



Intégration d'Amazon Aurora PostgreSQL compatible avec des bases de données hétérogènes et Services AWS

AWS Directives prescriptives



AWS Directives prescriptives: Intégration d'Amazon Aurora PostgreSQL compatible avec des bases de données hétérogènes et Services AWS

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

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

Table of Contents

Introduction	1
Présentation	1
Connexion à des bases de données distantes et hétérogènes	1
Journalisation	2
Se connecter au stockage	2
Calcul sans serveur	2
Intégrations pour l'analyse	2
Extensions supplémentaires pour l'intégration avec Services AWS	3
Objectifs	3
Prérequis	4
Intégration compatible avec Aurora PostgreSQL	5
Bases de données PostgreSQL distantes	6
Cas d'utilisation de postgres_fdw et étapes de haut niveau	6
Utiliser dblink pour créer des connexions	10
Bases de données hétérogènes	11
Cas d'utilisation de tds_fdw et étapes de haut niveau	12
CloudWatch Intégration des journaux	15
Nettoyage	16
Intégration Amazon S3	17
Cas d'utilisation de aws_s3 et étapes de haut niveau	17
Intégration Lambda	19
Cas d'utilisation Lambda	19
AWS DMS intégration	21
AWS DMS cas d'utilisation et étapes de haut niveau	21
AWS Glue intégration	23
AWS Glue cas d'utilisation et étapes de haut niveau	23
Intégration Amazon Redshift	26
Ressources	27
Historique de la documentation	28
Glossaire	29
#	29
A	30
B	33
C	35

D	38
E	43
F	45
G	47
H	48
I	50
L	52
M	54
O	58
P	61
Q	64
R	64
S	67
T	71
U	73
V	74
W	74
Z	75
.....	lxxvii

Intégration d'Amazon Aurora Postgre : SQL compatible avec les bases de données hétérogènes et Services AWS

Rambabu Karnena, Amazon Web Services (AWS)

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

Amazon Aurora Postgre SQL -Compatible Edition permet l'intégration à des bases de données hétérogènes et à divers services sur le cloud Amazon Web Services (AWS). Vous pouvez utiliser cette intégration pour créer des architectures de données évolutives AWS, ouvrant ainsi de nouvelles possibilités à vos applications.

Présentation

Ce guide fournit une présentation complète de l'intégration SQL compatible avec Aurora Postgre avec Services AWS des bases de données hétérogènes. Si vous utilisez actuellement Oracle Database ou Microsoft SQL Server, explorez les fonctionnalités SQL compatibles avec Aurora Postgre qui sont équivalentes aux serveurs liés, aux liens de base de données et aux tables externes. En utilisant ces instructions, vous pouvez également effectuer les tâches suivantes :

- Intégrez des services tels qu'Amazon Simple Storage Service (Amazon S3) AWS Lambda, Amazon Logs et CloudWatch Amazon Redshift.
- Évitez les erreurs de conception qui peuvent conduire à des erreurs ou des problèmes de performance.
- Prenez des décisions éclairées lors de l'intégration d'Aurora Postgre SQL -Compatible avec d'autres bases de données et Services AWS

Connexion à des bases de données distantes et hétérogènes

L'un des principaux atouts d'Aurora Postgre SQL -Compatible est sa capacité à se connecter à des SQL bases de données distantes [Postgre SQL](#), [SQLServer](#) et Oracle, My en utilisant des enveloppeurs de données étrangers (FDWs). Ces enveloppes incluent `postgres_fdw`, `oracle_fdw`, `tds_fdw` (pour le SQL serveur) et `mysql_fdw`. Vous pouvez utiliser ces enveloppeurs de données étrangères pour interroger directement les données provenant de ces sources multiples.

Journalisation

Aurora PostgreSQL -Compatible s'intègre également à [Amazon CloudWatch Logs](#) à l'aide de l'`log_fdw` extension. Vous pouvez l'utiliser `log_fdw` pour interroger et analyser les fichiers SQL journaux PostgreSQL directement depuis la base de données. Cette intégration rationalise la surveillance et l'analyse des journaux afin que vous puissiez obtenir des informations précieuses sur les performances, les erreurs et les activités de votre base de données.

Se connecter au stockage

L'`aws_s3` extension s'intègre à [Amazon S3](#) pour les importations, les exportations, les sauvegardes et l'archivage de données. En prenant en charge le mouvement des données entre Aurora PostgreSQL -Compatible et Amazon S3, l'`aws_s3` extension permet des processus efficaces d'ingestion, de sauvegarde et d'archivage des données.

Calcul sans serveur

Vous pouvez utiliser l'`aws_lambda` extension pour améliorer les performances et la rentabilité en transférant les tâches gourmandes en ressources informatiques vers des fonctions sans serveur. [AWS Lambda](#) prend en charge les calculs complexes, les transformations de données et les intégrations avec d'autres AWS services directement à partir de votre base de données SQL compatible Aurora PostgreSQL, sans avoir besoin de ressources informatiques dédiées.

Intégrations pour l'analyse

Pour faciliter la migration des données et les processus ETL (d'extraction, de transformation et de chargement), Aurora PostgreSQL -Compatible peut s'intégrer à des services tels que [AWS Database Migration Service \(AWS DMS\)](#) et AWS Glue. AWS DMS prend en charge la migration des bases de données vers Aurora PostgreSQL -Compatible. [AWS Glue](#) vous aide à créer des pipelines de traitement de données robustes pour transformer et charger des données provenant de diverses sources vers Aurora PostgreSQL -Compatible ou autre. Services AWS

[Pour une solution d'entreposage de données, Aurora PostgreSQL -Compatible peut s'intégrer à Amazon Redshift.](#) En faisant office de source de données ou de zone intermédiaire pour Amazon Redshift, Aurora PostgreSQL -Compatible prend en charge des fonctionnalités avancées d'analyse et de reporting. Vous pouvez utiliser ces fonctionnalités pour obtenir des informations précieuses à partir de vos données.

Que vous migriez des charges de travail existantes, créez des architectures hybrides ou développez de nouvelles applications pilotées par les données, les fonctionnalités d'intégration d'Aurora PostgreSQL -Compatible vous aident à créer des solutions évolutives, performantes et économiques.

