Migration großer MySQL- oder MariaDB-Datenbanken mit mehreren Terabyte zu AWS

AWS Prescriptive Guidance

AWS Prescriptive Guidance: Migration großer MySQL- oder MariaDB-Datenbanken mit mehreren Terabyte zu AWS

Table of Contents

Einführung 1
Zielgruppe 2
Gezielte Geschäftsergebnisse 2
Migrationsoptionen 3
Percona XtraBackup 4
Vorteile 6
Einschränkungen 7
Best Practices 8
MyDumper 8
Vorteile 11
Einschränkungen 11
Best Practices 12
mysqldump und mysqlpump 12
Vorteile 15
Einschränkungen 15
Best Practices 16
Geteiltes Backup 16
Amazon S3 File Gateway 19
Vorteile 20
Einschränkungen 20
Bewährte Methoden 21
Best Practices 22
Ressourcen 24
Dokumentverlauf 26
Glossar 27
..... 27
A 28
B 31
C 33
D 37
E 41
F 44
G 46
H 47

I 48
L 51
M 52
O 57
P 60
Q 63
R 63
S 67
T 71
U 73
V 73
W 74
Z 75
..... lxxvi

Migration großer MySQL- oder MariaDB-Datenbanken mit mehreren Terabyte zu AWS

Babaiah Valluru und Ankur Bhanawat, Amazon Web Services ()AWS

November 2024 (Geschichte der Dokumente)

Viele Organisationen mit lokalen MySQL- und MariaDB-Datenbankservern sind daran interessiert, ihre Datenbank-Workloads auf die zu migrieren. AWS Cloud Viele entscheiden sich für Amazon Relational Database Service (Amazon RDS) für MariaDB, Amazon RDS for MySQL oder Amazon Aurora MySQL-Compatible Edition. Amazon RDS wurde entwickelt, um die Einrichtung, den Betrieb und die Skalierung relationaler Datenbanken in der Cloud zu vereinfachen. Amazon Aurora ist Teil von Amazon RDS und bietet integrierte Sicherheit, kontinuierliche Backups, serverloses Computing, bis zu 15 Read Replicas, automatisierte Replikation in mehreren Regionen und Integration mit anderen. AWS-Services

Obwohl die Migration zu einem dieser Systeme viele Vorteile bieten AWS-Services kann, ist die Datenbankmigration eine der zeitaufwändigsten und kritischsten Aufgaben, die Datenbankadministratoren ausführen müssen. Die Migration großer Datenbanken erfordert eine genaue Planung und Implementierung und die Sicherstellung, dass die Leistung der migrierten Workloads gleichwertig ist oder sogar verbessert wird. In diesem Handbuch können sich große Datenbanken auf eine einzelne Datenbank mit mehreren Terabyte oder auf viele große Datenbanken beziehen, die zusammen mehrere Terabyte an Daten ergeben. Die Auswahl der richtigen Migrationsdienste und -tools ist der Schlüssel zum Erfolg der Migration. Es gibt zwei gängige Ansätze für die Migration einer Datenbank: logische und physische. Weitere Informationen zu diesen Ansätzen finden Sie in der MySQL - und MariaDB-Dokumentation.

In diesem Handbuch werden verschiedene Open-Source-Tools oder Tools von Drittanbietern beschrieben, mit denen Sie große, lokale MySQL- und MariaDB-Datenbanken mit mehreren Terabyte zu Amazon RDS for MariaDB, Amazon RDS for MySQL oder Amazon Aurora MySQL-Compatible Edition migrieren können. Die in diesem Handbuch beschriebenen Optionen verwenden logische oder physische Migrationsansätze, und jede Option umfasst mehrere Ansätze für die Übertragung der großen Datenbanksicherungsdateien vom lokalen Rechenzentrum in die Cloud, wo Sie die Datenbank aus der Sicherungsdatei wiederherstellen können.

Zielgruppe

Dieses Handbuch richtet sich an Programmdatenbankadministratoren, Datenbankingenieure, Migrationsingenieure, Projektmanager und Betriebs- oder Infrastrukturmanager, die planen, ihre MySQL- oder MariaDB-Datenbanken auf die zu migrieren. AWS Cloud

Gezielte Geschäftsergebnisse

Das Ziel dieses Leitfadens ist es, Ihnen zu helfen:

- Wählen Sie einen Migrationsansatz für eine große Datenbank, der am besten zu Ihrem Anwendungsfall und Ihrer Umgebung passt.
- Vermeiden Sie Verzögerungen und finanzielle Verluste, die entstehen können, wenn die Migrationsstrategie fehlerhaft ist.
- Erfahren Sie mehr über die Vor- und Nachteile der einzelnen Migrationsoptionen.
- Erfahren Sie mehr über verschiedene Ansätze, mit denen Sie große Datenbanksicherungsdateien von Ihrem lokalen Rechenzentrum in das AWS Cloudübertragen können.
- Informieren Sie sich über allgemeine bewährte Methoden für die Migration großer Datenbanken sowie über bewährte Methoden für jedes Tool, mit denen Sie die Datenbank effizienter migrieren können.

Migrationsoptionen für große MySQL- und MariaDB-Datenbanken

Sie können aus einer Vielzahl von Optionen wählen, um von lokalen MySQL- oder MariaDB-Datenbanken zu Amazon Relational Database Service (Amazon RDS) oder Amazon Aurora MySQL-Compatible Edition-Datenbank-Instances zu migrieren. Die Wahl des richtigen Migrationsansatzes und Tools ist für eine erfolgreiche Migration von entscheidender Bedeutung. In diesem Leitfaden bewerten Sie die Optionen anhand Ihrer Anforderungen an Benutzerfreundlichkeit, Datengröße und Ausfallzeiten.

Im Folgenden sind die gängigen Migrationstools und -ansätze aufgeführt, mit denen selbstverwaltete MySQL-Datenbanken mit mehreren Terabyte effizient zu Amazon RDS-, Aurora- oder Amazon Elastic Compute Cloud (Amazon EC2) -Datenbank-Instances migriert werden können:

- Percona XtraBackup(Physisch)
- MyDumper(Logisch)
- mysqldump und mysqlpump(Logisch)
- Geteiltes Backup(Physisch, logisch oder beides)

Im Folgenden sind die gängigen Migrationstools und -ansätze aufgeführt, die verfügbar sind, um MySQL-kompatible Datenbanken (wie MariaDB) mit mehreren Terabyte effizient zu Amazon RDS-, Aurora- oder Amazon EC2 EC2-Datenbank-Instances zu migrieren:

- MyDumper(Logisch)
- mysqldump und mysqlpump(Logisch)
- Geteiltes Backup(Physisch, logisch oder beides)

Für jedes Migrationstool gibt es mehrere Methoden, mit denen Sie die große Datenbank-Backup-Datei auf die übertragen können AWS Cloud. Für jedes Tool stehen Optionen zur Verfügung, und Sie können auch Amazon S3 File Gateway verwenden. Weitere Informationen finden Sie unter Verwenden von Amazon S3 File Gateway zum Übertragen von Backup-Dateien in diesem Handbuch.

