



Conseils relatifs à la ISVs gestion de bases de données Amazon Neptune en matière d'hébergement mutualisé

AWS Conseils prescriptifs



AWS Conseils prescriptifs: Conseils relatifs à la ISVs gestion de bases de données Amazon Neptune en matière d'hébergement mutualisé

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
Modèles de partitionnement des données	3
Modèle de silo	5
Cluster par locataire	5
Guide de mise en œuvre du modèle de silo	6
Modèle de groupe	8
Modèle de piscine pour LPGs	8
Stratégie de gestion immobilière	9
Stratégie d'étiquetage par préfixe	11
Stratégie multilabel	12
Implications en termes de performances pour les LPG modèles	14
Modèle de piscine pour RDF	16
SPARQLoptions de requête à l'aide du HTTP protocole Graph Store	16
Isolation des locataires pour RDF	17
Se préparer à la croissance	18
Les limites des scénarios multilocataire	18
Modèle hybride	20
Bonnes pratiques	21
Mettez à jour votre cluster Neptune avec les dernières versions	21
Utilisez des deltas au lieu de supprimer et de remplacer pour l'ingestion de données	21
Modélisez l'évolution des coûts de Neptune avec vos locataires	22
Adaptez vos clusters à la demande des clients	22
Étapes suivantes	24
Ressources	25
Collaborateurs	26
Historique de la documentation	27
Glossaire	28
#	28
A	29
B	32
C	34
D	37
E	42
F	44

G	46
H	47
I	49
L	51
M	53
O	57
P	60
Q	63
R	63
S	67
T	71
U	72
V	73
W	73
Z	74
.....	lxxvi

Conseils relatifs à la ISVs gestion de bases de données Amazon Neptune en matière d'hébergement mutualisé

Amazon Web Services ([contributeurs](#))

Août 2024 ([historique du document](#))

La mutualisation est une architecture de système informatique dans laquelle une seule instance d'une application dessert plusieurs clients. Chaque client est appelé « locataire ». Dans une architecture multi-locataires, ces instances de l'application fonctionnent dans un environnement partagé où chaque locataire est physiquement colocalisé sur la même infrastructure mais est logiquement séparé.

En tant que fournisseur de logiciels indépendant (ISV), vous pouvez utiliser Amazon Neptune pour alimenter des applications qui nécessitent de naviguer dans des données hautement connectées. Vous gérez peut-être une application logicielle en tant que service (SaaS) basée sur le cloud dans votre compte et que vous offrez des abonnements aux locataires. Les locataires peuvent ensuite accéder au service via Internet ou en privé AWS PrivateLink. L'économie de ce modèle fonctionne pour les deux parties, car le locataire a accès à des logiciels moins coûteux que ceux qu'il aurait dû acheter, créer et maintenir. En tant que tel ISV, vous pouvez facturer l'abonnement plus que ce qu'il vous en coûte pour créer et maintenir le logiciel. La question est de savoir comment adapter votre entreprise à plusieurs locataires.

La mutualisation présente ISVs d'importants avantages économiques et opérationnels. L'architecture multi-locataires offre à votre organisation un meilleur retour sur investissement (ROI). La mutualisation simplifie également les exigences opérationnelles afin que votre organisation puisse agir plus rapidement et réduire le coût de livraison du logiciel à vos locataires.

Ce document fournit des conseils pour exécuter efficacement une ISV application mutualisée à l'aide d'Amazon Neptune. Ces conseils sont basés sur les meilleures pratiques acquises au fil des années pour soutenir ISVs la fourniture réussie de solutions SaaS à leurs clients. L'évaluation de ces conseils dans le contexte des objectifs et des principes architecturaux de votre organisation vous aidera à trouver des moyens d'optimiser votre solution.

Note

Ce document ne fournit pas une liste exhaustive des meilleures pratiques. Il complète le document Applying [the AWS Well-Architected Framework for Amazon Neptune](#) en

fournissant des conseils spécifiques supplémentaires pour les charges de travail mutualisées. ISV Nous vous recommandons de prendre en compte les considérations contenues dans les deux documents lors de la conception de votre solution.

Modèles de partitionnement des données SaaS

L'un des défis pour les développeurs de SaaS est de concevoir des modèles architecturaux pour représenter et organiser les données dans un environnement mutualisé. Ces mécanismes et modèles de stockage mutualisés sont généralement appelés [partitionnement des données](#).

Dans un environnement SaaS à locataires multiples, il est important de faire la distinction entre le partitionnement des données et l'isolation des [locataires](#). Ces concepts, bien que liés, ne sont pas synonymes. Le partitionnement des données fait référence à la méthode de stockage des données pour chaque locataire. Cependant, le cloisonnement à lui seul ne garantit pas l'isolement des locataires. Des mesures supplémentaires sont nécessaires pour garantir que les données d'un locataire restent inaccessibles à un autre.

Les trois modèles courants de partitionnement des données dans les systèmes [SaaS à locataires](#) multiples sont le silo, le pool et l'hybride. Le choix entre autres des facteurs suivants :

- Conformité d'
- [Voisins bruyants](#)
- Stratégie de hiérarchisation
- Besoins opérationnels
- Besoins d'isolation des locataires

En outre, chaque type de base de données disponible sur propose AWS généralement un ensemble unique de modèles de partitionnement des données et d'isolation des locataires. Lorsque vous étudiez la manière dont les graphiques des locataires peuvent être organisés pour répondre aux différents besoins de votre solution, considérez les modèles proposés par Amazon Neptune.

Beaucoup ISVs commencent leur conception sur Neptune par l'une des assertions suivantes :

- La ISV solution nécessite une séparation physique des clients au sein de clusters distincts.
- La ISV solution nécessite des structures telles que des bases de données nommées ou des schémas utilisés dans les systèmes de gestion de bases de données relationnelles traditionnels.

Après mûre réflexion, ISVs réalisent que ces assertions ne sont pas vraies car, dans presque toutes les charges de travail, chacun de ses clients possède un graphe déconnecté dans sa base de données. La mise en œuvre de la modélisation des données et des directives d'accès décrites dans

ce document empêche le franchissement de ces limites de données et préserve la confidentialité des données des clients.