Extensions supplémentaires pour l'intégration avec Services AWS

Postgre SQL répertorie différents enveloppeurs de données pour la connexion à des fichiers, aucune base de données, systèmes SQL de base de données spécifiques. Pour plus d'informations, consultez la [SQLdocumentation Postgre](#).

Objectifs

Ce guide aide les nouveaux clients, en particulier ceux qui migrent depuis Oracle ou Microsoft SQL Server, à atteindre les objectifs suivants :

- Trouvez des fonctionnalités équivalentes sur AWS. Aurora Postgre SQL -Compatible fournit des équivalents fonctionnels aux serveurs liés, aux liens de base de données et aux tables externes.
- Concevez des systèmes et des tâches par lots qui s'intègrent et se connectent à des bases de données hétérogènes et Services AWS.
- Évitez les écueils de conception courants et optimisez les mises en œuvre de l'infrastructure.

Prérequis

Pour suivre ce guide, assurez-vous d'avoir accès aux éléments suivants :

- Un actif Compte AWS
- Un cluster Amazon Aurora Postgre SQL -Compatible Edition (pour les instructions, voir [Création d'un cluster de SQL base de données Aurora Postgre.](#))
- Amazon Simple Storage Service (Amazon S3)
- Amazon CloudWatch Logs
- AWS Lambda
- AWS Glue
- AWS Database Migration Service (AWS DMS)
- Une instance Amazon Elastic Compute Cloud (AmazonEC2) avec des SQL bases de données SQL Server, Oracle et Postgre installées

L'instance SQL compatible Aurora Postgre et les autres bases de données Services AWS doivent se trouver dans le même cloud privé virtuel (VPC) ou une connectivité réseau doit être établie entre elles. En outre, vous devez disposer des rôles et des privilèges de sécurité requis.

Intégration de base de données compatible avec Aurora PostgreSQL

Pour créer des connexions entre les bases de données PostgreSQL et les bases de données distantes, vous pouvez utiliser des enveloppeurs de données étrangers (FDWs). Les enveloppeurs de données étrangères offrent les avantages suivants par rapport aux serveurs liés à SQL Server et aux liens de base de données Oracle :

- Intégration native à PostgreSQL FDWs – est native de PostgreSQL et utilise ses fonctionnalités SQL. Cela améliore l'expérience d'intégration.
- Intégration et optimisation – Les serveurs liés (SQL Server) et les liens de base de données (Oracle) sont spécifiques à leurs écosystèmes de base de données respectifs. En prenant en charge les requêtes vers des sources de données distantes et via des moteurs de base de données tels qu'Oracle, SQL Server, MySQL, FDWs offrez une approche plus intégrée et optimisée pour PostgreSQL.
- Interrogation entre bases de données – Lorsque vous utilisez FDWs, vous pouvez interroger des données provenant de plusieurs sources de données distantes au moyen d'une seule instruction SQL. Cela prend en charge les analyses et les rapports entre bases de données.
- L'optimisation push down – FDWs peut transférer des opérations telles que le filtrage, les projections et le tri vers la source de données distante. Cela réduit le transfert de données et améliore les performances des requêtes.
- Exécutions parallèles – Les wrappers de données étrangers prennent en charge l'exécution de requêtes impliquant des sources de données distantes en parallèle, ce qui améliore les performances.

En utilisant l'intégration d'un wrapper de données étranger, vous pouvez interroger et manipuler des données à partir de bases de données distantes directement dans Amazon Aurora PostgreSQL Compatible Edition. Cela prend en charge les architectures hybrides et les scénarios d'intégration de données.

Ce guide se concentre sur `postgres_fdw` extension pour la connexion aux bases de données PostgreSQL distantes et sur `tds_fdw` l'extension pour la connexion aux bases de données SQL Server. Les extensions PostgreSQL suivantes ne sont pas abordées dans ce guide :

- `oracle_fdw` pour accéder aux données des bases de données Oracle

- `mysql_fdw` pour accéder aux données des bases de données MySQL

Intégration compatible avec Aurora PostgreSQL avec les bases de données PostgreSQL distantes

Cette section décrit l'intégration d'Amazon Aurora PostgreSQL Compatible Edition aux bases de données PostgreSQL distantes à l'aide de l'extension `postgres_fdw` (enveloppe de données étrangères) ou de la fonctionnalité `dblink`. Le `postgres_fdw` module fournit une fonctionnalité de requête fédérée pour interagir avec des bases de données distantes basées sur PostgreSQL. Les bases de données distantes peuvent être gérées ou autogérées sur [Amazon EC2](#) ou sur site. L'extension `postgres_fdw` est disponible dans toutes les versions actuellement prises en charge d'Amazon Relational Database Service (Amazon RDS) pour PostgreSQL et compatible avec Aurora PostgreSQL.

Grâce à cette `postgres_fdw` extension, vous pouvez accéder aux données des bases de données PostgreSQL distantes et les interroger comme s'il s'agissait de tables locales. L'extension `postgres_fdw` prend également en charge les éléments suivants :

- Compatibilité entre versions pour accéder aux données à partir de serveurs PostgreSQL externes exécutant différentes versions.
- Gestion des transactions, qui permet de garantir la cohérence et l'intégrité des données lorsque vous effectuez des opérations sur des serveurs PostgreSQL locaux et externes.
- Les transactions distribuées, qui fournissent des garanties d'atomicité (propriété des transactions ACID) et d'isolation lorsque vous effectuez des opérations sur plusieurs serveurs PostgreSQL externes. Cela permet de garantir que toutes les opérations d'une transaction sont validées ou qu'aucune n'est validée, préservant ainsi la cohérence et l'intégrité des données.

Bien que le `dblink` module permette d'interagir avec des bases de données PostgreSQL distantes, il ne prend pas en charge les transactions distribuées ni les autres fonctionnalités avancées. Si vous avez besoin de fonctionnalités plus avancées, pensez plutôt à utiliser l'extension `postgres_fdw`. L'extension `postgres_fdw` fournit davantage de fonctionnalités d'intégration et d'optimisation.