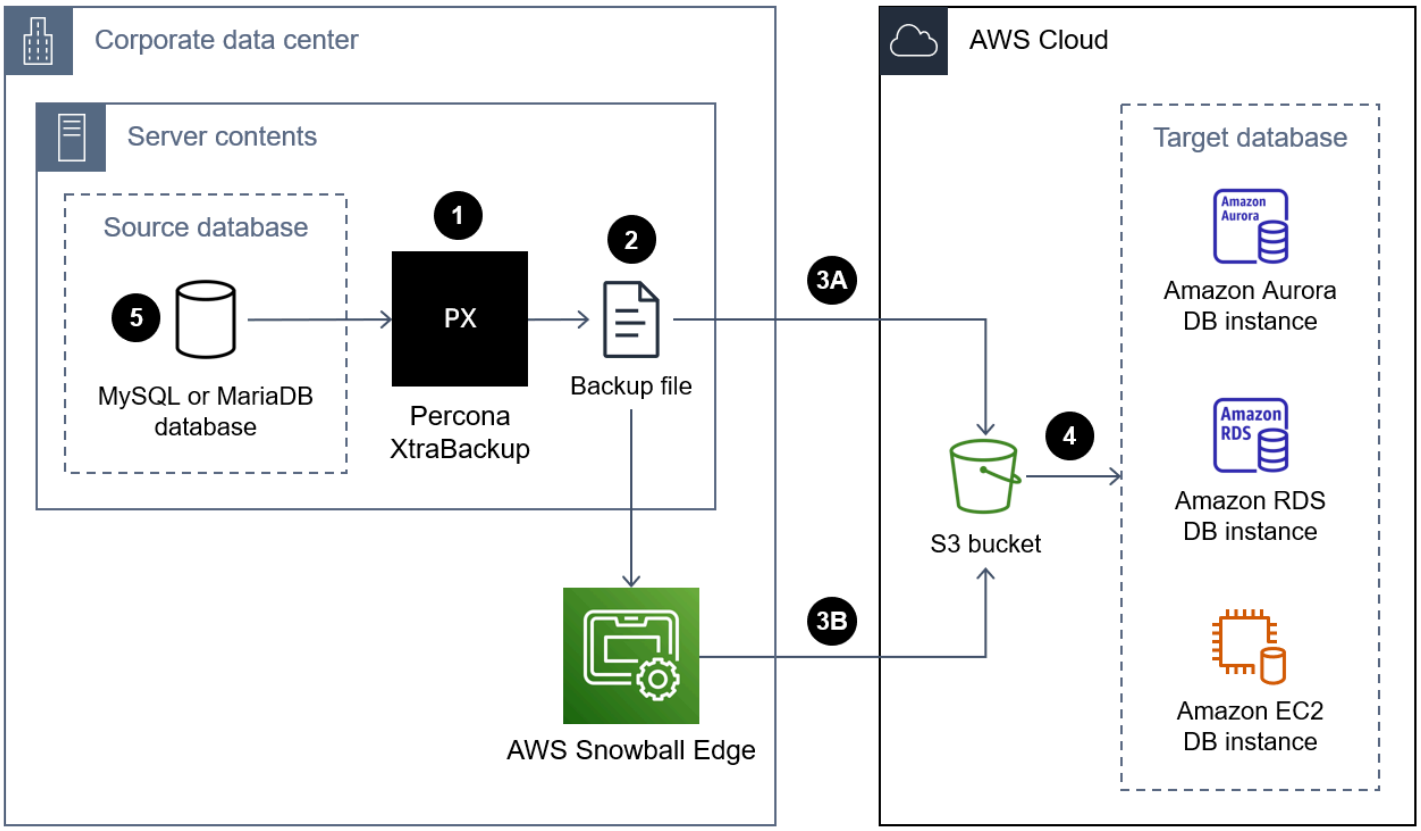
Percona XtraBackup

> **Important**
>
> Percona XtraBackup wird für die MariaDB-Versionen 10.3 oder höher nicht unterstützt und wird für die Versionen 10.1 und 10.2 nur teilweise unterstützt.

Percona XtraBackup ist eine gängige Open-Source-Warm-Backup-Software für MySQL und MariaDB, die blockierungsfreie Backups für InnoDB- und XtraDB-Speicher-Engines erstellt. Es funktioniert mit MySQL- oder MariaDB-Servern. Weitere Informationen über das Tool und einige seiner Funktionen und Vorteile finden Sie XtraBackup in der Percona-Dokumentation unter Über Percona. XtraBackup

Dieses Tool verwendet den Ansatz der physischen Migration. Es kopiert direkt das MySQL- oder MariaDB-Datenverzeichnis und die darin enthaltenen Dateien. Bei großen Datenbanken, z. B. solchen, die größer als 100 GB sind, kann dies zu einer deutlich besseren Wiederherstellungszeit führen als bei einigen anderen Tools. Sie erstellen eine Sicherungskopie der lokalen Quelldatenbank, migrieren die Sicherungsdateien in die Cloud und stellen die Sicherung dann auf der neuen Zieldatenbank-Instance wieder her.

Das folgende Diagramm zeigt die allgemeinen Schritte, die bei der Migration einer Datenbank mithilfe einer XtraBackup Percona-Backup-Datei erforderlich sind. Abhängig von der Größe der Sicherungsdatei stehen zwei Optionen für die Übertragung der Sicherung in einen Amazon Simple Storage Service (Amazon S3) -Bucket im zur Verfügung AWS Cloud.



Im Folgenden sind die Schritte aufgeführt, um mit Percona eine Datenbank XtraBackup zu migrieren: AWS Cloud

1. Installieren Sie Percona XtraBackup auf dem lokalen Server. Wenn Sie Amazon Aurora MySQL Version 2 oder Amazon RDS verwenden, finden Sie weitere Informationen unter Percona XtraBackup 2.4 installieren. Wenn Sie Amazon Aurora MySQL Version 3 verwenden, finden Sie weitere Informationen unter Percona XtraBackup 8.0 installieren in der Percona-Dokumentation XtraBackup.
2. Erstellen Sie eine vollständige Sicherung der MySQL- oder MariaDB-Quelldatenbank. Anweisungen für Percona XtraBackup 2.4 finden Sie unter Vollständige Sicherung. Anweisungen für Percona XtraBackup 8.0 finden Sie unter Erstellen Sie ein vollständiges Backup.
3. Übertragen Sie die Sicherungsdateien mithilfe eines zugelassenen Dienstes oder Tools in Ihrer Organisation über das Internet, z. B. den folgenden:
   - AWS Site-to-Site VPN
   - AWS Client VPN
   - AWS Direct Connect

- Amazon S3 File Gateway (Weitere Informationen finden Sie Verwenden von Amazon S3 File Gateway zum Übertragen von Backup-Dateien in diesem Handbuch.)
- AWS Command Line Interface (AWS CLI)

4. Stellen Sie die Sicherungsdateien aus dem Amazon S3 S3-Bucket auf der Zieldatenbank-Instance wieder her. Detaillierte Informationen finden Sie hier:
   - Informationen zur Aurora MySQL-Compatible Edition finden Sie unter Migrieren von Daten aus MySQL mithilfe eines Amazon S3 S3-Buckets in der Amazon RDS-Dokumentation.
   - Informationen zu Amazon RDS for MySQL oder Amazon EC2 finden Sie unter Daten in eine MySQL-DB-Instance importieren.
   - Informationen zu Amazon RDS for MariaDB oder Amazon EC2 finden Sie unter Daten in eine MariaDB-DB-Instance importieren.
5. (Optional) Sie können die Replikation zwischen der Quelldatenbank und der Zieldatenbank-Instance einrichten. Sie können die Replikation von Binärprotokollen (Binlog) verwenden, um Ausfallzeiten zu reduzieren. Weitere Informationen finden Sie hier:
   - Einstellung der Konfiguration der Replikationsquelle in der MySQL-Dokumentation
   - Für Amazon Aurora finden Sie Folgendes:
     - Synchronisieren des Amazon Aurora MySQL-DB-Clusters mit der MySQL-Datenbank mithilfe der Replikation in der Aurora-Dokumentation
     - Verwendung der Binlog-Replikation in Amazon Aurora in der Aurora-Dokumentation
   - Informationen zu Amazon RDS finden Sie im Folgenden:
     - Arbeiten mit der MySQL-Replikation in der Amazon RDS-Dokumentation
     - Arbeiten mit der MariaDB-Replikation in der Amazon RDS-Dokumentation
   - Informationen zu Amazon EC2 finden Sie im Folgenden:
     - Einrichtung der positionsbasierten Replikation von binären Logdateien in der MySQL-Dokumentation
     - Repliken einrichten in der MySQL-Dokumentation
     - Einrichtung der Replikation in der MariaDB-Dokumentation

Vorteile

- Da Percona einen physischen Migrationsansatz XtraBackup verwendet, ist der Wiederherstellungsprozess in der Regel schneller als bei Tools, die einen logischen

Migrationsansatz verwenden. Dies liegt daran, dass die Leistung eher durch den Festplatten- oder Netzwerkdurchsatz als durch die für die Datenverarbeitung erforderlichen Rechenressourcen begrenzt wird.

- Da der Wiederherstellungsprozess eine direkte Kopie der Dateien aus dem S3-Bucket zur Zieldatenbankinstanz ist, werden XtraBackup Percona-Dateien in der Regel schneller wiederhergestellt als Sicherungsdateien, die mit anderen Tools erstellt wurden.
- Percona XtraBackup ist anpassungsfähig. Es unterstützt beispielsweise mehrere Threads, damit Sie Dateien schneller kopieren können, und unterstützt die Komprimierung, um die Größe des Backups zu reduzieren.

Einschränkungen

- Eine Offline-Sicherung ist nicht möglich, da Percona Zugriff auf den Quelldatenbankserver haben XtraBackup muss.
- Percona XtraBackup kann nur auf Systemen mit identischen Systemarchitekturen verwendet werden. Es ist beispielsweise nicht möglich, eine Sicherungskopie einer Quelldatenbank, die auf Intel für Windows Server läuft, auf einem ARM für Linux-Zielserver wiederherzustellen.
- Percona wird für MariaDB Version 10.3 oder höher XtraBackup nicht unterstützt, und es wird nur teilweise für MariaDB Version 10.2 und Version 10.1 unterstützt. Weitere Informationen finden Sie unter Percona XtraBackup Overview: Compatibility with MariaDB in der MariaDB-Wissensdatenbank.
- Sie können Percona nicht verwenden XtraBackup , um eine MariaDB-Quelldatenbank auf einer MySQL-Zieldatenbank-Instance wie Amazon RDS for MySQL oder Aurora MySQL-Compatible wiederherzustellen.
- Das Gesamtdatenvolumen und die Anzahl der Objekte, die Sie in einem S3-Bucket speichern können, sind unbegrenzt, die maximale Dateigröße beträgt jedoch 5 TB. Wenn Ihre Backup-Datei 5 TB überschreitet, können Sie sie in mehrere kleinere Dateien aufteilen.
- Wenn die `innodb_file_per_table` Einstellung deaktiviert ist, unterstützt Percona XtraBackup keine Teilsicherungen, die`--tables`,`--tables-exclude`, `--tables-file` `--databases`-- `databases-exclude`, oder `--databases-file` verwenden. Weitere Informationen zu Percona XtraBackup Version 2.4 finden Sie unter Partielle Backups. Weitere Informationen für Percona XtraBackup Version 8.0 finden Sie unter Erstellen einer teilweisen Sicherung.