Ce guide décrit à la fois le modèle de [silo et le modèle](#) de [pool](#), mais la plupart ISVs choisissent le modèle de pool pour des raisons de coût et d'efficacité opérationnelle. Le guide décrit brièvement un modèle hybride qui combine les aspects des modèles de silo et de piscine. Certains ISVs utilisent un modèle hybride pour leurs plus gros clients afin de répondre aux exigences réglementaires ou de conformité liées à la taille du graphique.

Multi-location de type silo

Certains environnements SaaS mutualisés peuvent nécessiter le déploiement des données des locataires sur des ressources entièrement séparées pour des raisons de conformité et de réglementation. Dans certains cas, les grands clients ont besoin de clusters dédiés pour réduire l'impact du bruit sur les voisins. Dans ces situations, vous pouvez appliquer le modèle de silo.

Dans le modèle en silo, le stockage des données des locataires est totalement isolé de toutes les autres données des locataires. Toutes les structures utilisées pour représenter les données du locataire sont considérées comme physiquement uniques à ce client, ce qui signifie que chaque locataire bénéficiera généralement d'un stockage, d'une surveillance et d'une gestion distincts. Chaque locataire disposera également d'une clé AWS Key Management Service (AWS KMS) distincte pour le chiffrement. Dans Amazon Neptune, un silo correspond à un cluster par locataire.

Cluster par locataire

Vous pouvez implémenter un modèle de silo avec Neptune en ayant un locataire par cluster. Le schéma suivant montre trois locataires accédant à un microservice d'application dans un cloud privé virtuel (VPC), avec un cluster distinct pour chaque locataire.

Chaque cluster possède son propre point de [terminaison](#) afin de garantir des points d'accès distincts pour une interaction et une gestion efficaces des données. En plaçant chaque locataire dans son propre cluster, vous créez une limite bien définie entre les locataires, garantissant aux clients que leurs données sont correctement isolées des données des autres locataires. Cette isolation est également intéressante pour les solutions SaaS soumises à des contraintes réglementaires et de sécurité strictes. De plus, lorsque chaque locataire possède son propre cluster, vous n'avez pas à vous soucier des voisins bruyants, car un locataire impose une charge susceptible de nuire à l'expérience des autres locataires.

Bien que le modèle de cluster-per-tenant silo présente des avantages, il présente également des défis en matière de gestion et d'agilité. La nature distribuée de ce modèle complique l'agrégation et l'évaluation de l'activité des locataires et de la santé opérationnelle de tous les locataires. Le déploiement devient également plus difficile car la configuration d'un nouveau locataire nécessite désormais le provisionnement d'un cluster distinct. La mise à niveau devient plus difficile dans les

environnements dotés d'une couche client partagée lorsque les mises à niveau et les versions du client sont étroitement liées à la mise à niveau de la base de données.

Neptune prend en charge les clusters [sans serveur et provisionnés](#). Déterminez si la charge de travail de votre application est mieux gérée par des instances sans serveur ou provisionnées. En général, si le niveau de demande de votre charge de travail est constant, les instances provisionnées seront plus rentables. Le mode Serverless est optimisé pour les charges de travail exigeantes et très variables avec une utilisation intensive des bases de données pendant de courtes périodes, suivies de longues périodes avec une activité légère, voire pas d'activité.

Lorsque vous utilisez un cluster provisionné Neptune par locataire, vous devez sélectionner une taille d'instance qui correspond approximativement à la charge maximale de la demande de votre locataire. Cette dépendance à l'égard d'un serveur a également un impact en cascade sur la scalabilité, l'efficacité et le coût de votre environnement SaaS. Alors que l'un des objectifs du SaaS est de dimensionner dynamiquement en fonction de la charge réelle des locataires, un cluster provisionné par Neptune vous oblige à surapprovisionner pour tenir compte des périodes d'utilisation plus longues et des pics de charge. Le surprovisionnement augmente le coût par locataire. En outre, à mesure que l'utilisation des locataires évolue au fil du temps, l'augmentation ou la réduction du cluster doivent être appliquées séparément pour chaque locataire.

L'équipe Neptune déconseille généralement un modèle en silo en raison des coûts plus élevés liés aux ressources inutilisées et des complexités opérationnelles supplémentaires. Toutefois, si les charges de travail hautement réglementées ou sensibles nécessitent cette isolation supplémentaire, les clients peuvent être disposés à payer le coût supplémentaire.

Guide de mise en œuvre du modèle de silo

Pour implémenter un modèle d' cluster-per-tenant isolation en silo, créez AWS Identity and Access Management (IAM) des politiques d'accès aux [données](#). Ces politiques contrôlent l'accès aux clusters Neptune des locataires en garantissant que les locataires ne peuvent accéder qu'au cluster Neptune contenant leurs propres données. Associez la IAM politique de chaque locataire à un IAM rôle. Le microservice de l'application utilise ensuite le IAM rôle pour générer des informations d'[identification temporaires](#) détaillées à l'aide de la AssumeRole méthode de AWS Security Token Service ().AWS STS Ces informations d'identification, qui ont accès uniquement au cluster Neptune pour ce locataire, sont utilisées pour se connecter au cluster Neptune du locataire.