Cas d'utilisation de `postgres_fdw` et étapes de haut niveau

L'utilisation de l'extension `postgres_fdw` compatible avec Aurora PostgreSQL prend en charge les cas d'utilisation et les scénarios suivants :

- Requêtes fédérées et intégration de données – Interrogation et combinaison de données provenant de plusieurs bases de données PostgreSQL au sein d'une seule instance compatible avec Aurora PostgreSQL
- Déchargement des charges de travail de lecture – Connexion aux répliques en lecture de serveurs PostgreSQL externes, déchargement des charges de travail lourdes en lecture et amélioration des performances des requêtes
- Opérations entre bases de données – Exécution INSERT, UPDATE DELETE, et COPY opérations sur plusieurs bases de données PostgreSQL, permettant la manipulation des données et les tâches de maintenance entre bases de données

Pour configurer `postgres_fdw`, suivez les étapes de haut niveau suivantes :

1. Connectez-vous à votre cluster compatible Aurora PostgreSQL à l'aide d'un client PostgreSQL et créez l'extension : `postgres_fdw`

```
CREATE EXTENSION postgres_fdw;
```

Cette extension fournit les fonctionnalités permettant de se connecter à des bases de données PostgreSQL distantes.

2. Créez un serveur étranger nommé à `my_fdw_target` l'aide de la `CREATE SERVER` commande. Ce serveur représente la base de données PostgreSQL distante à laquelle vous souhaitez vous connecter. Spécifiez le nom de la base de données, le nom d'hôte et le mode SSL comme options pour ce serveur.
3. Assurez-vous que les groupes de sécurité et les configurations réseau nécessaires sont en place pour permettre à Aurora PostgreSQL compatible de se connecter à la base de données PostgreSQL distante.

Si la base de données distante est hébergée sur site, vous devrez peut-être configurer un réseau privé virtuel (VPN) ou une AWS Direct Connect connexion.

Exécutez la commande suivante :

```
CREATE SERVER my_fdw_target Foreign Data Wrapper postgres_fdw OPTIONS (DBNAME 'postgres', HOST 'SOURCE_HOSTNAME', SSLMODE 'require');
```

4. Créez un mappage utilisateur pour l'`dbuserutilisateur` sur le `my_fdw_target` serveur. Ce mappage associe l'`dbuserutilisateur` et le mot de passe de l'instance locale compatible Aurora PostgreSQL à l'utilisateur correspondant sur la base de données distante.

```
CREATE USER MAPPING FOR dbuser SERVER my_fdw_target OPTIONS (user 'DBUSER', password 'PASSWORD');
```

Cette étape est nécessaire pour authentifier et fournir un accès à la base de données distante.

5. Créez une table étrangère nommée `customer_fdw` avec le mappage de `my_fdw_target` serveurs et d'utilisateurs que vous avez configuré précédemment :

```
CREATE FOREIGN TABLE customer_fdw( id int, name varchar, emailid varchar, projectname varchar, contactnumber bigint) server my_fdw_target OPTIONS( TABLE_NAME 'customers');
```

La `customer_fdw` table est mappée à la `customers` table de la base de données distante spécifiée par le `my_fdw_target` serveur. La table étrangère possède la même structure que la table distante, de sorte que vous pouvez interagir avec les données distantes comme s'il s'agissait d'une table locale.

6. Vous pouvez effectuer diverses opérations de manipulation de données sur la table `customer_fdw` étrangère, telles que `INSERTUPDATE`, et des `SELECT` requêtes. Le script montre comment insérer une nouvelle ligne et mettre à jour une ligne existante, supprimer un enregistrement et tronquer une table de la table distante via la `customers customer_fdw` table étrangère :

```
INSERT INTO customer_fdw values ( 1, 'Test1', 'Test1@email.com', 'LMS1', '888888888');
INSERT INTO customer_fdw values ( 2, 'Test2', 'Test2@email.com', 'LMS2', '999999999');
INSERT INTO customer_fdw values ( 3, 'Test3', 'Test3@email.com', 'LMS3', '111111111');
UPDATE customer_fdw set contactnumber = '123456789' where id = 2;
DELETE FROM customer_fdw where id = 1;
TRUNCATE TABLE customer_fdw;
```

7. Vous pouvez valider un plan de requête SQL en utilisant l'`EXPLAIN` instruction pour analyser le plan de requête pour une `SELECT` requête sur la `customer_fdw` table :

```
EXPLAIN select * from customer_fdw where id =1;
```

Cela peut vous aider à comprendre comment la requête est exécutée et comment l'optimiser. Pour plus d'informations sur l'utilisation de EXPLAIN cette instruction, consultez la section [Optimisation des performances AWS des requêtes PostgreSQL dans Prescriptive Guidance](#).

8. Pour importer plusieurs tables de la base de données distante dans un schéma local, utilisez la `IMPORT FOREIGN SCHEMA` commande :

```
CREATE SCHEMA public_fdw;  
IMPORT FOREIGN SCHEMA public LIMIT TO (employees, departments)  
FROM SERVER my_fdw_target INTO public_fdw;
```

Cela crée des tables étrangères locales pour les tables spécifiées dans le `public_fdw` schéma. Dans cet exemple, les tables spécifiques sont les employés et les départements.

9. Pour accorder les autorisations nécessaires à un utilisateur de base de données spécifique afin qu'il puisse accéder au FDW et au serveur étranger associé et les utiliser, exécutez les commandes suivantes :

```
GRANT USAGE ON FOREIGN SERVER my_fdw_target TO targetdbuser;  
GRANT USAGE ON FOREIGN DATA WRAPPER postgres_fdw TO targetdbuser;
```

Cette étape peut être utile lorsque plusieurs utilisateurs ont besoin d'accéder aux tables étrangères facilitées par le wrapper de données étranger.

Lorsque vous utilisez des tables étrangères, tenez compte des limites suivantes :

- L'accès aux données depuis une source distante peut entraîner des coûts de transfert de données et une surcharge de performance en raison de la latence du réseau. Les problèmes de performances peuvent être perceptibles pour les ensembles de données volumineux ou les requêtes qui nécessitent un transfert de données important entre l'instance compatible Aurora PostgreSQL et la source de données distante.
- Dans les requêtes complexes impliquant des fonctionnalités telles que les fonctions de fenêtre, les requêtes récursives peuvent ne pas fonctionner comme prévu ou ne pas être prises en charge.