Best Practices

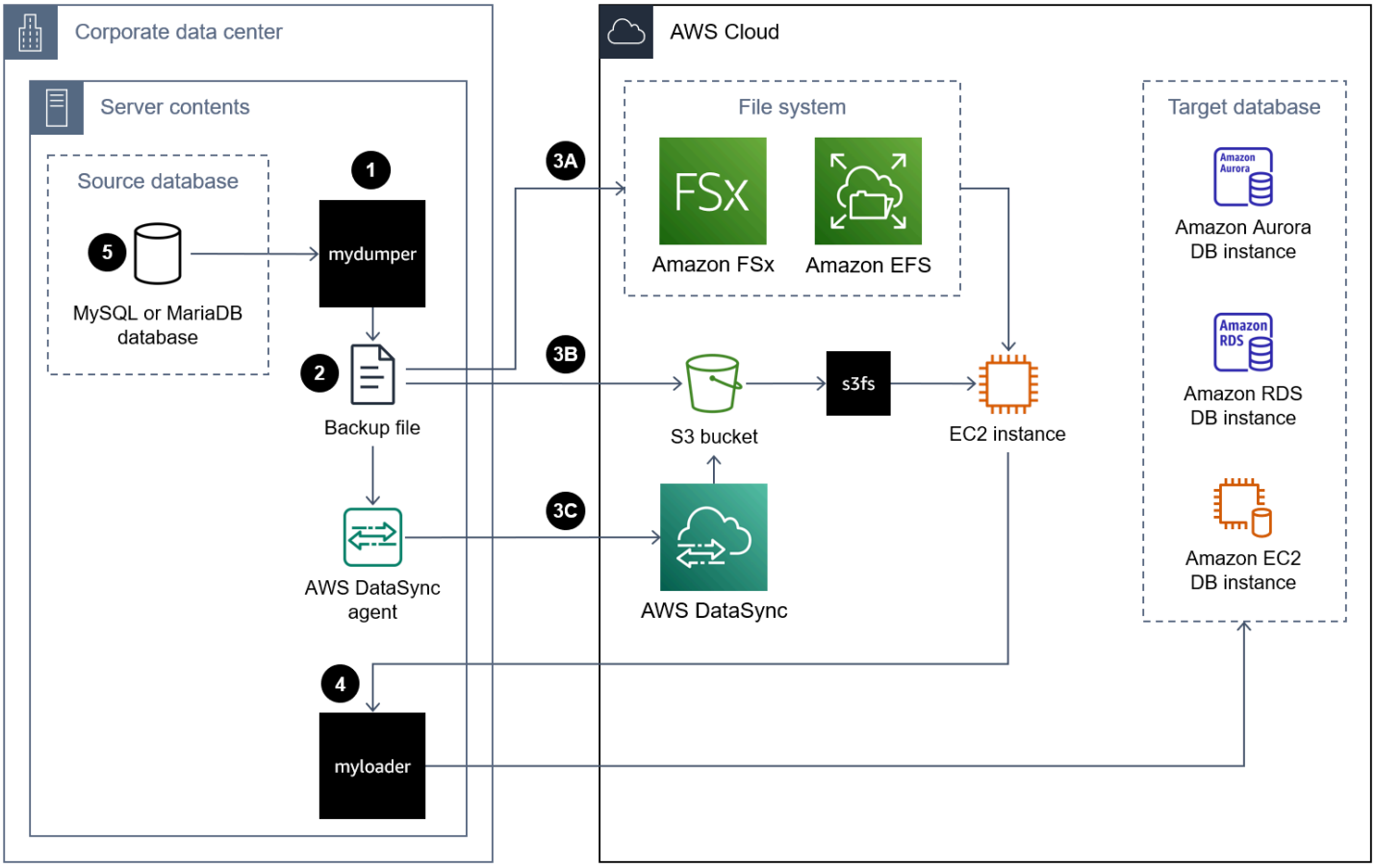
- Gehen Sie wie folgt vor, um die Leistung des Backup-Vorgangs zu verbessern:
  - Kopieren Sie mehrere Dateien parallel mit --parallel= <threads>
  - Komprimieren Sie mehrere Dateien parallel mit --compress-threads= <threads>
  - Erhöhen Sie den Speicher mit --use-memory= <size>
  - Verschlüsseln Sie mehrere Dateien parallel mit --encrypt-threads= <threads>
- Stellen Sie sicher, dass auf dem Quellserver ausreichend Speicherplatz für die Datenbanksicherungsdateien vorhanden ist.
- Generieren Sie die Datenbanksicherung mit der Percona-Datei im xbstream-Format (.xbstream). Weitere Informationen finden Sie in der Percona-Dokumentation unter Die xbstream-Binärdatei im Überblick. XtraBackup

MyDumper

MyDumper(GitHub) ist ein logisches Open-Source-Migrationstool, das aus zwei Dienstprogrammen besteht:

- MyDumper exportiert ein konsistentes Backup von MySQL-Datenbanken. Es unterstützt das Sichern der Datenbank mithilfe mehrerer parallel Threads, bis zu einem Thread pro verfügbarem CPU-Kern.
- myloader liest die von erstellten Sicherungsdateien MyDumper, stellt eine Verbindung zur Zieldatenbankinstanz her und stellt dann die Datenbank wieder her.

Das folgende Diagramm zeigt die wichtigsten Schritte, die bei der Migration einer Datenbank mithilfe einer MyDumper Sicherungsdatei erforderlich sind. Dieses Architekturdiagramm enthält drei Optionen für die Migration der Sicherungsdatei vom lokalen Rechenzentrum zu einer EC2-Instanz in der. AWS Cloud



Im Folgenden finden Sie die Schritte MyDumper zur Migration einer Datenbank auf die: AWS Cloud

1. Install MyDumper und Myloader. Anweisungen finden Sie unter So installieren Sie mydumper/myloader (). GitHub
2. Wird verwendet MyDumper , um eine Sicherungskopie der MySQL- oder MariaDB-Quelldatenbank zu erstellen. Anweisungen finden Sie unter Wie benutzt man. MyDumper
3. Verschieben Sie die Sicherungsdatei auf eine EC2-Instanz in der, AWS Cloud indem Sie einen der folgenden Ansätze verwenden:

   Ansatz 3A — Mounten Sie ein Amazon FSx - oder Amazon Elastic File System (Amazon EFS) -Dateisystem auf dem lokalen Server, auf dem Ihre Datenbank-Instance ausgeführt wird. Sie können AWS Direct Connect oder verwenden Site-to-Site VPN , um die Verbindung herzustellen. Sie können die Datenbank direkt auf der bereitgestellten Dateifreigabe sichern, oder Sie können die Sicherung in zwei Schritten durchführen, indem Sie die Datenbank in einem lokalen Dateisystem sichern und sie dann auf das gemountete FSx- oder EFS-Volume hochladen.

Mounten Sie als Nächstes das Amazon FSx- oder Amazon EFS-Dateisystem, das ebenfalls auf dem lokalen Server bereitgestellt ist, auf einer EC2-Instance.

Ansatz 3B — Verwenden Sie das AWS CLI AWS SDK oder die Amazon S3 S3-REST-API, um die Sicherungsdatei direkt vom lokalen Server in einen S3-Bucket zu verschieben. Befindet sich der Ziel-S3-Bucket in einem AWS-Region , der weit vom Rechenzentrum entfernt ist, können Sie Amazon S3 Transfer Acceleration verwenden, um die Datei schneller zu übertragen. Verwenden Sie das s3fs-fuse-Dateisystem, um den S3-Bucket auf der EC2-Instance zu mounten.

Methode 3C — Installieren Sie den AWS DataSync Agenten im lokalen Rechenzentrum und verwenden Sie ihn dann, AWS DataSyncum die Sicherungsdatei in einen Amazon S3 S3-Bucket zu verschieben. Verwenden Sie das s3fs-fuse-Dateisystem, um den S3-Bucket auf der EC2-Instance zu mounten.

> **Note**
>
> Sie können Amazon S3 File Gateway auch verwenden, um die großen Datenbank-Backup-Dateien in einen S3-Bucket im zu übertragen AWS Cloud. Weitere Informationen finden Sie unter Verwenden von Amazon S3 File Gateway zum Übertragen von Backup-Dateien in diesem Handbuch.