L'extrait de code suivant montre un exemple de politique basée sur les données IAM :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "neptune-db:ReadDataViaQuery",
        "neptune-db:WriteDataViaQuery"
      ],
      "Resource": "arn:aws:neptune-db:<region>:<account-id>:tenant-1-cluster/*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::<account-id>:role/tenant-role-1"
        }
      }
    }
  ]
}
```

Le code fournit un exemple de locataire `tenant-1`, avec un accès aux requêtes en lecture et en écriture à leur cluster Neptune respectif. L'élément `Condition` garantit que seule l'entité appelante (le principal), qui a assumé le rôle IAM `tenant-1` (`tenant-role-1`), est autorisée à accéder au cluster Neptune `tenant-1`.

Conception multilocataire basée sur des modèles de groupes

Parfois, il n'est pas nécessaire ou faisable de mettre en œuvre le modèle de silo en raison des coûts ou des frais d'exploitation :

- Il se peut que vous ne disposiez pas des ressources nécessaires pour gérer un cluster individuel par locataire.
- Il n'est peut-être pas nécessaire de séparer physiquement les données de chaque locataire, et une séparation logique est suffisante pour répondre à leurs besoins et aux exigences de conformité.

Le schéma suivant montre le modèle de pool, les données des locataires étant placées dans un seul cluster Amazon Neptune, et tous les locataires partageant une base de données commune.

Ce [modèle d'isolation des pools](#) réduit les frais de gestion et peut améliorer l'efficacité opérationnelle car il y a moins de clusters à gérer. En outre, les ressources informatiques peuvent être partagées entre plusieurs clients au lieu de rester inactives pendant les périodes d'inactivité des clients.

Lorsque vous utilisez le modèle de pool, vous pouvez modéliser les données de deux manières. Votre approche varie selon que vous créez un [graphe de propriétés étiqueté \(LPG\)](#) ou un graphe avec le [Resource Description Framework \(RDF\)](#).

Modèle de pool pour les graphes de propriétés étiquetés

Il existe trois approches différentes du modèle de pool pour LPGs Amazon Neptune :

- Stratégie de propriété – Choisissez la stratégie de propriété lorsque vous devez donner la priorité à l'utilisation de structures de bibliothèque établies, telles que le langage Apache TinkerPop Gremlin, aux performances [PartitionStrategy](#) supérieures.
- Stratégie d'étiquette préfixe – Nous recommandons la stratégie d'étiquette préfixe pour la plupart des scénarios en fonction des performances et de la limitation des effets de voisinage bruyants.
- Stratégie à étiquettes multiples – La stratégie à étiquettes multiples offre les meilleures performances de la stratégie à étiquettes préfixes. Il prend également en charge l'exécution de

requêtes couvrant tous les locataires d'un cluster (par exemple, des ISV requêtes de reporting ou de surveillance pour tous les locataires).

Stratégie de gestion immobilière

Avec LPGs, les utilisateurs peuvent ajouter des propriétés de paire clé-valeur aux nœuds, ou sommets, et aux arêtes. Pour obtenir une séparation logique, la plupart des clients la modélisent intuitivement sous la forme d'une propriété unique sur chaque nœud et chaque périphérie avec une clé de propriété commune au locataire. La clé de propriété du locataire représente tous les locataires propriétaires du nœud. L'identifiant du locataire est une valeur unique qui identifie un locataire individuel.

Le schéma suivant illustre ce modèle. Les deux sous-graphes déconnectés comportent différents nœuds et arêtes étiquetés, la clé de propriété du locataire étant représentée par TId. Chaque nœud et chaque arête d'un sous-graphe ont une TId valeur de 1. Dans l'autre sous-graphe, chaque nœud et chaque arête ont une TId valeur de 2.

Dans les graphes de propriétés étiquetés, il existe deux manières de gérer cela. Le langage de requête Gremlin propose la bibliothèque de [PartitionStrategy](#) traversée pour aider à gérer le partitionnement des données. Le code de l'exemple suivant s'attend à ce que chaque nœud et chaque arête aient une propriété appelée TId :

```
strategy1 = new PartitionStrategy(partitionKey: "TId", writePartition: "1",
    readPartitions: ["1"])
strategy2 = new PartitionStrategy(partitionKey: "TId", writePartition: "2",
    readPartitions: ["2"])
```

Lorsque de nouveaux nœuds ou arêtes sont écrits, la propriété "TId" est ajoutée avec une valeur de "1" ou "2", selon que strategy1 ou strategy2 a été sélectionné. Pour le client avec "TId" ou "1", vous utilisez strategy1. L'exemple suivant montre comment écrire des données pour ce client :

```
g.withStrategies(strategy1).addV("Label1").property("Value", "123456").property(id,
    "Item_1")
```

Pour les requêtes de lecture, un filtre pour "TId == '1'" ou "TId == '2'" est ajouté à chaque traversée de nœud ou de bord en utilisant `strategy1` ou `strategy2`, respectivement. Ces stratégies de partition simplifient votre code, mais ne sont pas nécessaires. L'avantage de l'utilisation de cette stratégie est qu'elle peut être injectée au niveau d'autorisation et transmise au code de niveau inférieur qui forme la requête. Cela permet de séparer le code qui détermine l'identifiant du client (TId) de la logique de la requête.

L'exemple de code suivant montre une requête Gremlin pour lire des données :

```
g.withStrategies(strategy1).V().hasLabel("Label1")
```

Le code précédent équivaut à l'exemple suivant :

```
g.V().hasLabel("Label1").has("TId", "1")
```

De même, lorsque vous écrivez des données à l'aide de Gremlin, vous pouvez utiliser la requête suivante :

```
g.withStrategies(strategy1).addV("Label1").property("Value").property(id, "Item_1")
```

Le code précédent est équivalent à l'exemple suivant, qui n'utilise pas la stratégie de partition et nécessite donc que la "TId" propriété soit écrite explicitement :

```
g.addV("Label1").property("TId", "1").property("Value").property(id, "Item_1")
```

Dans openCypher, ces bibliothèques n'existent pas. Vous êtes responsable de la rédaction et de la modification de vos requêtes pour ajouter l'identifiant du locataire en tant que propriété sur les nœuds et les arêtes. Par exemple :

```
CREATE (n:Item {`~id`: 'Item_1', Value: '123456', TId: '1'})
CREATE (n:Item {`~id`: 'Item_2', Value: '123456', TId: '2'})
```

Notez la similitude entre le code Gremlin sans la stratégie de partition. Vous pouvez ensuite lire le nœud écrit à partir de la première CREATE instruction en utilisant le code suivant :