- Le chiffrement des mots de passe n'est actuellement pas pris en charge. Mettez en œuvre des contrôles pour garantir que seuls les utilisateurs autorisés peuvent accéder aux données des bases de données distantes FDWs et les récupérer.
- Les contraintes de clé primaire ne peuvent pas être définies sur les tables étrangères, comme le montre la tentative de script de création de table suivante :

```
CREATE FOREIGN TABLE customer_fdw2( id int primary key, name varchar, emailid
  varchar, projectname varchar, contactnumber bigint) server my_fdw_target
  OPTIONS( TABLE_NAME 'customers');
Primary keys cannot be defined on Foreign table
```

- La ON CONFLICT clause pour les INSERT instructions n'est pas prise en charge sur les tables étrangères, comme le montre l'exemple suivant :

```
INSERT INTO customer_fdw (id, name, emailid, projectname, contactnumber) VALUES
(1, 'test1', 'test@email.com', 'LMS', 11111111 ),
(3, 'test3', 'test3@email.com', 'LMS', 22222222 )
ON CONFLICT (id) DO UPDATE
SET name = EXCLUDED.name;
On Conflict option doesnot work.
```

Nettoyage

Pour nettoyer les objets créés, notamment en supprimant l'`postgres_fdw` extension, le `my_fdw_target` serveur, les mappages d'utilisateurs et les tables étrangères, exécutez les commandes suivantes :

```
DROP FOREIGN TABLE customer_fdw;
DROP USER MAPPING for postgres;
DROP SERVER my_fdw_target;
DROP EXTENSION postgres_fdw cascade;
```

Utiliser dblink pour créer des connexions

Les fonctions du `dblink` module offrent un autre moyen de créer des connexions et d'exécuter des instructions SQL sur des bases de données PostgreSQL distantes. La `dblink` solution est un moyen plus simple et plus flexible d'exécuter des requêtes ou des opérations ponctuelles sur des bases de données distantes. Pour les scénarios plus complexes impliquant une intégration de données

à grande échelle, une optimisation des performances et des exigences en matière d'intégrité des données, nous vous recommandons d'utiliser `postgres_fdw`.

L'utilisation `dblink` implique les étapes de haut niveau suivantes :

1. Créez l'extension `dblink` :

```
CREATE EXTENSION dblink;
```

Cette extension fournit les fonctionnalités permettant de se connecter à des bases de données PostgreSQL distantes.

2. Pour établir une connexion à une base de données PostgreSQL distante, utilisez la fonction : `dblink_connect`

```
SELECT dblink_connect('myconn', 'dbname=postgres port=5432 host=SOURCE_HOSTNAME  
user=postgres password=postgres');
```

3. Après vous être connecté à la base de données PostgreSQL distante, exécutez des instructions SQL sur la base de données distante à l'aide des fonctions suivantes : `dblink`

```
SELECT FROM dblink('myconn', 'SELECT col1, col2 FROM remote_table') AS  
remote_data(col1 int, col2 text);
```

Cette requête exécute l'`SELECT * FROM remote_table` instruction sur la base de données distante à l'aide de la `myconn` connexion. La requête extrait les résultats dans une table temporaire locale avec les colonnes `col1` et `col2`.

4. Vous pouvez également exécuter des instructions autres que des requêtes, telles que `INSERT`, ou `UPDATE` `DELETE`, sur la base de données distante à l'aide de la `dblink_exec` fonction :

```
SELECT dblink_exec('myconn', 'INSERT INTO remote_table VALUES (1, 'value')');
```

Intégration compatible avec Aurora PostgreSQL avec des bases de données hétérogènes

Pour intégrer la compatibilité Aurora PostgreSQL aux bases de données SQL Server distantes, utilisez l'extension Tabular Data Stream foreign data wrapper (`tds_fdw`) [En utilisant cette](#)

[tds_fdw extension](#), vous pouvez implémenter une fonctionnalité de requête fédérée pour interagir avec n'importe quelle base de données distante basée sur SQL Server, à la fois sur site et gérée ou autogérée sur Amazon. EC2 L'`tds_fdw` extension est disponible dans toutes les versions actuellement prises en charge d'Amazon RDS pour PostgreSQL et compatible avec Aurora PostgreSQL.

Cas d'utilisation de `tds_fdw` et étapes de haut niveau

L'intégration de la compatibilité Aurora PostgreSQL à des bases de données hétérogènes telles que SQL Server prend en charge les cas d'utilisation suivants :

- Architectures hybrides – Votre organisation possède peut-être des bases de données SQL Server existantes qui doivent coexister et s'intégrer avec Aurora PostgreSQL compatible. Dans de tels cas, la compatibilité avec Aurora PostgreSQL peut faire partie d'une architecture hybride, dans laquelle elle interagit avec les bases de données hétérogènes pour échanger des données ou effectuer des opérations spécifiques. Grâce à cette intégration, votre organisation peut tirer parti des points forts des différentes plateformes de base de données tout en conservant ses investissements existants.
- Rapports et analyses – Vous pouvez utiliser la version compatible avec Aurora PostgreSQL comme base de données de rapports ou d'analyses. Vous pouvez consolider les données provenant de plusieurs sources, notamment les bases de données Oracle et SQL Server. Ce cas d'utilisation est courant dans les scénarios où les entreprises souhaitent créer des bases de données de reporting spécialisées ou des data marts adaptés à des unités commerciales ou à des cas d'utilisation spécifiques.

Pour configurer l'`tds_fdw` extension de manière compatible avec Aurora PostgreSQL, suivez les étapes de haut niveau suivantes :

1. Connectez-vous à votre cluster compatible Aurora PostgreSQL à l'aide d'un client PostgreSQL et créez l'extension : `tds_fdw`

```
CREATE EXTENSION tds_fdw;
```

Cette extension fournit les fonctionnalités permettant d'accéder aux données des bases de données SQL Server distantes et de les interroger comme s'il s'agissait de tables locales.

2. Créez un objet serveur qui représente la base de données distante compatible avec SQL Server ou TDS à laquelle vous souhaitez vous connecter.

3. Assurez-vous que les groupes de sécurité et les configurations réseau nécessaires sont en place pour permettre à Aurora PostgreSQL compatible de se connecter à la base de données SQL Server distante.