4. Verwenden Sie myloader, um das Backup auf der Zieldatenbank-Instance wiederherzustellen. Anweisungen finden Sie unter Verwendung von myloader ()GitHub.
5. (Optional) Sie können die Replikation zwischen der Quelldatenbank und der Zieldatenbankinstanz einrichten. Sie können die Replikation von Binärprotokollen (Binlog) verwenden, um Ausfallzeiten zu reduzieren. Weitere Informationen finden Sie hier:
   - Einstellung der Konfiguration der Replikationsquelle in der MySQL-Dokumentation
   - Für Amazon Aurora finden Sie Folgendes:
     - Synchronisieren des Amazon Aurora MySQL-DB-Clusters mit der MySQL-Datenbank mithilfe der Replikation in der Aurora-Dokumentation
     - Verwendung der Binlog-Replikation in Amazon Aurora in der Aurora-Dokumentation
   - Informationen zu Amazon RDS finden Sie im Folgenden:
     - Arbeiten mit der MySQL-Replikation in der Amazon RDS-Dokumentation
     - Arbeiten mit der MariaDB-Replikation in der Amazon RDS-Dokumentation
   - Informationen zu Amazon EC2 finden Sie im Folgenden:

- Einrichtung der positionsbasierten Replikation von binären Logdateien in der MySQL-Dokumentation
- Repliken einrichten in der MySQL-Dokumentation
- Einrichtung der Replikation in der MariaDB-Dokumentation

Vorteile

- MyDumper unterstützt Parallelität mithilfe von Multithreading, wodurch die Geschwindigkeit von Sicherungs- und Wiederherstellungsvorgängen verbessert wird.
- MyDumper vermeidet teure Routinen zur Zeichensatzkonvertierung, wodurch sichergestellt wird, dass der Code hocheffizient ist.
- MyDumper vereinfacht das Anzeigen und Analysieren von Daten, indem separate Dumping-Dateien für Tabellen und Metadaten verwendet werden.
- MyDumper verwaltet Schnappschüsse für alle Threads und stellt genaue Positionen der primären und sekundären Protokolle bereit.
- Sie können Perl Compatible Regular Expressions (PCRE) verwenden, um anzugeben, ob Tabellen oder Datenbanken ein- oder ausgeschlossen werden sollen.

Einschränkungen

- Sie können ein anderes Tool wählen, wenn Ihre Datentransformationsprozesse Zwischenspeicherdateien im Flatformat statt im SQL-Format erfordern.
- myloader importiert Datenbankbenutzerkonten nicht automatisch. Wenn Sie das Backup auf Amazon RDS oder Aurora wiederherstellen, erstellen Sie die Benutzer mit den erforderlichen Berechtigungen neu. Weitere Informationen finden Sie unter Rechte für Master-Benutzerkonten in der Amazon RDS-Dokumentation. Wenn Sie das Backup auf einer Amazon EC2 EC2-Datenbank-Instance wiederherstellen, können Sie die Benutzerkonten der Quelldatenbank manuell exportieren und in die EC2-Instance importieren.

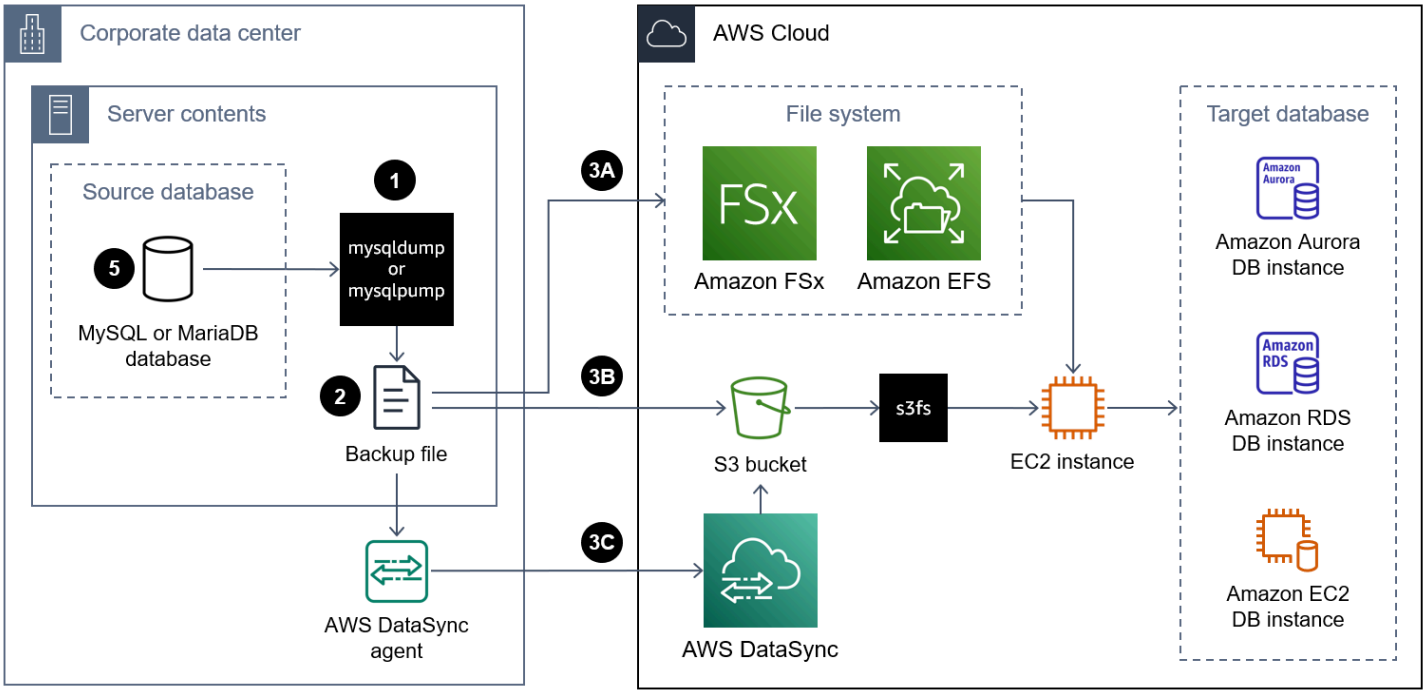
Best Practices

- Konfigurieren MyDumper Sie es so, dass jede Tabelle in Segmente unterteilt wird, z. B. 10.000 Zeilen in jedem Segment, und jedes Segment in eine separate Datei geschrieben wird. Dadurch ist es möglich, die Daten später parallel zu importieren.
- Wenn Sie die InnoDB-Engine verwenden, verwenden Sie die `--trx-consistency-only` Option, um das Sperren zu minimieren.
- Die Verwendung MyDumper zum Exportieren der Datenbank kann leseintensiv werden, und der Vorgang kann sich auf die Gesamtleistung der Produktionsdatenbank auswirken. Wenn Sie über eine Replikatdatenbankinstanz verfügen, führen Sie den Exportvorgang vom Replikat aus aus. Bevor Sie den Export aus dem Replikat ausführen, beenden Sie den Replikations-SQL-Thread. Dadurch kann der Exportvorgang schneller ausgeführt werden.
- Exportieren Sie die Datenbank nicht während der Hauptgeschäftszeiten. Durch die Vermeidung von Spitzenzeiten kann die Leistung Ihrer primären Produktionsdatenbank während des Datenbankexports stabilisiert werden.
- Amazon RDS for MySQL unterstützt das `keyring_aws` Plugin nicht. Weitere Informationen finden Sie unter Bekannte Probleme und Einschränkungen. Um die lokalen verschlüsselten Tabellen zur Amazon RDS-Instance zu migrieren, müssen Sie in den Backup-Skripten `ENCRYPTION` oder `DEFAULT ENCRYPTION` aus der `CREATE TABLE` Syntax entfernen. Für die Verschlüsselung im Ruhezustand können Sie einen AWS Key Management Service (AWS KMS) -Schlüssel verwenden. Weitere Informationen finden Sie unter Verschlüsseln von Amazon-RDS-Ressourcen.

mysqldump und mysqlpump

mysqldump und mysqlpump sind native Datenbank-Backup-Tools für MySQL. MariaDB unterstützt mysqldump, aber nicht mysqlpump. Beide Tools erstellen logische Backups und sind Teil der MySQL-Client-Programme. mysqldump unterstützt Single-Thread-Verarbeitung. mysqlpump unterstützt die parallel Verarbeitung von Datenbanken und Objekten innerhalb von Datenbanken, um den Dump-Prozess zu beschleunigen. Es wurde in MySQL Version 5.7.8 eingeführt. mysqlpump wurde in MySQL Version 8.4 entfernt.

Das folgende Diagramm zeigt die wichtigsten Schritte bei der Migration einer Datenbank mithilfe einer mysqldump- oder mysqlpump-Backup-Datei.