```
MATCH (n:Item {TId: '1'})
RETURN n
```

```
--oI  
MATCH (n:Item)  
WHERE n.TId == '1'  
RETURN n
```

Vous pouvez choisir la stratégie de propriété lorsque vous souhaitez utiliser des constructions natives de TinkerPop Gremlin telles que `PartitionStrategy`. Cependant, ce modèle présente des inconvénients en termes de performances sur Amazon Neptune par rapport à la stratégie préfixe-étiquette. Pour en savoir plus sur ces inconvénients en termes de performances, consultez la section [Implications des LPG modèles en termes de performances](#).

Si les conditions suivantes s'appliquent, envisagez de modéliser la stratégie de propriété uniquement sur les nœuds, et non sur les arêtes :

- Votre graphique comporte nettement plus d'arêtes que d'étiquettes.
- Chaque locataire est un graphe déconnecté.
- Vous accédez au graphe uniquement en utilisant des nœuds comme point de départ, et non des étiquettes.

Stratégie d'étiquetage par préfixe

Si la performance est une préoccupation majeure, nous vous recommandons vivement de privilégier la stratégie d'étiquette préfixe plutôt que la stratégie immobilière.

Dans la stratégie d'étiquette préfixe, vous étiquetez chaque nœud avec une combinaison d'identifiant de locataire et d'étiquette de nœud. Par exemple, si le locataire possède un identifiant de "1" et que l'étiquette du nœud est "Label1", vous spécifiez l'étiquette du nœud sous la forme "1-Label1". Le schéma suivant montre deux sous-graphes déconnectés qui utilisent ce modèle.

Lorsque vous écrivez des données dans Gremlin, vous pouvez ajouter un numéro d'identification à l'étiquette de n'importe quel nœud :

```
g.addV("1-Label1")  
g.addV("2-Label16")
```

Lorsque vous interrogez ce graphe, vous pouvez vérifier l'existence de ce préfixe sur un nœud :

```
g.V().hasLabel("1-Label1")
```

openCypher Vous pouvez y écrire des données en utilisant une CREATE instruction :

```
CREATE (n:`1-Label1` {`~id`: 'Item_1', Value: 'XYZ123456'})
```

Pour rechercher les données que vous avez saisies openCypher, utilisez le code suivant :

```
MATCH n= (:`1-Label1`)  
RETURN n
```

La stratégie d'étiquette préfixe suppose que tous les nœuds sont affectés à un ou plusieurs locataires et que les autorisations ne sont pas attribuées à la périphérie. Évitez d'utiliser cette stratégie sur les étiquettes de bord, car cela provoquera un grand nombre de prédicats et aura un impact négatif sur les performances de Neptune.

L'approche de l'étiquette par préfixe présente deux inconvénients principaux. Tout d'abord, il est difficile d'exécuter des requêtes qui concernent tous les locataires. Par exemple, une requête qui compte tous les nœuds d'une étiquette donnée à des fins de reporting ou de surveillance. Si tel est votre cas d'utilisation, envisagez de combiner cette stratégie avec la stratégie à étiquettes multiples. Pour plus d'informations sur la combinaison de stratégies, consultez la section sur le [modèle hybride](#).

Deuxièmement, la stratégie du préfixe-étiquette nécessite des contrôles qui garantissent l'application correcte du préfixe approprié à chaque requête afin d'éviter les fuites de données. Cependant, cette stratégie est l'option la plus efficace pour les charges de travail qui nécessitent des requêtes à faible latence, et nous la recommandons vivement. La section [Implications en termes de performances pour les LPG modèles](#) fournit des exemples expliquant pourquoi il s'agit de la stratégie la plus efficace.

Stratégie multilabel

La troisième option consiste à utiliser une stratégie à étiquettes multiples. Pour cette approche, vous ajoutez des étiquettes supplémentaires à chaque nœud du graphe. Par exemple, si vous devez filtrer toutes les données d'un locataire donné, ajoutez l'étiquette d'identification du locataire. Si vous devez filtrer toutes les données d'une étiquette donnée, quel que soit le locataire, ajoutez cette étiquette. Le schéma suivant montre la stratégie à étiquettes multiples appliquée en utilisant trois étiquettes pour chaque nœud.

Vous pouvez désormais accéder au graphique en utilisant trois modèles différents :

- Filtrez sur Label1 Activé pour renvoyer tous les nœuds avec Label1 tous les locataires.
- Filtrez 1 pour renvoyer tous les nœuds du locataire 1.
- Filtrez 1-Label1 pour renvoyer tous les nœuds uniquement pour le locataire 1 avec étiquetteLabel1.

En LPGs effet, il existe deux manières de le mettre en œuvre.

Dans Gremlin, vous pouvez utiliser la stratégie de traversée appelée [SubgraphStrategy](#) pour limiter la portée de toutes les requêtes aux seuls sommets portant une étiquette spécifique, tels que : "Label1"

```
g.withStrategies(  
  new SubgraphStrategy(  
    vertices=hasLabel("Label1")  
  )  
)
```

Contrairement à PartitionStrategy cela, a un SubgraphStrategy impact sur la lecture des données uniquement, et non sur leur écriture. Pour écrire les données, attribuez manuellement les libellés à chaque requête :

```
g.addV("Label1").property("Value", "XYZ123456")  
.addV("Label2").property("Value", "XYZ123456")
```

Lors de la lecture des données, vous pouvez les utiliser SubgraphStrategy pour interroger tous les nœuds avec "Label1" :

```
g.withStrategies(  
  new SubgraphStrategy(vertices=.hasLabel("Label1"))  
)  
V().has("Value", "XYZ123456")
```

Neptune renvoie uniquement le premier enregistrement, dont la valeur est "Label1" égale à. "XYZ123456" C'est équivalent à la requête suivante, qui n'utilise pas SubgraphStrategy :

```
g.V().hasLabel("Label1").hasValue("XYZ123456")
```

Dans cette requête de base, il apparaît que SubgraphStrategy son utilisation est plus complexe. N'oubliez pas que vos bibliothèques peuvent fournir une instance g de la stratégie déjà définie. Les développeurs n'ont pas à s'assurer que les filtres appropriés sont appliqués :

```
def getGraphTraversal():
    return g.withStrategies(new SubgraphStrategy(vertices=.hasLabel("Label1"))

getGraphTraversal().has("Value", "XYZ123456")
```

Les openCypher bibliothèques n'ont pas ces structures, vous devez donc créer plusieurs étiquettes pour chaque nœud :