Si la base de données distante est hébergée sur site, vous devrez peut-être configurer un VPN ou une AWS Direct Connect connexion.

Exécutez la commande suivante :

```
CREATE SERVER my_remote_sql_server
  FOREIGN DATA WRAPPER tds_fdw
  OPTIONS (
    servername 'your_server_name',
    port '1433',
    instance 'your_instance_name'
  );
```

4. Définissez un mappage utilisateur qui mappe un utilisateur compatible Aurora PostgreSQL à un utilisateur de la base de données distante compatible avec SQL Server ou TDS :

```
CREATE USER MAPPING FOR postgres
  SERVER my_remote_sql_server
  OPTIONS (
    username 'your_sql_server_username',
    password 'your_sql_server_password'
  );
```

5. Créez une table étrangère qui représente une table ou une vue dans la base de données distante compatible avec SQL Server ou TDS :

```
CREATE FOREIGN TABLE sql_server_table (
  column1 INTEGER,
  column2 VARCHAR(50)
) SERVER my_remote_sql_server
  OPTIONS (
    schema_name 'your_schema_name',
    table_name 'your_table_name'
  );
```

6. Créez une table étrangère en fonction de la requête SQL :

```
CREATE FOREIGN TABLE mssql_people ( empno INT NOT NULL , ename VARCHAR(10) NULL, dept INT) SERVER my_remote_sql_server OPTIONS ( query 'SELECT empno, ename, dept FROM dbo.emp');
```

7. Interrogez la table étrangère comme vous le feriez pour n'importe quelle autre table compatible avec Aurora PostgreSQL :

```
SELECT * FROM sql_server_table;  
SELECT * FROM mssql_people; -- Query based on table
```

8. Importez la table de SQL Server vers PostgreSQL :

```
IMPORT FOREIGN SCHEMA dbo LIMIT TO (emp) FROM SERVER  
my_remote_sql_server INTO public_fdw;
```

9. Pour valider le plan de requête, exécutez EXPLAIN SELECT :

```
EXPLAIN SELECT * FROM mssql_people;
```

Note

Les opérations du langage DML (Data Manipulation Language) ne sont pas disponibles via l'extension `tds_fdw`. Le système ne prend pas en charge les opérations DML sur différents moteurs de base de données. `INSERT`, `DELETE`, `UPDATE`, et `TRUNCATE TABLE` échouera sur le serveur SQL distant.

Aurora Postgre SQL - Intégration compatible avec Logs CloudWatch

Amazon CloudWatch Logs est un service de gestion des journaux permettant de collecter, de surveiller et d'analyser les journaux de différents types. Services AWS Vous pouvez diffuser les journaux Amazon Aurora Postgre SQL -Compatible Edition, notamment les journaux d'erreurs, les journaux de requêtes lentes et les journaux d'audit, vers Logs. CloudWatch Vous pouvez centraliser et surveiller les journaux de votre base de données en temps réel, ce qui facilite l'identification et le dépannage des problèmes.

Vous pouvez surveiller les journaux en utilisant AWS Management Console ou vous pouvez interroger les journaux à l'aide de l'`log_fdw` extension. L'`log_fdw` extension permet d'interroger et d'analyser les fichiers SQL journaux Postgre directement depuis la base de données. Cela vous permet de mieux comprendre les performances de la base de données, de résoudre les problèmes et d'identifier de manière proactive les problèmes potentiels.

Pour configurer `log_fdw` l'intégration avec CloudWatch Logs, suivez les étapes de haut niveau suivantes :

1. Connectez-vous à votre cluster SQL compatible Aurora Postgre à l'aide d'un SQL client Postgre et créez l'extension : `log_fdw`

```
CREATE EXTENSION log_fdw;
```

Cette extension fournit les fonctionnalités permettant de se connecter à CloudWatch Logs.

2. Créez un serveur de journaux nommé `log_server` qui pointe vers le répertoire dans lequel les fichiers SQL journaux Postgre sont stockés. L'emplacement par défaut des fichiers journaux SQL compatibles avec Aurora Postgre est le suivant : `/rdsdbdata/log/`

```
CREATE SERVER log_server FOREIGN DATA WRAPPER log_fdw OPTIONS (log_directory '/rdsdbdata/log/');
```

[Pour plus d'informations sur la publication de fichiers journaux depuis Aurora Postgre SQL - Compatible to CloudWatch Logs, consultez la AWS documentation.](#)

3. Pour répertorier tous les fichiers journaux accessibles via l'`log_fdw` extension, exécutez la requête suivante :

```
SELECT * FROM log_file_list('log_server');
```

4. Pour créer une table `log_table` étrangère mappée vers le `postgres.log` fichier, exécutez la commande suivante :

```
SELECT create_foreign_table_for_log_file('log_table', 'log_server', 'postgres.log');
```

Les colonnes du tableau correspondent aux champs présents dans le format de fichier SQL journal Postgre.

5. Vous pouvez désormais interroger les données du journal comme s'il s'agissait d'une table normale, en filtrant et en analysant les entrées du journal en fonction de vos besoins :

```
SELECT * FROM log_table
```

Nettoyage

Pour nettoyer les objets créés, notamment en supprimant l'`log_fdwextension`, le serveur et les tables étrangères, exécutez les commandes suivantes :

```
DROP FOREIGN TABLE log_table;  
DROP SERVER log_server;  
DROP EXTENSION log_fdw;
```

Aurora Postgre SQL - Intégration compatible avec Amazon S3

Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une évolutivité, une évolutivité, une disponibilité des données, une sécurité et des performances de pointe. Amazon Aurora Postgre SQL -Compatible Edition s'intègre à Amazon S3 via l'`aws_s3extension`, qui fournit un accès direct en lecture et en écriture aux compartiments S3. Cette intégration facilite l'échange de données, notamment l'ingestion de données, les sauvegardes et les autres opérations liées aux données.

