.

# Ressources supplémentaires

## AWSressources

- [AWSConseils prescriptifs](#)
- [Documentation AWS](#)
- [AWSRéférence générale](#)
- [AWSglossaire](#)

## AWSservices

- [AWS CloudFormation](#)
- [Amazon CloudWatch](#)
- [Amazon EC2](#)
- [GIA](#)
- [AWS Lambda](#)
- [Amazon QuickSight](#)
- [AWS Systems Manager](#)

## Autres ressources

- [Comment corriger les instances Amazon EC2 dans des sous-réseaux privés à l'aide deAWS Systems Manager](#)(AWSBlog Gestion et Gouvernance)
- [Comment Moody's utiliseAWS Systems Managerpour corriger les serveurs entre plusieurs fournisseurs de cloud](#)(AWSBlog Gestion et Gouvernance)
- [Configuration d'AWS Systems Managerpour les environnements hybrides](#)(documentation Systems Manager)
- [Correctifs centralisés multi-comptes et multi-régions avecAWS Systems ManagerAutomation](#)(AWSBlog Gestion et Gouvernance)
- [Correctif à vos instances Amazon EC2 à l'aideAWS Systems ManagerGestionnaire de correctifs](#)(AWSBlog Gestion et Gouvernance)
- [Comment corriger, inspecter et protéger les charges de travail Microsoft Windows surAWS—Partie 1](#)(AWSBlog de sécurité)



## 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="#">Première version</a>	—	12 juin 2020

# AWS Glossaire des directives prescriptives

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

## Nombres

### 7 R

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

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

### ACID

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

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

### AI

Voir [intelligence artificielle](#).

## AIOps

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

### anonymisation

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

### anti-motif

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

### contrôle des applications

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

### portefeuille d'applications

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

### intelligence artificielle (IA)

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

### opérations d'intelligence artificielle (AIOps)

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

## chiffrement asymétrique

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

## atomicité, consistance, isolation, 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 basé sur les attributs () ABAC

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

## source de données faisant autorité

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

## Zone de disponibilité

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

## AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

## B

### mauvais bot

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

### BCP

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

### graphique de comportement

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

### système de poids fort

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

### classification binaire

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

### filtre de Bloom

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

## déploiement bleu/vert

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

## bot

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

## botnet

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

## branche

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

## accès par brise-vitre

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

## stratégie existante (brownfield)

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

## cache de tampon

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

## capacité métier

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

## planification de la continuité des activités (BCP)

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

# C

## CAF

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

## déploiement de Canary

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

## CCoE

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

## CDC

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

## modifier la capture de données (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 l'utiliser à diverses CDC fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.



## ingénierie du chaos

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

## CI/CD

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

## classification

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

## chiffrement côté client

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

## Centre d'excellence du cloud (CCoE)

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

## cloud computing

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

## modèle d'exploitation du cloud

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

## étapes d'adoption du cloud

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

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

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

## CMDB

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

## référentiel de code

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

## cache passif

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

## données gelées

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

## vision par ordinateur (CV)

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

## dérive de configuration

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

## base de données de gestion de configuration (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 issues de la phase CMDB de découverte et d'analyse du portefeuille lors de la migration.

## pack de conformité

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

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

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

## CV

Voir [vision par ordinateur](#).

## D

### données au repos

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

## classification des données

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

## dérive des données

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

## données en transit

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

## maillage de données

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

## minimisation des données

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

## périmètre de données

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

## prétraitement des données

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

## provenance des données

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

## sujet des données

Personne dont les données sont collectées et traitées.

## entrepôt des données

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

## langage de définition de base de données (DDL)

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

## langage de manipulation de base de données (DML)

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

## DDL

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

## ensemble profond

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

## deep learning

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

## defense-in-depth

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

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

## administrateur délégué

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

## déploiement

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

## environnement de développement

Voir [environnement](#).

## contrôle de détection

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

## cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSMétend 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 la façon dont vous pouvez utiliser le design piloté par domaine avec le motif Strangler Fig, voir [Modernisation de l'ancienne version de Microsoft. ASP NET\(ASMX\) des services Web de manière incrémentielle à l'aide de conteneurs et d'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 dans un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou à AWS Identity and Access Management (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre service



de point de terminaison de manière privée en créant des points de VPC terminaison d'interface. Pour plus d'informations, consultez la section [Créer un service de point de terminaison](#) dans la documentation Amazon Virtual Private Cloud (AmazonVPC).