```
CREATE (n:`1`:`Label1`:`1-Label1` {`~id`: 'Item_1', Value: '12345'})
```

Lorsque vous utilisez ces étiquettes pour filtrer un sous-graphe, vous pouvez renvoyer des nœuds portant l'étiquette client que vous recherchez ou qui partagent une relation avec un autre nœud portant cette étiquette :

```
MATCH n=(:`Label1`:`1`)
// or
MATCH n=(:`1-Label1`)
```

La stratégie à étiquettes multiples vous donne la plus grande flexibilité pour interroger les nœuds par type (Label1) ou par tenant (1), ou pour utiliser la stratégie d'étiquette de préfixe la plus efficace lorsque les performances sont primordiales (). 1-Label1

Le principal inconvénient de cette stratégie est que chaque étiquette est un objet supplémentaire stocké dans votre graphique. Un objet est un nœud, une arête ou une propriété d'un nœud ou d'une arêteLPGs. La vitesse d'ingestion est mesurée et limitée par le nombre d'objets par seconde, et les coûts de stockage dépendent du nombre de gigaoctets consommés. Cela signifie que des objets supplémentaires peuvent avoir un impact mesurable à grande échelle.

Implications en termes de performances pour les LPG modèles

Le cours [Data Modeling for Amazon Neptune](#) de AWS Skill Builder décrit en détail les aspects internes du modèle de données Neptune et ses implications en termes de modélisation, mais nous allons résumer ici les considérations importantes relatives à ces conceptions. Envisagez d'avoir trois locataires (T1, T2, T3) sur un seul cluster Neptune. Ces locataires ont les attributs suivants :

- Le locataire 1 (T1) compte 100 millions de nœuds au total, dont 10 millions sont de type Item.
- Le locataire 2 (T2) compte 10 millions de nœuds au total, dont 1 million sont de type Item.
- Le locataire 3 (T3) compte 100 millions de nœuds au total, dont 1 million sont de type Item.

Exécutez une requête qui récupérera les objets pour Tenant 3 en utilisant la stratégie immobilière. Neptune examine les statistiques de deux appels d'index :

- Où `tenant property key=T3` ont 100 millions de résultats
- Où `label = Item` a 12 millions de résultats (10 millions de T1 + 1 million de T2 + 1 million de T3)

L'optimiseur de requêtes Neptune détermine qu'il est préférable d'appliquer cette dernière requête en premier (12 millions de résultats), puis inspecte chaque élément. `tenant property key=T3` Vous récupérez 12 millions d'éléments pour trouver le million de résultats.

Notez l'impact bruyant de cette requête sur les voisins. Si vous aviez 100 millions de nœuds Item par locataire, la première requête aurait 300 millions de résultats au lieu de 12 millions (cela est trop simplifié à des fins d'illustration). L'optimiseur Neptune a peut-être appliqué un ordre d'opérations différent).

Ensuite, considérez la stratégie du préfixe-étiquette. Effectuez un seul appel d'index `where label=T3-Item`, qui renvoie 1 million de résultats. Cela donne le même résultat que la stratégie immobilière, mais permet de récupérer 11 millions d'enregistrements de moins. De plus, vous n'avez plus à vous soucier des voisins bruyants, car l'étiquette ne se chevauche pas dans l'index.

La stratégie à étiquettes multiples n'améliore pas directement les performances des requêtes par rapport à la stratégie immobilière. Le filtrage par valeur de propriété est comparable au filtrage par valeur d'étiquette lorsque l'espace de recherche est également comparable. Au contraire, la stratégie à étiquettes multiples favorise une plus grande flexibilité. La stratégie à étiquettes multiples fournit des performances équivalentes à la stratégie d'étiquette préfixe pour `label=T3` ou `label=Item`. La stratégie à labels multiples fournit des performances équivalentes à celles de la stratégie immobilière pour `label=Item`. L'avantage est de prendre en charge une variété de modèles d'accès.

Modèle de piscine pour RDF

Le Resource Description Framework (RDF) utilise le concept de graphes nommés, qui fournit un moyen logique de séparer les données. Dans Amazon Neptune, vous disposez d'un graphe nommé par défaut et de graphes nommés définis par l'utilisateur. Vous pouvez créer autant de graphes nommés que vous le souhaitez. Collectivement, ils sont appelés RDF ensemble de données. Tous les graphes nommés, qu'ils soient définis par défaut ou définis par l'utilisateur, sont définis par un identifiant de ressource internationalisé (IRI) au sein du RDF jeu de données. Dans Neptune, à moins qu'un utilisateur n'ait déclaré un graphe nommé lors de l'écriture de données, tous les [triplets](#) sont considérés comme faisant partie du graphe nommé par défaut.

Il existe plusieurs cas d'utilisation pour les graphes nommés :

- Partitionnement et isolation des données
- Provenance des données
- Gestion des versions
- Inférence

Ce guide se concentre sur le cas d'utilisation du partitionnement des données. Nous recommandons de créer un graphe nommé défini par l'utilisateur pour chaque locataire.

SPARQL options de requête à l'aide du HTTP protocole Graph Store

Les exemples de requêtes suivants utilisent le SPARQL protocole et le langage de RDF requête (SPARQL) et le HTTP protocole Graph Store pour interroger ou créer un graphe nommé pour un locataire.

- HTTP GET– Pour récupérer un graphique spécifique d'un locataire :

```
curl --request GET 'https://your-neptune-endpoint:port/sparql/gsp/?graph=http%3A//  
www.example.com/named/tenant1'
```

- HTTP PUT– Pour créer ou remplacer un graphe nommé spécifique par une charge utile spécifiée dans la demande :

```
curl --request PUT -H "Content-Type: text/turtle" \ --data-raw "@prefix ex: http://  
example.com/ . ex:subject ex:predicate ex:object ." \
```

```
'https://your-neptune-endpoint:port/sparql/gsp/?graph=http%3A//www.example.com/named/tenant1'
```

Dans RDF, un objet est un triple.

- HTTP POST– Pour créer un nouveau graphe nommé s'il n'en existe pas, ou pour le fusionner avec un graphique existant :