Im Folgenden finden Sie die Schritte zur Verwendung von mysqldump oder mysqlpump zur Migration einer Datenbank auf die: AWS Cloud

1. Installieren Sie MySQL Shell auf dem lokalen Server. Anweisungen finden Sie in der MySQL-Dokumentation unter Installation von MySQL Shell. Dadurch werden sowohl mysqldump als auch mysqlpump installiert.
2. Erstellen Sie mit mysqldump oder mysqlpump eine Sicherungskopie der lokalen Quelldatenbank. Anweisungen finden Sie unter mysqldump und mysqlpump in der MySQL-Dokumentation oder unter Backups mit mysqldump erstellen in der MariaDB-Dokumentation. Weitere Hinweise zum Aufrufen von MySQL-Programmen und zum Angeben von Optionen finden Sie unter MySQL-Programme verwenden.
3. Verschieben Sie die Sicherungsdatei auf eine EC2-Instanz in der, AWS Cloud indem Sie einen der folgenden Ansätze verwenden:

   Ansatz 3A — Mounten Sie ein Amazon FSx - oder Amazon Elastic File System (Amazon EFS) -Dateisystem auf dem lokalen Server, auf dem Ihre Datenbank-Instance ausgeführt wird. Sie können AWS Direct Connect oder verwenden Site-to-Site VPN , um die Verbindung herzustellen. Sie können die Datenbank direkt auf der bereitgestellten Dateifreigabe sichern, oder Sie können die Sicherung in zwei Schritten durchführen, indem Sie die Datenbank in einem lokalen Dateisystem sichern und sie dann auf das gemountete FSx- oder EFS-Volume hochladen.

Mounten Sie als Nächstes das Amazon FSx- oder Amazon EFS-Dateisystem, das ebenfalls auf dem lokalen Server bereitgestellt ist, auf einer EC2-Instance.

Ansatz 3B — Verwenden Sie das AWS CLI AWS SDK oder die Amazon S3 S3-REST-API, um die Sicherungsdatei direkt vom lokalen Server in einen S3-Bucket zu verschieben. Befindet sich der Ziel-S3-Bucket in einem AWS-Region , der weit vom Rechenzentrum entfernt ist, können Sie Amazon S3 Transfer Acceleration verwenden, um die Datei schneller zu übertragen. Verwenden Sie das s3fs-fuse-Dateisystem, um den S3-Bucket auf der EC2-Instance zu mounten.

Methode 3C — Installieren Sie den AWS DataSync Agenten im lokalen Rechenzentrum und verwenden Sie ihn dann, AWS DataSyncum die Sicherungsdatei in einen Amazon S3 S3-Bucket zu verschieben. Verwenden Sie das s3fs-fuse-Dateisystem, um den S3-Bucket auf der EC2-Instance zu mounten.

> **Note**
>
> Sie können Amazon S3 File Gateway auch verwenden, um die großen Datenbank-Backup-Dateien in einen S3-Bucket im zu übertragen AWS Cloud. Weitere Informationen finden Sie unter Verwenden von Amazon S3 File Gateway zum Übertragen von Backup-Dateien in diesem Handbuch.

4. Verwenden Sie die native Wiederherstellungsmethode, um das Backup in der Zieldatenbank wiederherzustellen. Anweisungen finden Sie unter Reloading Backups im SQL-Format in der MySQL-Dokumentation oder unter Daten aus Dump-Dateien wiederherstellen in der MariaDB-Dokumentation.
5. (Optional) Sie können die Replikation zwischen der Quelldatenbank und der Zieldatenbank-Instance einrichten. Sie können die Replikation von Binärprotokollen (Binlog) verwenden, um Ausfallzeiten zu reduzieren. Weitere Informationen finden Sie hier:
   - Einstellung der Konfiguration der Replikationsquelle in der MySQL-Dokumentation
   - Für Amazon Aurora finden Sie Folgendes:
     - Synchronisieren des Amazon Aurora MySQL-DB-Clusters mit der MySQL-Datenbank mithilfe der Replikation in der Aurora-Dokumentation
     - Verwendung der Binlog-Replikation in Amazon Aurora in der Aurora-Dokumentation
   - Informationen zu Amazon RDS finden Sie im Folgenden:
     - Arbeiten mit der MySQL-Replikation in der Amazon RDS-Dokumentation
     - Arbeiten mit der MariaDB-Replikation in der Amazon RDS-Dokumentation

- Informationen zu Amazon EC2 finden Sie im Folgenden:
  - Einrichtung der positionsbasierten Replikation von binären Logdateien in der MySQL-Dokumentation
  - Repliken einrichten in der MySQL-Dokumentation
  - Einrichtung der Replikation in der MariaDB-Dokumentation

Vorteile

- mysqldump und mysqlpump sind in der MySQL Server-Installation enthalten
- Die von diesen Tools generierten Sicherungsdateien haben ein besser lesbares Format.
- Bevor Sie die Sicherungsdatei wiederherstellen, können Sie die resultierende .sql-Datei mit einem Standard-Texteditor ändern.
- Sie können eine bestimmte Tabelle, Datenbank oder sogar eine bestimmte Datenauswahl sichern.
- mysqldump und mysqlpump sind unabhängig von der Maschinenarchitektur.

Einschränkungen

- mysqldump ist ein Backup-Prozess mit einem einzigen Thread. Die Leistung bei der Erstellung eines Backups ist für kleine Datenbanken gut, kann jedoch ineffizient werden, wenn die Backup-Größe größer als 10 GB ist.
- Sicherungsdateien im logischen Format sind umfangreich, insbesondere wenn sie als Text gespeichert werden, und lassen sich oft nur langsam erstellen und wiederherstellen.
- Die Datenwiederherstellung kann langsam sein, da das erneute Anwenden von SQL-Anweisungen in der Ziel-DB-Instance eine intensive Festplatten I/O - und CPU-Verarbeitung für das Einfügen, die Indexerstellung und die Durchsetzung von Einschränkungen der referentiellen Integrität erfordert.
- Das Hilfsprogramm mysqlpump wird für MySQL-Versionen vor 5.7.8 oder für Versionen 8.4 und höher nicht unterstützt.
- Standardmäßig erstellt mysqlpump keine Sicherungskopie der Systemdatenbanken, wie z. B. oder. `performance_schema` `sys` Um einen Teil der Systemdatenbank zu sichern, geben Sie ihm in der Befehlszeile einen expliziten Namen.
- mysqldump sichert keine InnoDB-Anweisungen. `CREATE TABLESPACE`

> **Note**
>
> Backups von CREATE TABLESPACE-Anweisungen und Systemdatenbanken sind nur nützlich, wenn Sie MySQL- oder MariaDB-Datenbanksicherungen auf einer EC2-Instance wiederherstellen. Diese Backups werden nicht für Amazon RDS oder Aurora verwendet.

Best Practices

- Wenn Sie die Datenbanksicherung wiederherstellen, deaktivieren Sie die SchlüsselprüfungenFOREIGN_KEY_CHECKS, z. B. auf Sitzungsebene in der Zieldatenbank. Dadurch wird die Wiederherstellungsgeschwindigkeit erhöht.
- Stellen Sie sicher, dass der Datenbankbenutzer über ausreichende Rechte verfügt, um das Backup zu erstellen und wiederherzustellen.

Geteiltes Backup

Bei einer Split-Backup-Strategie migrieren Sie einen großen Datenbankserver, indem Sie das Backup in mehrere Teile aufteilen. Sie können unterschiedliche Ansätze verwenden, um jeden Teil des Backups zu migrieren. Dies kann die beste Option für die folgenden Anwendungsfälle sein:

- Großer Datenbankserver, aber kleine Einzeldatenbanken — Dies ist ein guter Ansatz, wenn die Größe des gesamten Datenbankservers mehrfach ist, die Größe jeder einzelnen, unabhängigen Benutzerdatenbank TBs jedoch weniger als 1 TB beträgt. Um den Gesamtmigrationszeitraum zu verkürzen, können Sie einzelne Datenbanken separat und parallel migrieren.

  Lassen Sie uns ein Beispiel für einen lokalen Datenbankserver mit 2 TB verwenden. Dieser Server besteht aus vier Datenbanken, die jeweils 0,5 TB groß sind. Sie können Backups jeder einzelnen Datenbank separat erstellen. Beim Wiederherstellen der Sicherung können Sie entweder alle Datenbanken auf einer Instanz parallel wiederherstellen, oder wenn die Datenbanken unabhängig sind, können Sie jede Sicherung auf einer separaten Instanz wiederherstellen. Es hat sich bewährt, unabhängige Datenbanken auf separaten Instanzen wiederherzustellen, anstatt sie auf derselben Instanz wiederherzustellen. Weitere Informationen finden Sie unter Bewährte Methoden in diesem Handbuch.
- Großer Datenbankserver, aber kleine einzelne Datenbanktabellen — Dies ist ein guter Ansatz, wenn der gesamte Datenbankserver mehrfach groß ist, die Größe jeder unabhängigen

Datenbanktabelle TBs jedoch weniger als 1 TB beträgt. Um den Gesamtmigrationszeitraum zu verkürzen, können Sie unabhängige Tabellen einzeln migrieren.

Lassen Sie uns ein Beispiel für eine Einzelbenutzerdatenbank verwenden, die 1 TB groß ist und die einzige Datenbank auf einem lokalen Datenbankserver ist. Es gibt 10 Tabellen in der Datenbank, von denen jede 100 GB groß ist. Sie können Backups jeder einzelnen Tabelle separat erstellen. Beim Wiederherstellen des Backups können Sie alle Tabellen auf einer Instanz parallel wiederherstellen.