Cas d'utilisation de `aws_s3` et étapes de haut niveau

Les cas d'utilisation de haut niveau les plus courants et les avantages de l'intégration à Amazon S3 sont les suivants :

- Ingestion de données depuis Amazon S3 – Utilisez l'`aws_s3extension` pour charger des données à partir de valeurs séparées par des virgules (CSV) ou d'autres formats de fichiers stockés dans Amazon S3 directement dans une table compatible avec Aurora PostgreSQL. JSON Cela est particulièrement utile pour les processus d'ingestion de données par lots, les flux de travail ETL (extraction, transformation et chargement) ou les migrations de données.
- Exportation de données vers Amazon S3 – Exportez des données depuis des tables SQL compatibles avec Aurora Postgre vers CSV ou vers d'autres formats de fichier, et stockez les données dans Amazon S3. JSON Cela est utile pour l'archivage des données, les sauvegardes ou le partage de données avec d'autres systèmes ou services.
- Interrogation de données directement depuis Amazon S3 – Interrogez des données stockées CSV ou JSON des fichiers dans Amazon S3 directement depuis votre base de données SQL compatible Aurora Postgre sans charger les données dans des tables. Cela est utile pour l'analyse ponctuelle des données ou pour le traitement exploratoire des données.
- Sauvegarde et restauration – Utilisez Amazon S3 comme destination de sauvegarde pour vos bases de données SQL compatibles Aurora Postgre. Cela fournit une couche supplémentaire de protection des données et vous pouvez restaurer des bases de données à partir des sauvegardes Amazon S3 si nécessaire.

Pour intégrer votre cluster de base de données SQL compatible Aurora Postgre à un compartiment S3, suivez les étapes de haut niveau suivantes :

1. Connectez-vous à votre cluster SQL compatible Aurora Postgre à l'aide d'un SQL client Postgre et créez l'extension : `aws_s3`

```
create extension aws_s3
```

2. Configurez l'accès à un compartiment S3 en utilisant un rôle IAM Pour connaître les étapes détaillées, consultez la [AWS documentation](#).

3. Utilisez une requête PSQL pour importer ou exporter les données de la base de données :

- Pour importer le fichier depuis Amazon S3 vers une table SQL compatible Aurora Postgre, exécutez les commandes suivantes :

```
SELECT aws_s3.table_import_from_s3( 'Table_Name', '', '(format text)',  
  
aws_commons.create_s3_uri('S3_BUCKETNAME', 'FileName.dat', 'Region-Name') );
```

- Pour exporter le fichier vers Amazon S3 depuis la table Aurora Postgre SQL -Compatible, exécutez la commande suivante :

```
SELECT * FROM aws_s3.query_export_to_s3('TABLE_NAME',  
aws_commons.create_s3_uri('S3_BUCKETNAME', 'FileName.dat', 'Region-Name') );
```

- Pour exporter vers Amazon S3 à l'aide d'une SQL requête, exécutez la commande suivante :

```
SELECT * FROM aws_s3.query_export_to_s3('SELECT * FROM data_table',  
aws_commons.create_s3_uri('S3_BUCKETNAME', 'FileName.dat', 'Region-Name') );
```

Aurora Postgre SQL - Intégration compatible avec Lambda

AWS Lambda est un service informatique sans serveur permettant d'exécuter du code sans demander la mise en service ou la gestion des serveurs. En intégrant Lambda à Amazon Aurora PostgreSQL -Compatible Edition, vous pouvez créer des architectures pilotées par les événements et étendre les fonctionnalités de votre base de données compatible Aurora PostgreSQL.

Cas d'utilisation Lambda

Les cas d'utilisation courante d'Aurora PostgreSQL -Compatible avec Lambda sont notamment les suivants :

- **Traitement et transformation des données** – Déchargez les tâches complexes de traitement des données des fonctions Aurora PostgreSQL -Compatible vers les fonctions Lambda. Les scénarios peuvent être le nettoyage des données, l'enrichissement des données, la validation des données et des calculs complexes.
- **Flux de travail pilotés par les événements** – Utilisez les fonctions Lambda pour déclencher des actions ou des flux de travail en fonction d'événements ou de modifications dans Aurora PostgreSQL -Compatible. SQL Les scénarios incluent l'envoi de notifications, le déclenchement de ETL processus ou l'appel d'autres processus Services AWS lorsque des données sont insérées, mises à jour ou supprimées dans Aurora PostgreSQL -CompatibleSQL.
- **Analyses et rapports en temps réel** – Utilisez les fonctions Lambda pour effectuer des analyses en temps réel ou générer des rapports basés sur les données stockées dans Aurora SQL PostgreSQL -Compatible. Les fonctions Lambda peuvent interroger Aurora PostgreSQL -Compatible, traiter les données et générer des rapports ou des visualisations à la demande ou selon un calendrier.
- **Sans serveur APIs et microservices** – Utilisez les fonctions Lambda pour créer des microservices sans serveur APIs ou des microservices qui interagissent avec Aurora PostgreSQL -Compatible. SQL Les fonctions Lambda peuvent gérer les API demandes, interroger ou modifier des données dans Aurora PostgreSQL -Compatible, et renvoyer la réponse.
- **Traitement asynchrone** – Déchargez les tâches asynchrones ou de longue durée des fonctions Aurora SQL PostgreSQL -Compatible vers les fonctions Lambda. Les scénarios incluent l'envoi de messages électroniques, la génération de rapports ou le traitement de grands ensembles de données sans bloquer l'application ou la base de données principale. Les tâches de longue durée doivent respecter le délai Lambda de 15 minutes.

[Pour configurer l'intégration entre Aurora Postgre SQL -Compatible et Lambda, suivez les instructions de la documentation.AWS](#)

Aurora Postgre SQL - Intégration compatible avec AWS DMS

AWS Database Migration Service (AWS DMS) vous aide à migrer des bases de données relationnelles, des entrepôts de données, des SQL bases de données sans base de données et d'autres magasins de données entre différents moteurs. AWS DMS prend en charge les migrations homogènes (par exemple, Postgre SQL vers PostgreSQL) et les migrations hétérogènes (par exemple, Oracle, SQL Server ou My vers Amazon SQL Aurora Postgre SQL -Compatible Edition).

En intégrant Aurora Postgre SQL -Compatible avec AWS DMS, vous minimisez les temps d'arrêt. AWS DMS contribue également à garantir la cohérence des données lors de la migration depuis un environnement sur site ou d'autres environnements cloud vers Aurora Postgre -CompatibleSQL. En outre, il AWS DMS prend en charge différents moteurs de base de données source et cible, offrant ainsi une flexibilité lors de la migration des charges de travail vers Aurora SQL Postgre -Compatible.