```
curl --request POST -H "Content-Type: text/turtle" \  
--data-raw "@prefix ex: http://example.com/ . ex:subject ex:predicate ex:object ." \  
'https://your-neptune-endpoint:port/sparql/gsp/?graph=http%3A//www.example.com/named/tenant1'
```

Isolation des locataires pour RDF

Pour une isolation logique des données avec les garde-fous nécessaires en place au niveau de la couche application, créez un mappage entre le locataire et les graphes nommés définis par l'utilisateur. Lorsque vous concevez une solution mutualisée pour un RDF ensemble de données, tenez compte des aspects suivants de RDF et : [SPARQL](#)

- Dans Neptune, lorsque vous effectuez une requête sans spécifier de graphe nommé, il récupère tous les triplets correspondant au modèle dans tous les graphes nommés de la base de données.
- Dans RDF, il n'existe aucune contrainte concernant les connexions entre les nœuds de graphes nommés différents. Par exemple, dans le schéma précédent, un nœud en entrée : G1 peut être connecté à un nœud en : G2 via une arête.

Par exemple, si l'utilisateur final d'un locataire particulier soumet une requête au API, il API doit valider les exigences suivantes avant de soumettre la requête à la base de données Neptune :

- Toute requête étendue à un seul locataire doit spécifier un graphe nommé. Dans le cas contraire, vous risquez de divulguer des données entre locataires.
- Les requêtes de mise à jour ou de suppression doivent toujours spécifier un graphe nommé.
- Les nœuds situés de part et d'autre d'une arête ou d'une relation doivent toujours appartenir au graphe nommé correctement.

Pour plus d'informations sur les bonnes pratiques, consultez la documentation de [Neptune](#).

Se préparer à la croissance

Lorsque vous utilisez le modèle de pool avec succès, vous finissez par dépasser la taille d'un seul cluster Neptune. Le nombre de locataires augmente, ou le nombre de locataires augmente, et le taux d'ingestion des données nécessaires pour tous vos clients dépasse les capacités du cluster. Dans ce cas, vous devrez répartir vos clients sur plusieurs clusters. Concevez cette configuration dès le départ au lieu d'essayer de la modifier ultérieurement. Même si votre échelle initiale consiste à n'utiliser qu'un seul cluster, modélisez les composants dont vous aurez besoin pour acheminer les locataires entre plusieurs clusters à l'avenir lorsque vous atteindrez cette échelle.

Si votre solution nécessite davantage de ressources en fonction de la taille de votre locataire, préparez-vous également à sa croissance. Si plusieurs clients d'un même cluster augmentent de manière significative, ce cluster risque de ne plus répondre à vos besoins. Concevez une stratégie pour déplacer les locataires vers un autre cluster ou diviser un cluster existant en deux à l'aide de la fonctionnalité de [clonage de base](#) de données Amazon Neptune.

Familiarisez-vous avec le [protocole Neptune Copy-on-Write](#), qui peut vous faire économiser de l'argent lorsque vous implémentez le clonage de bases de données. Si vous divisez un cluster en raison de problèmes d'ingestion, il peut être plus efficace de ne pas supprimer de données des clusters, à condition que vos politiques le permettent. Les deux clusters partageront une page de données si elle est inchangée, mais pas si la page de données a été modifiée (car certaines données ont été supprimées).

Note

Ces directives s'appliquent à la version la plus récente de Neptune au moment de la rédaction de cet article, à savoir la version 1.3.1 de Neptune. Ces instructions sont susceptibles de changer dans les futures versions au fur et à mesure de l'évolution de la couche de stockage Neptune.

Les limites des scénarios multilocataire

Sachez que certaines fonctionnalités de Neptune ne sont pas conçues pour les scénarios de location multiple. Les locataires ne doivent pas avoir un accès direct aux points de terminaison Neptune dans un modèle de pool, car ces stratégies de mutualisation ne sont pas appliquées au niveau de la base de données. Conservez toujours une sorte de proxy entre vos clients et le terminal Neptune qui applique les conceptions décrites dans ce document. Voici quelques exemples de ce type de proxy :

-
- Ajouter les filtres d'étiquettes dans votre couche client
 - Avoir un API qui mappe le jeton d'authentification à un identifiant de locataire et injecte ce filtre dans la requête

Ces conseils s'appliquent également à l'accès direct aux clients à des fonctionnalités telles que les carnets graphiques Neptune, l'explorateur de graphes Neptune ou Neptune Streams.

Multi-location du modèle hybride

Les solutions SaaS utilisent souvent une combinaison de modèles de silo et de pool. Différents facteurs influencent la décision quant au moment et à la manière d'utiliser à la fois les modèles de silo et de piscine dans le même environnement.

L'un de ces facteurs est la hiérarchisation, où une solution SaaS offre des expériences uniques à chaque niveau de locataires. Par exemple, si vos niveaux sont Free, Standard et Premium, les données de vos locataires du niveau Free peuvent être stockées dans un cluster Neptune partagé à l'aide d'un modèle de pool. Pour vos locataires des niveaux Standard et Premium, vous pouvez utiliser un modèle de cluster-per-tenant silo.

En outre, certains fournisseurs de SaaS ont la capacité de créer leur solution de pool sur un cluster Amazon Neptune partagé comme base. Ils peuvent ensuite créer un cluster Neptune distinct pour les locataires qui ont besoin d'un stockage cloisonné, souvent pour des raisons de conformité et de réglementation.

Bien que cela puisse ajouter un niveau de complexité à votre couche d'accès aux données et à votre profil de gestion, cela peut également permettre à votre entreprise de hiérarchiser son offre pour répondre aux exigences des clients.

Bonnes pratiques opérationnelles relatives à ISVs

La plupart des directives de cette section constituent les meilleures pratiques pour tous les clients, mais elles ont une importance accrue pour les ISVs.

Mettez à jour votre cluster Neptune avec les dernières versions

Dans les [notes de mise à jour](#) d'Amazon Neptune, vous pouvez voir que chaque version apporte un certain nombre de corrections de bogues, d'améliorations des performances et de nouvelles fonctionnalités. Utilisez la dernière version de vos clusters Neptune autant que possible.

Si vous trouvez un bogue non découvert dans votre charge de travail et que votre cluster utilise la dernière version, les ingénieurs de Neptune peuvent créer un correctif privé pour votre cluster (si cela est justifié et si vous le souhaitez). Le correctif peut être transféré jusqu'à la prochaine version, date à laquelle ce correctif sera généralement disponible. Pour vous aider à mettre à jour vos clusters vers la dernière version, utilisez la solution [Neptune Blue/Green](#).

Utilisez des deltas au lieu de supprimer et de remplacer pour l'ingestion de données

Vous pouvez utiliser plusieurs techniques pour apporter ou écrire des données dans Neptune. De nombreux clients essaient de simplifier leur ingestion de données en supprimant et en réinsérant leur graphique chaque fois qu'une modification est reçue dans le flux. Ils peuvent ajouter une `last-modified` propriété à chaque nœud et rechercher régulièrement les nœuds qui n'ont pas été modifiés depuis une date spécifiée et les supprimer. Bien que ces techniques simplifient le processus d'ingestion des données, elles ont des répercussions sur la santé et l'évolutivité à long terme de votre cluster Neptune.

Neptune utilise tout d'abord le [codage des chaînes par dictionnaire](#). À moins que vous ne spécifiez explicitement les IDs nœuds et les arêtes, Neptune génère une chaîne GUID représentée sous forme de chaîne pour l'ID et stocke cette chaîne dans le dictionnaire. Si vous supprimez et ajoutez constamment des objets, la génération automatique des IDs provoquera une surcharge dans le dictionnaire.

Ensuite, Neptune évolue pour ingérer au maximum 120 000 objets par seconde. Si vous supprimez et ajoutez continuellement des objets, vous consommez une grande partie de cette bande passante sur

des objets qui ne changent pratiquement pas. Cela limite le nombre de locataires que vous pouvez héberger sur un cluster, nécessite des instances d'écriture plus importantes dans les clusters et nécessite davantage d'opérations d'E/S. Tous ces facteurs augmentent vos coûts.