- Eine Datenbank enthält sowohl transaktionale als auch nicht-transaktionale Workload-Tabellen. Ähnlich wie im vorherigen Anwendungsfall können Sie einen Split-Backup-Ansatz verwenden, wenn Sie sowohl transaktionale als auch nicht-transaktionale Workload-Tabellen in derselben Datenbank haben.

  Lassen Sie uns ein Beispiel für eine 2-TB-Datenbank verwenden, die aus 0,5 TB an Tabellen für kritische Workloads besteht, die für die Online-Transaktionsverarbeitung (OLTP) verwendet werden, und einer einzelnen 1,5-TB-Tabelle, die für die Archivierung alter Daten verwendet wird. Sie können die Sicherung aller Datenbankobjekte mit Ausnahme der Archivtabelle als konsistente Sicherung mit einer einzigen Transaktion durchführen. Dann erstellen Sie eine weitere, separate Sicherung nur der Archivtabelle. Für die Sicherung der Archivtabelle können Sie auch erwägen, mehrere parallel Sicherungen zu erstellen, indem Sie Bedingungen verwenden, um die Anzahl der Zeilen in der Sicherungsdatei aufzuteilen. Im Folgenden wird ein Beispiel gezeigt:

  ```
  mysqldump -p your_db1 --tables your_table1 --where="column1 between 1 and 1000000 " >
   your_table1_part1.sql
  mysqldump -p your_db1 --tables your_table1 --where="column1 between 1000001 and
   2000000 " > your_table1_part2.sql
  mysqldump -p your_db1 --tables your_table1 --where="column1 > 2000000 " >
   your_table1_part3.sql
  ```

  Beim Wiederherstellen der Sicherungsdateien können Sie die transaktionale Workload-Backup und die Sicherung der Archivtabelle parallel wiederherstellen.

- Einschränkungen der Rechenressourcen — Wenn Sie auf dem lokalen Server nur begrenzte Rechenressourcen wie CPU, Arbeitsspeicher oder Festplatten-I/O haben, kann dies die Stabilität und Leistung bei der Erstellung des Backups beeinträchtigen. Anstatt ein vollständiges Backup zu erstellen, können Sie es in Teile aufteilen.

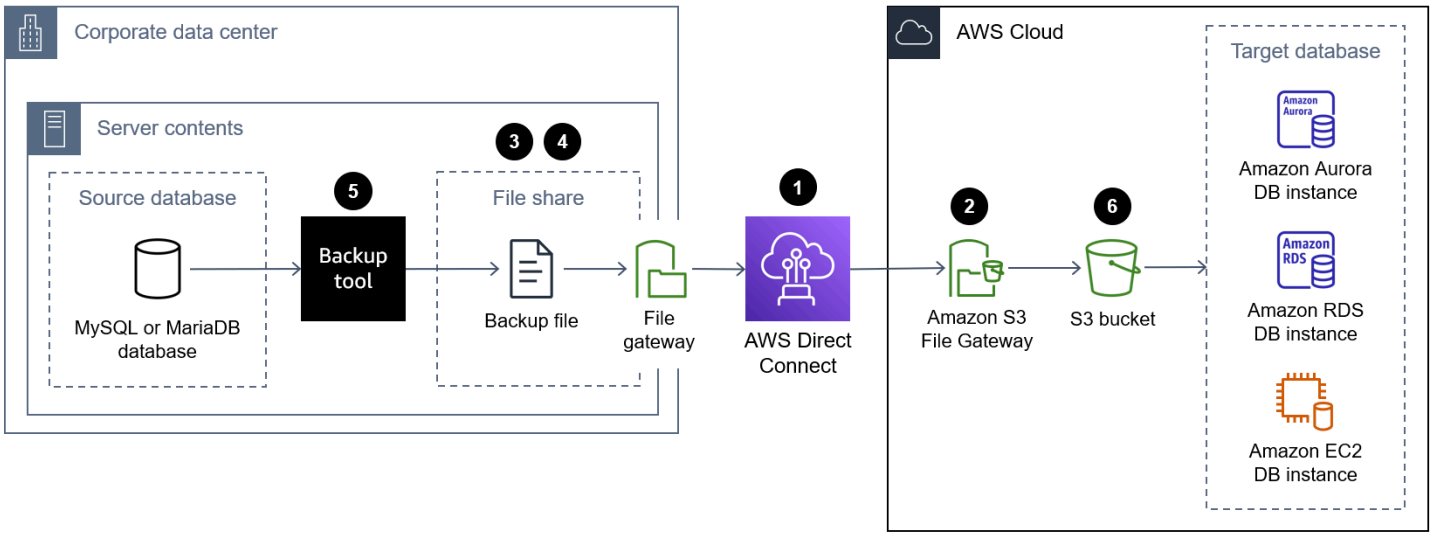
  Beispielsweise kann ein lokaler Produktionsserver stark mit Workloads belastet sein und über begrenzte CPU-Ressourcen verfügen. Wenn Sie ein Backup einer Datenbank mit mehreren

Terabyte auf diesem Server in einem einzigen Durchlauf erstellen, kann dies zusätzliche CPU-Ressourcen verbrauchen und sich negativ auf den Produktionsserver auswirken. Anstatt die gesamte Datenbanksicherung zu erstellen, teilen Sie die Sicherung in mehrere Teile auf, z. B. jeweils 2—3 Tabellen.

Verwenden von Amazon S3 File Gateway zum Übertragen von Backup-Dateien

Amazon S3 File Gateway verbindet Ihre lokale Umgebung über eine Dateischnittstelle mit Amazon Simple Storage Service (Amazon S3), sodass Sie Amazon S3-Objekte mithilfe branchenüblicher Dateiprotokolle wie Network File System (NFS) und Server Message Block (SMB) speichern und abrufen können. Es wurde als kostengünstige, skalierbare Lösung für die Speicherung von Daten in der Cloud konzipiert. Da Sie ihn zum Speichern von Datenbanksicherungsdateien verwenden können, kann Ihnen dieser Service bei der Migration großer, lokaler Datenbanken auf die AWS Cloud helfen. Sie könnten beispielsweise Amazon S3 File Gateway und Ihr bevorzugtes Datenbank-Backup-Tool verwenden, um die große MySQL- oder MariaDB-Datenbank direkt in einem Amazon S3 S3-Bucket zu sichern. Anschließend können Sie den S3-Bucket auf der Ziel-Instance bereitstellen und das Backup wiederherstellen.

Das folgende Diagramm zeigt die wichtigsten Schritte, die erforderlich sind, wenn Sie Amazon S3 File Gateway verwenden, um die Sicherungsdatei für eine lokale Datenbank in einen S3-Bucket in der AWS Cloud zu übertragen.



Im Folgenden finden Sie die Schritte zur Verwendung von Amazon S3 File Gateway zur Übertragung einer Datenbank-Backup-Datei von einem lokalen Rechenzentrum in einen S3-Bucket im AWS Cloud:

1. Connect das lokale Rechenzentrum mit dem, AWS Cloud indem Sie einen Dienst wie AWS Direct Connect oder AWS Site-to-Site VPN oder über eine öffentliche Internetverbindung verwenden.

2. Erstellen Sie ein S3 File Gateway. Anweisungen finden Sie unter Ihr Gateway erstellen.
3. Erstellen Sie eine NFS- oder SMB-Dateifreigabe, die vom S3 File Gateway gehostet wird. Anweisungen finden Sie unter Erstellen einer Dateifreigabe.
4. Mounten Sie die NFS- oder SMB-Dateifreigabe auf dem lokalen Server, der Ihre MySQL- oder MariaDB-Datenbank hostet. Anweisungen finden Sie unter Bereitstellen und Verwenden Ihrer Dateifreigabe.
5. Sichern Sie die lokale MySQL- oder MariaDB-Datenbank in dem Verzeichnis, in dem die NFS-Dateifreigabe eingehängt ist. Sie können jedes der in diesem Handbuch beschriebenen Backup-Tools verwenden.
6. Stellen Sie die Datenbanksicherung auf der Zieldatenbankinstanz wieder her, indem Sie einen der in diesem Handbuch beschriebenen Ansätze verwenden.

Vorteile

- Indem Sie Datenbank-Backups direkt im S3-Bucket erstellen und das Backup auf der Ziel-DB-Instance direkt aus demselben S3-Bucket wiederherstellen, können Sie den end-to-end Migrationsprozess erheblich beschleunigen.
- Datenbank-Backup-Dateien werden dauerhaft in Amazon S3 gespeichert, und Sie wählen die Lifecycle-Management-Richtlinie und die S3-Speicherklasse.