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environnement

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

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un 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 grands enjeux en matière de AWS CAF sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, la

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

## ERP

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

## analyse exploratoire des données () EDA

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. EDAest 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. Ceci est généralement exprimé sous la forme d'un score numérique qui peut être calculé à l'aide de diverses techniques, telles que les explications additives de Shapley (SHAP) et les dégradés 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 organisationnelles (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Ils sont mis en œuvre à l'aide de politiques de contrôle des services et de limites IAM d'autorisations. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

# H

## HA

Découvrez [la haute disponibilité](#).

## migration de base de données hétérogène

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

## haute disponibilité (HA)

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

## modernisation des historiques

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

## migration de base de données homogène

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

## données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données 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 IAM principaux qui définit leurs autorisations au sein de l'AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne CPU 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.

entrant (entrée) VPC

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

migration incrémentielle

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

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.

## Industry 4.0

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

## infrastructure

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

## infrastructure en tant que code (IaC)

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

## Internet industriel des objets (IIoT)

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

## inspection VPC

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

## Internet des objets (IoT)

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

## interprétabilité

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

## IoT

Voir [Internet des objets](#).

## bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. 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 ITSM outils, consultez le [guide d'intégration des opérations](#).

## ITIL

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

## ITSM

Voir [Gestion des services informatiques](#).

## L

### contrôle d'accès basé sur des étiquettes ( ) LBAC

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

### zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement



de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter [Setting up a secure and scalable multi-account AWS environment](#).

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, consultez la section [Appliquer les autorisations du moindre privilège](#) dans la IAM documentation.

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](#).

malware

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

ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

## services gérés

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

## système d'exécution de la fabrication (MES)

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

## MAP

Voir [Migration Acceleration Program](#).

## mécanisme

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

## compte membre

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

## MES

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

## Transport de télémétrie en file d'attente de messages () MQTT

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

## microservice

Un petit service indépendant qui communique via un réseau bien défini APIs et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le

marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section [Intégration de microservices à l'aide de services AWS sans serveur](#).

## architecture de microservices

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

## Migration Acceleration Program (MAP)

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

## migration à grande échelle

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

## usine de migration

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

## métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration.

Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

## modèle de migration

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

## Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le. AWS Cloud MPA fournit une évaluation détaillée du portefeuille (dimensionnement correct des serveurs, tarification, TCO comparaisons, analyse des coûts de migration) ainsi que la planification de la migration (analyse et collecte des données des applications, regroupement des applications, hiérarchisation des migrations et planification des vagues). L'[MPAoutil](#) (nécessite une connexion) est disponible gratuitement pour tous les AWS consultants et consultants APN partenaires.

## Évaluation de l'état de préparation à la migration (MRA)

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

## stratégie de migration

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

## ML

Voir [apprentissage automatique](#).

## modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de

gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez [la section Stratégie de modernisation des applications dans le AWS Cloud](#).

## évaluation de la préparation à la modernisation

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

## applications monolithiques (monolithes)

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

## MPA

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

## MQTT

Voir [Message Queuing Telemetry Transport](#).

## classification multi-classes

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

## infrastructure mutable

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

## O

### OAC

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

### OAI

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

### OCM

Voir [gestion du changement organisationnel](#).

### migration hors ligne

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

### OI

Voir [Intégration des opérations](#).

### OLA

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

### migration en ligne

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

### OPC-États-Unis

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

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

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

## accord au niveau opérationnel ( ) OLA

Un accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de soutenir un accord de niveau de service ( ). SLA

## examen de l'état de préparation opérationnelle (ORR)

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

## technologie opérationnelle (OT)

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

## intégration des opérations (OI)

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

## journal de suivi d'organisation

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

## gestion du changement organisationnel (OCM)

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

## contrôle d'accès à l'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 Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les DELETE requêtes dynamiques PUT adressées au compartiment S3.

## identité d'accès à l'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, 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 granulaire et amélioré.

## ORR

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

## DE

Voir [technologie opérationnelle](#).

## sortant (sortie) VPC

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

## P

### limite des autorisations

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

### informations personnellement 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. PII Les exemples incluent les noms, les adresses et les coordonnées.



## PII

Voir les [informations personnelles identifiables](#).