Nous vous recommandons vivement de développer un moyen de calculer le delta réel de ce qui a changé au lieu d'utiliser les méthodes de suppression et d'ajout. Cependant, certaines sources de données ne sont pas propices à cela (par exemple, les API appels renvoyant l'état actuel ou les événements qui ne permettent pas de suivre exactement ce qui a changé). Si votre source de données brutes ne permet pas d'identifier les modifications, utilisez vos processus d'extraction, de transformation et de chargement (ETL) pour calculer le delta. Par exemple, vous pouvez conserver les instantanés de chaque capture de données précédente au format Parquet, les utiliser AWS Glue pour calculer les différences entre ces instantanés et transmettre uniquement les différences à Neptune.

Modélisez l'évolution des coûts de Neptune avec vos locataires

Que vous utilisiez un modèle de silo, de pool ou hybride, vos coûts de cloud évolueront en fonction de la taille de vos locataires. Les locataires qui ont besoin d'un plus grand nombre de connexions simultanées ont besoin d'instances plus grandes ou de répliques en lecture que ceux qui ont moins de connexions simultanées. Il en va de même pour les locataires qui ont besoin d'une ingestion de données plus rapide.

Les trois composantes du coût du cluster Neptune sont la taille (et le nombre) d'instances, la taille des données (Go-mois) et les opérations d'E/S (par million). Bien que ces coûts soient généralement spécifiques à la charge de travail, ils varient en fonction de la taille et du volume de données et peuvent être mesurés à l'aide d'AWS outils. Suivez et comprenez les économies d'échelle par rapport aux indicateurs clés de la taille de vos locataires, notamment la façon dont leur taille varie au fil du temps. Si l'imprévisibilité de vos frais d'E/S a un impact sur vos marges, pensez à choisir le stockage [optimisé pour les E/S de Neptune pour un coût plus](#) prévisible.

Adaptez vos clusters à la demande des clients

Il n'existe aucune formule éprouvée pour dimensionner correctement la taille de votre instance Neptune. La [documentation de Neptune](#) fournit des conseils, mais les variables sont trop nombreuses pour recommander un mappage direct. Ces variables incluent, mais sans s'y limiter :

- Modèle de données

- Forme de données
- Simultanéité des requêtes
- Complexité de requête

Planifiez des tests afin de déterminer la taille optimale pour vos charges de travail et vos profils de locataires. En général, nous recommandons d'utiliser des instances provisionnées pour des raisons de rentabilité et de prévisibilité. Si vos objectifs en matière d'expérience client privilégient une évolutivité optimale par rapport aux coûts, pensez à utiliser les [instances Neptune Serverless](#) pour garantir une expérience plus cohérente, quelles que soient les fluctuations de charge de travail.

[Si les charges de travail de lecture de votre locataire présentent une variabilité significative entre leurs pics et leurs creux, combinez les instances Neptune Serverless avec l'auto-scaling de Neptune.](#)

Il faut généralement 10 à 15 minutes pour qu'une nouvelle réplique de lecture soit mise en ligne après son initialisation. Cela signifie que l'auto-scaling peut à lui seul gérer les variations prolongées du trafic, mais qu'il n'est pas suffisant pour les pics d'activité qui évoluent rapidement. En combinant Neptune Serverless et Neptune auto-scaling, vous pouvez à la fois augmenter ou diminuer le nombre de répliques de lecture entrantes et sortantes.

Si vos locataires ont des profils de charge de travail ou des accords de niveau de service (SLAs) très différents, envisagez d'utiliser des [points de terminaison personnalisés](#) et des répliques de lecture dédiées pour diriger le trafic vers des instances optimisées pour ce trafic. L'optimisation peut inclure un dimensionnement différent de l'instance, des modèles de requête spécifiques ou le préchauffage du cache tampon.

Étapes suivantes

Si vous commencez tout juste à implémenter Amazon Neptune pour votre ISV application mutualisée, réfléchissez bien au modèle que vous souhaitez. Le changement de modèle sera plus coûteux plus tard dans votre voyage.

Si vous en êtes au début de votre parcours, vérifiez que vous utilisez le modèle le mieux adapté à vos besoins et que vous suivez les instructions relatives à ce modèle.

Planification anticipée. Lorsque vous en êtes au début de votre parcours, il est tentant de différer le travail visant à répartir les clients entre les clusters ou à optimiser vos ETL processus pour intégrer le delta des modifications au lieu de supprimer et d'ajouter à nouveau des sommets et des arêtes. À mesure que vous évoluez, ces décisions peuvent avoir un impact négatif sur les performances et les coûts.

Enfin, si vous êtes déjà bien avancé, ces conseils peuvent vous rassurer sur le fait que votre architecture est optimale, ou ils peuvent apporter des modifications pour améliorer votre architecture.

Si vous avez des questions sur ces conseils ou si vous avez besoin d'une assistance supplémentaire, contactez votre Compte AWS équipe et demandez une session avec un spécialiste de Neptune.

Ressources

- [Documentation Amazon Neptune](#)
- [Modélisation des données pour Amazon Neptune \(cours\)](#)
- [Appliquer le framework AWS Well-Architected pour Amazon Neptune](#)
- [Cadre Well-Architected](#)
- [Conseils pour les architectures à locataires multiples sur AWS](#)
- [Stratégies d'isolation des locataires en mode SaaS : isoler les ressources dans un environnement multi-locataires](#)
- [TinkerPop Documentation d'Apache](#)
- [SPARQL](#)

Collaborateurs

Les personnes qui ont contribué à ce guide incluent :

- Brian O'Keefe, directeur de WW NeptuneSSA, AWS
- Veeresham Gande, directeur technique principal des comptes, AWS
- Dana Owens, architecte de solutions pour les startups, AWS
- Nima Seifi, architecte de solutions de démarrage, AWS

Historique du document

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

Modification	Description	Date
Publication initiale	—	3 septembre 2024

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

ACIDE

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

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir [intelligence artificielle](#).

AIOps

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

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

Un emplacement distinct au sein d'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 La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, la AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications afin de préparer

l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le [site Web AWS CAF](#) et le [livre blanc AWS CAF](#).

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

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

B

mauvais bot

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

BCP

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

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'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.

CCo E

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

CDC

Consultez la section [Capture des données de modification](#).

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

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

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

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

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub 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 AI fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir [vision par ordinateur](#).

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

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

ensemble profond

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

deep learning

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

defense-in-depth

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

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

administrateur délégué

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

déploiement

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

environnement de développement

Voir [environnement](#).

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

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

reprise après sinistre (DR)

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

DML

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

conception axée sur le domaine

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

DR

Consultez la section [Reprise après sinistre](#).

détection de dérive

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

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

DVSM

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

E

EDA

Voir [analyse exploratoire des données](#).

EDI

Voir échange [de données informatisé](#).