Einschränkungen

Bei der Verwendung von Amazon S3 File Gateway-Dateifreigaben gelten folgende Einschränkungen:

- Die maximale Anzahl von Dateifreigaben pro Gateway beträgt 50.
- Um Lese- und Schreibkonflikte zu vermeiden, wenn mehrere Dateifreigaben denselben S3-Bucket verwenden, müssen Sie jede Dateifreigabe so konfigurieren, dass sie einen eindeutigen Präfixnamen verwendet.
- Die maximale Größe einer einzelnen Datei beträgt 5 TB, was der maximalen Größe jedes einzelnen Objekts in Amazon S3 entspricht.
- Die maximale Pfadlänge beträgt 1024 Zeichen.
- Windows ACLs wird nur auf Dateifreigaben unterstützt, die für Active Directory aktiviert sind, wenn Sie Windows SMB-Clients für den Zugriff auf die Dateifreigaben verwenden.

- Amazon S3 File Gateway unterstützt maximal 10 ACL-Einträge für jede Datei und jedes Verzeichnis.
- Die Root-ACL-Einstellungen von SMB-Dateifreigaben befinden sich nur auf dem Gateway. Diese Einstellungen bleiben bei Gateway-Updates und Neustarts erhalten.

> **Note**
>
> Wenn Sie den Ordner ACLs im Stammverzeichnis statt im übergeordneten Ordner unter dem Stammverzeichnis konfigurieren, sind die ACL-Berechtigungen in Amazon S3 nicht dauerhaft.

Bewährte Methoden

Weitere Informationen zu den bewährten Methoden für Amazon S3 File Gateway finden Sie unter Bewährte Methoden in der S3 File Gateway-Dokumentation.

Bewährte Methoden für die Migration großer MySQL- und MariaDB-Datenbanken

Lesen Sie zusätzlich zu den toolspezifischen Best Practices, die für jede Migrationsoption aufgeführt sind, auch die folgenden allgemeinen bewährten Methoden. Diese bewährten Methoden gelten für die Migration großer MySQL- und MariaDB-Datenbanken mit mehreren Terabyte, unabhängig vom ausgewählten Tool:

- Stellen Sie sicher, dass in den Quell- und Zieldatenbanken ausreichend Speicherplatz vorhanden ist, um das Backup zu erstellen und wiederherzustellen.
- Erstellen Sie keine sekundären Indizes auf der Zieldatenbank-Instance, bis die Migration abgeschlossen ist. Sekundäre Indizes erhöhen den Wartungsaufwand beim Import und können den Importvorgang verlangsamen.
- Wenn Sie einen Multithread-Ansatz verwenden, wählen Sie die richtige Anzahl von Threads. Für den Export empfehlen wir, einen Thread für jeden CPU-Kern zu verwenden. Für den Import empfehlen wir, einen Thread für jeweils zwei CPU-Kerne zu verwenden.
- Datendumps werden häufig von aktiven Datenbankservern aus ausgeführt, die Teil einer unternehmenskritischen Produktionsumgebung sind. Wenn der Datendump die Leistung erheblich beeinträchtigt und dies in Ihrer Umgebung nicht akzeptabel ist, sollten Sie eine der folgenden Optionen in Betracht ziehen:
  - Der Quellserver verfügt über Replikate. Sie können Daten von einem der Replikate sichern.
  - Der Quellserver wird durch regelmäßige Backup-Verfahren abgedeckt:
    - Wenn das Backup-Format für den direkten Import in die Zieldatenbank geeignet ist, verwenden Sie die Backup-Daten als Eingabe für den Importvorgang.
    - Wenn das Backup-Format nicht für den direkten Import in die Zieldatenbank geeignet ist, verwenden Sie das Backup, um eine temporäre Datenbank bereitzustellen und Daten daraus zu sichern.
  - Wenn Replikate und Backups nicht verfügbar sind:
    - Führen Sie Dumps außerhalb der Spitzenzeiten durch, wenn der Produktionsverkehr am geringsten ist.
    - Reduzieren Sie die Parallelität von Dump-Vorgängen, sodass der Server über genügend freie Kapazität für den Produktionsdatenverkehr verfügt.
- Erstellen Sie nur Dumps von vom Benutzer erstellten Datenbanken.

- Erstellen Sie die Benutzer in der Zieldatenbank neu und konfigurieren Sie ihre Berechtigungen. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon RDS, Identitäts- und Zugriffsmanagement für Amazon Aurora oder Identitäts- und Zugriffsmanagement für Amazon EC2.
- Wenn Sie einen großen Datenbankserver migrieren, der aus mehreren unabhängigen Datenbanken besteht, erstellen Sie für jede Datenbank eine separate Instanz. Auf diese Weise können Sie die Datenbank effizienter verwalten und die Ressourcenbereitstellung verbessern, und die separaten Rechenressourcen können die Datenbankleistung verbessern.

Ressourcen

AWS Präskriptive Leitlinien

- Portfolio-Leitfaden für große Migrationen AWS
- Migrationsstrategie für relationale Datenbanken
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon RDS for MySQL
- Richten Sie die Datenreplikation zwischen Amazon RDS for MySQL und MySQL auf Amazon EC2 mithilfe von GTID ein
- Migrieren Sie eine lokale MariaDB-Datenbank mit nativen Tools zu Amazon RDS for MariaDB

AWS Blog-Beiträge

- Bewährte Sicherheitsmethoden für Amazon RDS for MySQL- und MariaDB-Instances
- Migrieren Sie selbstverwaltetes MariaDB zu Amazon Aurora MySQL

Ressourcen für die Wiederherstellung des Backups

- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)
- Mit SSH eine Verbindung zu Ihrer Linux-Instance herstellen (EC2 Amazon-Dokumentation)
- Konfiguration der AWS CLI (AWS CLI Dokumentation)
- Befehl sync (AWS CLI Befehlsreferenz)
- Erstellen einer IAM-Richtlinie für den Zugriff auf Amazon S3 S3-Ressourcen (Aurora-Dokumentation)
- Voraussetzungen für DB-Cluster (Aurora-Dokumentation)
- Arbeiten mit DB-Subnetzgruppen (Aurora-Dokumentation)
- Erstellen einer VPC-Sicherheitsgruppe für einen privaten DB-Cluster (Aurora-Dokumentation)
- Wiederherstellen eines Aurora MySQL-DB-Clusters aus einem Amazon S3 S3-Bucket (Aurora-Dokumentation)
- Einrichtung der Replikation mit MySQL oder einem anderen Aurora-DB-Cluster (Aurora-Dokumentation)
- rds_set_external_master-Verfahren (Amazon RDS-Dokumentation)

- rds_start_replication-Verfahren (Amazon RDS-Dokumentation)

AWS Marketing

- Amazon Aurora
- Amazon RDS für MariaDB
- Amazon RDS für MySQL
- Amazon S3 File Gateway

Sonstige Ressourcen

- Percona XtraBackup
- MyDumper
- Mein SQL-Dump
- mysql-Pumpe

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Verfügbarkeit von mysqlpump	mysqlpump wurde in MySQL Version 8.4 entfernt. Wir haben die Abschnitte mysqldump und mysqlpump aktualisiert, um dieser Änderung der Verfügbarkeit Rechnung zu tragen.	21. November 2024
MyDumper bewährte Verfahren	Wir haben die bewährten Methoden aktualisiert MyDumper , um Informationen zur Migration verschlüsselter Datenbanktabellen hinzuzufügen.	24. Oktober 2024
Percona-Versionen XtraBackup	Im XtraBackup Abschnitt Percona haben wir die Anweisungen aktualisiert, sodass sie den Versionen von Percona entsprechen, die von Amazon Aurora MySQL und Amazon RDS XtraBackup unterstützt werden.	3. August 2023
Erste Veröffentlichung	—	06. April 2023

AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern verwendet, die von AWS Prescriptive Guidance bereitgestellt werden. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Refactor/re-architect — Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile der Cloud-nativen Funktionen nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-Compatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr Kundenbeziehungsmanagement (CRM) -System zu. Salesforce.com
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2-Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

A2A () Agent-to-Agent

Ein Stateful-Protokoll für die Zusammenarbeit zwischen Agenten, das die Delegierung von Aufgaben und die Zustandsübertragung unterstützt.

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank verarbeitet Transaktionen von verbindenden Anwendungen, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Agent

Ein KI-System, das mithilfe von Tools selbständig Überlegungen anstellen, planen und Maßnahmen ergreifen kann, um Ziele zu erreichen.

Agent Ops

Operative Verfahren zum Erstellen, Testen, Bereitstellen und Ausführen von KI-Agenten in der Produktion im großen Maßstab.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung von AIOps in der AWS - Migrationsstrategie finden Sie im Leitfaden zur Betriebsintegration.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Einführung der Cloud (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

blue/green Einsatz

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, sogenannte bösartige Bots, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet.

Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er in der Regel keine Zugriffsrechte besitzt. Weitere Informationen finden Sie in den Leitlinien unter dem Indikator „Glasbruchverfahren implementieren“. AWS Well-Architected

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter AWS Framework für die Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

Citizen Developer

Ein Geschäftsanwender, der KI-Anwendungen mithilfe von Plattformen ohne Programmierkenntnisse erstellt. code/low

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Re-invention — Optimierung von Produkten und Dienstleistungen sowie Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen

Cloud-Repositorys gehören GitHub oderBitbucket Cloud. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD Pipeline kann mehrere Repositorys verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. Amazon SageMaker AI bietet beispielsweise Bildverarbeitungsalgorithmen für CV.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

kontinuierliche Integration und kontinuierliche Bereitstellung () CI/CD

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD wird allgemein als Pipeline beschrieben. CI/CD kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil der Sicherheitssäule des AWS Well-Architected Frameworks. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, die sicherstellen, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen historischer Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

Tiefgreifende Verteidigung

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein umfassender Verteidigungsansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren AWS Organizations, um die Konten der Organisation zu verwalten und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Einsatz

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, die Sie zur Minimierung von Ausfallzeiten und Datenverlusten aufgrund einer Katastrophe anwenden. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domänengesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweise Modernisierung älterer Microsoft ASP.NET (ASMX) -Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung der Wertströme in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

elektronischer Datenaustausch (EDI)

Der automatisierte Austausch von Geschäftsdokumenten zwischen Organisationen. Weitere Informationen finden Sie unter Was ist elektronischer Datenaustausch.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-endian Systeme speichern das höchstwertige Byte zuerst. Little-endian Systeme speichern das niedrigstwertige Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.
- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsepen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn

Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

Eingabeaufforderung mit wenigen Klicks

Bereitstellung einer kleinen Anzahl von Beispielen für ein LLM, die die Aufgabe und das gewünschte Ergebnis veranschaulichen, bevor es aufgefordert wird, eine ähnliche Aufgabe auszuführen. Bei dieser Technik handelt es sich um eine Anwendung des kontextbezogenen Lernens, bei der Modelle anhand von Beispielen (Aufnahmen) lernen, die in Eingabeaufforderungen eingebettet sind. Few-shot Eingabeaufforderungen können bei Aufgaben, die spezifische Formatierungs-, Argumentations- oder Fachkenntnisse erfordern, effektiv sein. Siehe auch Zero-Shot-Eingabeaufforderung.

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

Ein großes neuronales Deep-Learning-Netzwerk, das mit riesigen Datensätzen generalisierter und unbeschrifteter Daten trainiert wurde. FMs sind in der Lage, eine Vielzahl allgemeiner Aufgaben zu erfüllen, z. B. Sprache zu verstehen, Text und Bilder zu generieren und Konversationen in natürlicher Sprache zu führen. Weitere Informationen finden Sie unter Was sind Foundation-Modelle.

FM-Gateway

Ein zentraler Vermittler, der den Zugriff auf Basismodelle kontrolliert und normalisiert. Wird auch als LLM-Gateway bezeichnet.

G

Generative KI

Eine Untergruppe von KI-Modellen, die mit großen Datenmengen trainiert wurden und mithilfe einer einfachen Textaufforderung neue Inhalte und Artefakte wie Bilder, Videos, Text und Audio erstellen können. Weitere Informationen finden Sie unter Was ist Generative KI.

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

goldenes Bild

Ein Snapshot eines Systems oder einer Software, der als Vorlage für die Bereitstellung neuer Instanzen dieses Systems oder dieser Software verwendet wird. In der Fertigung kann ein Golden Image beispielsweise zur Bereitstellung von Software auf mehreren Geräten verwendet werden und trägt so zur Verbesserung der Geschwindigkeit, Skalierbarkeit und Produktivität bei der Geräteherstellung bei.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

Leitplanken (KI)

Sicherheitsmechanismen, die Eingaben und Ausgaben von Agenten filtern, validieren und einschränken, um ein verantwortungsbewusstes und sicheres Verhalten der KI zu gewährleisten.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Holdout-Daten

Ein Teil historischer, beschrifteter Daten, der aus einem Datensatz zurückgehalten wird, der zum Trainieren eines Modells für maschinelles Lernen verwendet wird. Sie können Holdout-Daten verwenden, um die Modellleistung zu bewerten, indem Sie die Modellvorhersagen mit den Holdout-Daten vergleichen.

Der Mensch im Kreis (HiTL)

Ein Workflow-Muster, bei dem die Ausführung von Agenten an kritischen Entscheidungspunkten unterbrochen wird, um von einem Mitarbeiter geprüft und genehmigt zu werden.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im Framework. AWS Well-Architected

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und bezieht. AI/ML

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

Industrielles Internet der Dinge (IIoT)

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Mehr Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in derselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

großes Sprachmodell (LLM)

Ein Deep-Learning-KI-Modell, das anhand einer riesigen Datenmenge vorab trainiert wurde. Ein LLM kann mehrere Aufgaben ausführen, z. B. Fragen beantworten, Dokumente zusammenfassen,

Text in andere Sprachen übersetzen und Sätze vervollständigen. Weitere Informationen finden Sie unter Was sind LLMs.

Große Migration

Eine Migration von 300 oder mehr Servern.

LBAC

Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Verfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

MCP

Siehe Model Context Protocol.

Model Context Protocol (MCP)

Ein zustandsloses Protokoll für die Kommunikation zwischen Agenten und Tool.

MCP-Server

Ein Dienst, der ein oder mehrere Tools über das Model Context Protocol verfügbar macht.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Mechanismen im AWS Well-Architected Framework erstellen.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind AWS Organizations. Ein Konto kann jeweils nur Mitglied einer Organisation sein.

MES

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes, auf dem publish/subscribeMuster basierendes M2M-Kommunikationsprotokoll (Machine-to-Machine) für IoT-Geräte mit beschränkten Ressourcen.

Microservice

Ein kleiner, unabhängiger Service, der über klar definierte APIs kommuniziert und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren über eine klar definierte Schnittstelle mithilfe einfacher APIs. Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementieren von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads

durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Cross-functional Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams von Migration Factory gehören in der Regel Betriebsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Um die Konsistenz, Zuverlässigkeit und Vorhersagbarkeit zu verbessern, empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Siehe Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein Machine-to-Machine-Kommunikationsprotokoll (M2M) für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Einen Trail für eine Organisation erstellen.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder

einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz von Natur aus

Ein systemtechnischer Ansatz, der den Datenschutz während des gesamten Entwicklungsprozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Mit diesen Steuerelementen werden Ressourcen gescannt, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

schnelle Verkettung

Verwenden Sie die Ausgabe einer LLM-Eingabeaufforderung als Eingabe für die nächste Aufforderung, um bessere Antworten zu generieren. Diese Technik wird verwendet, um eine komplexe Aufgabe in Unteraufgaben zu unterteilen oder um eine vorläufige Antwort iterativ zu

verfeinern oder zu erweitern. Sie trägt dazu bei, die Genauigkeit und Relevanz der Antworten eines Modells zu verbessern und ermöglicht detailliertere, personalisierte Ergebnisse.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RAG

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares

Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten für alle Parteien definiert, die an Migrationsaktivitäten und Cloud-Vorgängen beteiligt sind. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

Eine generative KI-Technologie, bei der ein LLM auf eine maßgebliche Datenquelle verweist, die sich außerhalb seiner Trainingsdatenquellen befindet, bevor eine Antwort generiert wird. Ein RAG-Modell könnte beispielsweise eine semantische Suche in der Wissensdatenbank oder in benutzerdefinierten Daten einer Organisation durchführen. Weitere Informationen finden Sie unter Was ist RAG.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel für die Erholungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS-Managementkonsole oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheit durch Design

Ein systemtechnischer Ansatz, der die Sicherheit während des gesamten Entwicklungsprozesses berücksichtigt.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt

werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPs definieren Integritätsschutz oder legen Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Services oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, während Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

Schatten-KI

Nicht autorisierte KI-Anwendungen, die außerhalb der kontrollierten Kanäle innerhalb eines Unternehmens erstellt oder verwendet wurden.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

Split-and-Seed-Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue

Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der. AWS Cloud

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweise Modernisierung älterer Microsoft ASP.NET (ASMX) -Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

Systemaufforderung

Eine Technik, mit der einem LLM Kontext, Anweisungen oder Richtlinien zur Verfügung gestellt werden, um sein Verhalten zu steuern. Systemaufforderungen helfen dabei, den Kontext festzulegen und Regeln für Interaktionen mit Benutzern festzulegen.

T

tags

Key-value Paare, die als Metadaten für die Organisation Ihrer AWS Ressourcen dienen. Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die

Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

tool

Eine Funktion oder API, die ein Agent aufrufen kann, um Operationen in externen Systemen auszuführen.

Transit-Gateway

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der AWS Transit Gateway Dokumentation unter Was ist ein Transit-Gateway.

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs, mit der Sie den Datenverkehr mithilfe von privaten IP-Adressen weiterleiten können. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems gefährdet.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Mal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur wird als unveränderlich angesehen.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Eingabeaufforderung ohne Vorwarnung

Bereitstellung von Anweisungen für die Ausführung einer Aufgabe an einen LLM, jedoch ohne Beispiele (Schnappschüsse), die ihm als Orientierungshilfe dienen könnten. Der LLM muss sein vortrainiertes Wissen einsetzen, um die Aufgabe zu bewältigen. Die Effektivität von Zero-Shot Prompting hängt von der Komplexität der Aufgabe und der Qualität der Aufforderung ab. Siehe auch Few-Shot-Eingabeaufforderungen.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.