AWS DMS cas d'utilisation et étapes de haut niveau

AWS DMS l'intégration avec Aurora Postgre SQL -Compatible prend en charge les cas d'utilisation suivants :

- Migration depuis des bases de données locales – AWS DMS À utiliser pour migrer des bases de données locales existantes (par exemple, Oracle, SQL ServerSQL, My ou Postgre) SQL vers Aurora Postgre -Compatible. SQL
- Migration depuis d'autres bases de données cloud – AWS DMS À utiliser pour faciliter la migration de bases de données hébergées sur d'autres moteurs ou plateformes cloud (par exemple, AmazonRDS, Azure SQL Database ou Google CloudSQL) vers Aurora Postgre SQL -Compatible.
- Migration entre clusters SQL compatibles Aurora Postgre – AWS DMS À utiliser pour migrer des données entre des clusters SQL compatibles Aurora Postgre, au sein d'une même Région AWS région ou entre différentes régions.
- Réplication continue des données et CDC – À utiliser AWS DMS pour la réplication continue des données et modifier la capture des données (CDC) d'une base de données source vers une base de données SQL compatible avec Aurora Postgre. Cela est utile pour gérer une réplique en direct ou un entrepôt de données à des fins d'analyse.

Pour effectuer la configuration AWS DMS, appliquez la procédure suivante :

1. Configurez l'instance de AWS DMS réplication dans Région AWS celle que vous souhaitez utiliser.
2. Créez un point de terminaison source dans AWS DMS, en spécifiant les détails de la base de données depuis laquelle vous souhaitez migrer des données.
3. Créez un point de terminaison cible dans AWS DMS, en spécifiant les détails de votre cluster SQL compatible Aurora Postgre.
4. Configurez la tâche de migration dans AWS DMS, en spécifiant les points de terminaison source et cible ainsi que le type de migration. Le type peut être le chargement complet, la capture des données modifiées (CDC) ou les deux. Spécifiez les règles de mappage ou les transformations nécessaires.
5. Démarrez la tâche de migration.

AWS DMS gérera le transfert et la réplication des données de la base de données source vers le cluster SQL compatible Aurora Postgre cible.

Pour obtenir des instructions détaillées, consultez la [AWS DMS documentation](#).

Aurora Postgre SQL - Intégration compatible avec AWS Glue

AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré pour préparer et charger des données à des fins d'analyse. Vous pouvez intégrer AWS Glue Amazon Aurora Postgre SQL -Compatible Edition pour tous les flux de travail de traitement et d'analyse des données.

AWS Glue cas d'utilisation et étapes de haut niveau

L'intégration d'Aurora Postgre SQL -Compatible with AWS Glue prend en charge les cas d'utilisation suivants :

- **Entreposage et analyse des données** – Utilisez AWS Glue l'intégration avec Aurora Postgre SQL -Compatible pour créer des solutions d'entreposage et d'analyse des données. AWS Glue peut extraire des données de bases de données SQL compatibles Aurora Postgre et les transformer selon vos besoins. AWS Glue Vous pouvez ensuite charger les données transformées dans un entrepôt de données tel qu'Amazon Redshift ou Amazon Athena pour des analyses et des rapports avancés.
- **Création d'un lac de données** – AWS Glue À utiliser pour extraire des données d'Aurora Postgre SQL -Compatible et les charger dans un lac de données stocké dans Amazon S3. Vous pouvez ensuite utiliser ce lac de données à diverses fins, telles que l'apprentissage automatique, l'exploration de données ou l'alimentation d'autres systèmes analytiques.
- **ETLpipelines** – Utilisez le ETL service AWS Glue sans serveur pour créer des pipelines de données robustes. Vous pouvez extraire des données depuis Aurora Postgre SQL -Compatible et effectuer des transformations complexes à l'aide d'Apache Spark ou. PySpark Vous pouvez charger les données traitées dans une cible telle qu'Amazon S3 ou Amazon Redshift, ou vous pouvez les charger à nouveau dans Aurora SQL Postgre -Compatible.
- **Catalogage des données et gestion des métadonnées** – AWS Glue Data Catalog À utiliser pour analyser et cataloguer automatiquement les métadonnées à partir de bases de données et de tables SQL compatibles Aurora Postgre. Services AWS tels qu'Amazon Athena et Amazon Redshift Spectrum peuvent utiliser ce référentiel de métadonnées centralisé pour interroger et analyser des données.

- Préparation des données pour l'apprentissage automatique – AWS Glue À utiliser pour préparer les données à partir d'Aurora PostgreSQL -Compatible pour les charges de travail d'apprentissage automatique (ML). Les données traitées peuvent être chargées dans Amazon SageMaker AI ou dans d'autres services de machine learning pour la formation et le déploiement de modèles.
- Migration et réplication des données – Bien que AWS Database Migration Service (AWS DMS) soit le service principal pour les migrations de bases de données, vous pouvez également l'utiliser AWS Glue. Migrez ou répliquez des données depuis Aurora PostgreSQL -Compatible vers d'autres magasins de données, tels qu'Amazon S3, Amazon Redshift ou même d'autres moteurs de base de données.

Votre entreprise peut tirer parti de la puissance des services d'intégration et d'analyse de AWS données grâce à l'évolutivité, aux performances et à la compatibilité d'Aurora PostgreSQL -CompatibleSQL. Grâce à ces cas d'utilisation, vous pouvez créer des pipelines de données robustes, effectuer des transformations de données complexes et les intégrer à d'autres Services AWS pour des analyses et des rapports avancés.

Pour intégrer Aurora PostgreSQL -Compatible avec AWS Glue, suivez les étapes de haut niveau suivantes :

1. Connectez-vous au AWS Management Console, accédez à la AWS Glue console et créez un AWS Glue Data Catalog.

Le catalogue de données est un référentiel central qui stocke les métadonnées relatives à vos sources de données, notamment les bases de données et les SQL tables compatibles Aurora PostgreSQL.