## manuel stratégique

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

## PLC

Voir [contrôleur logique programmable](#).

## PLM

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

## politique

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

## persistance polyglotte

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

## évaluation du portefeuille

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

## predicate

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

## prédicat pushdown

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

## contrôle préventif

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

## principal

Entité capable d'effectuer AWS des actions et d'accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS, un IAM rôle ou un utilisateur. Pour plus d'informations, consultez les [termes et concepts de Principal in Roles](#) dans la IAM documentation.

## Confidentialité dès la conception

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

## zones hébergées privées

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

## contrôle proactif

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

## gestion du cycle de vie des produits (PLM)

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

## environnement de production

Voir [environnement](#).

## contrôleur logique programmable (PLC)

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

## pseudonymisation

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

## publish/subscribe (pub/sub)

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

## Q

### plan de requête

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

### 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

### RACImatrice

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.

## RASCImatrice

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 replica de lecture pour réduire la charge sur votre base de données principale.

## réarchitecte

Voir [7 Rs](#).

## objectif du point de récupération (RPO)

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

## objectif de temps de récupération (RTO)

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

## refactoriser

Voir [7 Rs](#).

## Région

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

## régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de

régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir [7 Rs.](#)

version

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

déplacer

Voir [7 Rs.](#)

replateforme

Voir [7 Rs.](#)

rachat

Voir [7 Rs.](#)

résilience

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

politique basée sur les ressources

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

matrice responsable, responsable, consultée, informée (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 RASCI-matrice, et si vous l'excluez, elle est appelée RACI-matrice.

## 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)

L'utilisation d'SQL expressions simples et flexibles qui ont défini des règles d'accès. RCAC consiste en des autorisations de ligne et des masques de colonnes.

## RPO

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

## RTO

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

## runbook

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

# S

## SAML2,0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les AWS API opérations sans que vous ayez à créer un

compte utilisateur IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML basée sur la version 2.0, consultez la section [À propos de la fédération SAML basée sur la version 2.0](#) dans la documentation. IAM

## SCADA

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

## SCP

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

## secret

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

## contrôle de sécurité

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

## renforcement de la sécurité

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

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

Outils et services qui combinent des systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un SIEM système 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 et de générer des alertes.

## automatisation des réponses de sécurité

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

qui vous aident à mettre en œuvre les meilleures pratiques en matière AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe VPC de sécurité, l'application de correctifs à une EC2 instance Amazon ou la rotation des informations d'identification.

#### chiffrement côté serveur

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

#### politique de contrôle des services (SCP)

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

#### point de terminaison du service

Le URL point d'entrée d'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.

#### accord de niveau de service ( ) SLA

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

#### indicateur de niveau de service ( ) SLI

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

#### objectif de niveau de service ( ) SLO

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

#### modèle de responsabilité partagée

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



## SIEM

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

### point de défaillance unique (SPOF)

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

## SLA

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

## SLI

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

## SLO

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

### split-and-seed modèle

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

## SPOF

Voir [point de défaillance unique](#).

### schéma en étoile

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

### modèle de figuier étrangleur

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

un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour un exemple de la façon d'appliquer ce modèle, voir [Modernisation de l'ancienne version de Microsoft ASP.NET\(ASMX\) des services Web de manière incrémentielle à l'aide de conteneurs et d'Amazon API Gateway](#).

#### sous-réseau

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

#### contrôle de supervision et acquisition de données (SCADA)

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

#### chiffrement symétrique

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

#### tests synthétiques

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

## T

#### balises

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

#### variable cible

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

#### liste de tâches

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

## environnement de test

Voir [environnement](#).

## entraînement

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

## passerelle de transit

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

## flux de travail basé sur jonction

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

## accès sécurisé

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

## réglage

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

## équipe de deux pizzas

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

## U

### incertitude

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

### tâches indifférenciées

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

### environnements supérieurs

Voir [environnement](#).

## V

### mise à vide

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

### contrôle de version

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

## VPCpeering

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des adresses IP privées. Pour plus d'informations, consultez [What is VPC peering](#) dans la VPC documentation Amazon.

## 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

SQLFonction 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.

## WORM

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

## WQF

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

écrire une fois, lire plusieurs (WORM)

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

## Z

exploit Zero-Day

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

vulnérabilité de type « jour zéro »

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

application zombie

Application dont l'utilisation moyenne de CPU 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.