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

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

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

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 points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le [guide d'implémentation du programme](#).

ERP

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

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

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

branche de fonctionnalités

Voir [la succursale](#).

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

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

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le [modèle de fondation](#).

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les [restrictions géographiques](#).

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez [la haute disponibilité](#).

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation de l'historien

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

laC

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

politique basée sur l'identité

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

application inactive

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

Ilo T

Voir [Internet industriel des objets](#).

infrastructure immuable

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

VPC entrant (d'entrée)

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

I

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

migration incrémentielle

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

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

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

VPC d'inspection

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

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

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir [Internet des objets](#).

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

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

ITSM

Consultez la section [Gestion des services informatiques](#).

L

contrôle d'accès basé sur des étiquettes (LBAC)

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

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

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

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

principe de moindre privilège

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

lift and shift

Voir [7 Rs](#).

système de poids faible

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

LLM

Voir le [grand modèle de langage](#).

environnements inférieurs

Voir [environnement](#).

M

machine learning (ML)

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

branche principale

Voir [la succursale](#).

malware

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

services gérés

Services AWS 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 AWS Well-Architected Framework.

compte membre

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

MAILLES

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

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

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

microservice

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

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir [apprentissage automatique](#).

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

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

MQTT

Voir [Message Queuing Telemetry Transport](#).

classification multi-classes

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

infrastructure mutable

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

O

OAC

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

OAI

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

OCM

Voir [gestion du changement organisationnel](#).

migration hors ligne

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

OI

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

OLA

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

migration en ligne

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

OPC-UA

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

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir [technologie opérationnelle](#).

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les [informations personnelles identifiables](#).

manuel stratégique

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

PLC

Voir [contrôleur logique programmable](#).

PLM

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

politique

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

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

confidentialité dès la conception

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

zones hébergées privées

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

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir [environnement](#).

contrôleur logique programmable (PLC)

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

chaînage rapide

Utiliser le résultat d'une invite [LLM](#) comme entrée pour l'invite suivante afin de générer de meilleures réponses. Cette technique est utilisée pour décomposer une tâche complexe en sous-tâches ou pour affiner ou développer de manière itérative une réponse préliminaire. Cela

permet d'améliorer la précision et la pertinence des réponses d'un modèle et permet d'obtenir des résultats plus précis et personnalisés.

pseudonymisation

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

publish/subscribe (pub/sub)

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

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

CHIFFON

Voir [Retrieval Augmented Generation](#).

rançongiciel

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

Matrice RASCI

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

RCAC

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

réplica en lecture

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

réarchitecte

Voir [7 Rs](#).

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir [7 Rs](#).

Région

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

régression

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

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

réhéberger

Voir [7 Rs.](#)

version

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

déplacer

Voir [7 Rs.](#)

replateforme

Voir [7 Rs.](#)

rachat

Voir [7 Rs.](#)

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir [7 Rs](#).

se retirer

Voir [7 Rs](#).

Génération augmentée de récupération (RAG)

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

rotation

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

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

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

RPO

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

RTO

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

runbook

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

S

SAML 2.0

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

SCADA

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

SCP

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

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

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

SLI

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

SLO

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

split-and-seed modèle

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

SPOF

Voir [point de défaillance unique](#).

schéma en étoile

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

modèle de figuier étrangleur

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

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir [environnement](#).

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La

branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

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

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir [environnement](#).

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

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

flux de travail

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

VER

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

WQF

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

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité 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.

invite Zero-Shot

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

application zombie

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

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