2. Créez une AWS Glue connexion.

Accédez à la page Connexions et créez une AWS Glue connexion. Sélectionnez Aurora PostgreSQL -Compatible comme type de connexion et fournissez le point de terminaison du cluster Aurora PostgreSQL -Compatible, le nom de la base de données, ainsi que le nom d'utilisateur et le mot de passe de votre base de données.

3. Explorez la source de données SQL compatible Aurora PostgreSQL.

Accédez à la section Crawlers et créez un robot configuré pour utiliser la connexion que vous avez créée. Spécifiez les noms de base de données et de tables que vous souhaitez analyser et inclure dans le catalogue de données, puis exécutez le robot d'exploration.

4. Créez et exécutez une AWS Glue ETL tâche.

Accédez à la section Tâches et créez une ETL tâche pour accéder aux données de la base de données SQL compatible Aurora Postgre et les interroger à l'aide du catalogue de données. Choisissez le type de poste en fonction de vos besoins. Dans le script de ETL tâche, effectuez les transformations ou traitements nécessaires et spécifiez l'emplacement cible des données traitées. L'emplacement cible peut être Amazon S3, Amazon Redshift ou une autre base de données compatible avec Aurora PostgreSQL.

Pour obtenir des instructions détaillées, consultez la [AWS Glue documentation](#).

Aurora Postgre SQL - Intégration compatible avec Amazon Redshift

Amazon Redshift est un service d'entrepôt de données entièrement géré dans le, doté d'une capacité de plusieurs péta-octets. L'intégration permet un transfert et une analyse efficaces des données entre Amazon Redshift et Amazon Aurora Postgre SQL -Compatible Edition.

AWS prend en charge l'ETL intégration nulle entre ces deux services. Zero- ETL for Aurora Postgre SQL -Compatible est actuellement disponible en version préliminaire publique. Pour en savoir plus, consultez la [documentation AWS](#).

Ressources

- [Enveloppeurs de données étrangers](#) (Postgre wikiSQL)
- [Support des requêtes fédérées pour Amazon Aurora Postgre et SQL Amazon RDS for Postgre SQL — Partie 1](#) (AWSarticle de blog)
- [Support des requêtes fédérées pour Amazon Aurora Postgre et SQL Amazon RDS for Postgre SQL — Partie 2](#) (AWSarticle de blog)
- [Intégration d'Amazon Aurora Postgre à SQL d'autres Services AWS](#)
- [Documentation Amazon CloudWatch Logs](#)
- [Documentation AWS DMS](#)
- [Documentation AWS Glue](#)
- [Documentation AWS Lambda](#)
- [Documentation Amazon S3](#)

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 [RSS](#)[fil RSS](#).

Modification	Description	Date
Publication initiale	—	22 août 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 sur site vers Oracle sur une instance EC2 dans le AWS Cloud
- **Relocaliser (lift and shift au niveau de l'hyperviseur)** : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers AWS.
- **Retenir** : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

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

A

ABAC

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

services abstraits

Consultez la section [Services gérés](#).

ACIDE

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

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir [intelligence artificielle](#).

AIOps

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

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

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

B

mauvais bot

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

BCP

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

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

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

planification de la continuité des activités (BCP)

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

C

CAF

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

déploiement de Canary

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

CCo E

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

CDC

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

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

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

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

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

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir [vision par ordinateur](#).

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

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

ensemble profond

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

deep learning

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

defense-in-depth

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

la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une 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

Voir [reprise après sinistre](#).

détection de dérive

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

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

DVSM

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

E

EDA

Voir [analyse exploratoire des données](#).

EDI

Voir échange [de données informatisé](#).

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

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

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environnement

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

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

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

épopée

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

ERP

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

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

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

branche de fonctionnalités

Voir [succursale](#).

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

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

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le [modèle de fondation](#).

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les [restrictions géographiques](#).

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez [la haute disponibilité](#).

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiques

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

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

politique basée sur l'identité

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

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

migration incrémentielle

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

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

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

VPC d'inspection

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

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

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir [Internet des objets](#).

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

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

ITSM

Voir [Gestion des services informatiques](#).

L

contrôle d'accès basé sur des étiquettes (LBAC)

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

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

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

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

principe de moindre privilège

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

lift and shift

Voir [7 Rs](#).

système de poids faible

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

LLM

Voir le [grand modèle de langage](#).

environnements inférieurs

Voir [environnement](#).

M

machine learning (ML)

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

branche principale

Voir [succursale](#).

malware

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

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir [Migration Acceleration Program](#).

mécanisme

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

compte membre

Tous, à l'exception 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 téléométrique en file d'attente de messages (MQTT)

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

microservice

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

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir [apprentissage automatique](#).

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

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

MQTT

Voir [Message Queuing Telemetry](#) Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

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

OAI

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

OCM

Voir [gestion du changement organisationnel](#).

migration hors ligne

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

OI

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

OLA

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

migration en ligne

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

OPC-UA

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

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir [technologie opérationnelle](#).

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les [informations personnelles identifiables](#).

manuel stratégique

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

PLC

Voir [contrôleur logique programmable](#).

PLM

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

policy

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

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

confidentialité dès la conception

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

zones hébergées privées

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

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir [environnement](#).

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

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

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

RAG

Voir [Retrieval Augmented Generation](#).

rançongiciel

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

Matrice RASCI

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

RCAC

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

réplica en lecture

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

réarchitecte

Voir [7 Rs](#).

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir [7 Rs](#).

Région

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

régression

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

réhéberger

Voir [7 Rs](#).

version

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

déplacer

Voir [7 Rs](#).

replateforme

Voir [7 Rs](#).

rachat

Voir [7 Rs](#).

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir [7 Rs](#).

se retirer

Voir [7 Rs](#).

Génération augmentée de récupération (RAG)

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

rotation

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

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

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

RPO

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

RTO

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

runbook

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

S

SAML 2.0

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

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

SCADA

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

SCP

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

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

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

SLI

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

SLO

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

split-and-seed modèle

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

SPOF

Voir [point de défaillance unique](#).

schéma en étoile

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

modèle de figuier étrangleur

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

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

tags

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

variable cible

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

liste de tâches

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

environnement de test

Voir [environnement](#).

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

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

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

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir [environnement](#).

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

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

VER

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

WQF

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

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité « jour zéro »

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

invite Zero-Shot

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

application zombie

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

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