Implementierung von verwaltetem PostgreSQL für mehrinstanzenfähige SaaS-Anwendungen auf AWS

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Implementierung von verwaltetem PostgreSQL für mehrinstanzenfähige SaaS-Anwendungen auf AWS

Table of Contents

Implementierung von verwaltetem PostgreSQL für mehrinstanzenfähige SaaS-Anwendungen auf AWS

Tabby Ward und Thomas Davis, Amazon Web Services ()AWS

April 2024 (Verlauf der Dokumente)

Wenn Sie eine Datenbank zum Speichern von Betriebsdaten auswählen, müssen Sie unbedingt berücksichtigen, wie die Daten strukturiert sein sollten, welche Abfragen sie beantworten, wie schnell sie Antworten liefern und wie robust die Datenplattform selbst ist. Zu diesen allgemeinen Überlegungen kommen die Auswirkungen von Software as a Service (SaaS) auf Betriebsdaten hinzu, wie z. B. Leistungsisolierung, Mandantensicherheit sowie einzigartige Merkmale und Entwurfsmuster, die typisch für Daten für mehrinstanzenfähige SaaS-Anwendungen sind. In diesem Leitfaden wird erläutert, wie sich diese Faktoren auf die Verwendung einer PostgreSQL-Datenbank auf Amazon Web Services (AWS) als primärer Betriebsdatenspeicher für eine SaaS-Anwendung mit mehreren Mandanten auswirken. Der Leitfaden konzentriert sich insbesondere auf zwei AWS verwaltete PostgreSQL-Optionen: Amazon Aurora PostgreSQL-Compatible Edition und Amazon Relational Database Service (Amazon RDS) für PostgreSQL.

Gezielte Geschäftsergebnisse

Dieser Leitfaden bietet eine detaillierte Analyse der Best Practices für SaaS-Anwendungen mit mehreren Mandanten, die Aurora PostgreSQL-kompatibel und Amazon RDS for PostgreSQL verwenden. Wir empfehlen Ihnen, die in diesem Leitfaden beschriebenen Entwurfsmuster und Konzepte zu verwenden, um Ihre Implementierung von Aurora PostgreSQL-Compatible oder Amazon RDS for PostgreSQL für Ihre mehrinstanzenfähigen SaaS-Anwendungen zu unterstützen und zu standardisieren.

Diese präskriptiven Leitlinien tragen dazu bei, die folgenden Geschäftsergebnisse zu erzielen:

- Auswahl der optimalsten AWS verwalteten PostgreSQL-Option für Ihren Anwendungsfall — In dieser Anleitung werden relationale und nicht-relationale Optionen für die Datenbanknutzung mit SaaS-Anwendungen verglichen. Es wird auch erörtert, welche Anwendungsfälle für Aurora PostgreSQL-kompatibel und Amazon RDS für PostgreSQL am besten geeignet sind. Diese Informationen helfen Ihnen bei der Auswahl der besten Option für Ihre SaaS-Anwendung.

- Durchsetzung von SaaS-Best-Practices durch die Einführung eines SaaS-Partitionierungsmodells — In diesem Leitfaden werden drei allgemeine SaaS-Partitionierungsmodelle erörtert und verglichen, die auf ein PostgreSQL-Datenbankmanagementsystem (DBMS) anwendbar sind: Pool-, Bridged- und Silo-Modelle sowie deren Varianten. Diese Ansätze erfassen bewährte SaaS-Methoden und bieten Flexibilität beim Entwerfen einer SaaS-Anwendung. Die Durchsetzung eines SaaS-Partitionierungsmodells ist ein entscheidender Bestandteil der Wahrung bewährter Verfahren.
- Effektiver Einsatz von RLS in Pool-SaaS-Partitionierungsmodellen — Sicherheit auf Zeilenebene (RLS) unterstützt die Durchsetzung der Mandantendatenisolierung innerhalb einer einzigen PostgreSQL-Tabelle, indem die Zeilen, die angezeigt werden können, basierend auf dem Benutzer oder einer Kontextvariablen eingeschränkt werden. Wenn Sie das Pool-Partitionierungsmodell verwenden, ist RLS erforderlich, um einen mandantenübergreifenden Zugriff zu verhindern.

Auswahl einer Datenbank für eine SaaS-Anwendung

Bei vielen mehrinstanzenfähigen SaaS-Anwendungen kann die Auswahl einer betriebsbereiten Datenbank auf die Wahl zwischen relationalen und nicht relationalen Datenbanken oder einer Kombination aus beidem reduziert werden. Berücksichtigen Sie bei Ihrer Entscheidung die folgenden allgemeinen Anforderungen und Merkmale von Anwendungsdaten:

- Datenmodell der Anwendung
- Zugriffsmuster für die Daten
- Anforderungen an die Datenbanklatenz
- Anforderungen an Datenintegrität und Transaktionsintegrität (Atomizität, Konsistenz, Isolierung und Haltbarkeit oder ACID)
- Regionsübergreifende Verfügbarkeits- und Wiederherstellungsanforderungen

In der folgenden Tabelle werden die Anforderungen und Merkmale von Anwendungsdaten aufgeführt und im Zusammenhang mit AWS Datenbankangeboten erörtert: Aurora PostgreSQL-kompatibel und Amazon RDS für PostgreSQL (relational) sowie Amazon DynamoDB (nicht relational). Sie können auf diese Matrix zurückgreifen, wenn Sie versuchen, sich zwischen relationalen und nicht-relationalen operativen Datenbankangeboten zu entscheiden.

Datenbanken	Anforderungen und Eigenschaften von SaaS-Anwendungsdaten				
	Datenmodell	Zugriffsmuster	Anforderungen an die Latenz	Daten- und Transaktionsintegrität	Regionsübergreifende Verfügbarkeit und Wiederherstellung
Relational (Aurora PostgreSQL-kompatibel und Amazon	Relational oder stark normalisiert.	Muss nicht im Voraus gründlich geplant werden.	Vorzugsweise höhere Latenztoleranz; kann standardmäßig mit	Standardmäßig wird eine hohe Daten- und Transaktionsintegrität beibehalten.	In Amazon RDS können Sie eine Read Replica für regionsübergreifende

RDS für PostgreSQL)	Aurora und durch Implementierung von Read Replicas, Caching und ähnlichen Funktionen niedriger e Latenzen erreichen.	Skalierung und Failover erstellen . Aurora automatisiert diesen Prozess größtenteils. Für mehrere AWS-Regionen Active-Active-Konfigurationen können Sie die Schreibweiterleitung in Verbindung mit den globalen Aurora-Datenbanken verwenden.

Nicht relational (Amazon DynamoDB)	Normalerweise denormalisiert. Diese Datenbanken nutzen Muster für die Modellierung von many-to-manyBeziehungen, großen Datenmengen und Zeitreihendaten.	Alle Zugriffsmuster (Abfragen) für Daten müssen gründlich verstanden werden, bevor ein Datenmodell erstellt wird.	Sehr niedrige Latenz mit Optionen wie Amazon DynamoDB Accelerator (DAX), die die Leistung noch weiter verbessern können.	Optionale Transaktionsintegrität auf Kosten der Leistung. Bedenken hinsichtlich der Dateninte grität werden auf die Anwendung verlagert.	Einfache regionsübergreifende Wiederherstellung und Active-Active-Konfiguration mit globalen Tabellen. (Die ACID-Konformität ist nur in einer einzigen Region möglich.) AWS

Einige mehrinstanzenfähige SaaS-Anwendungen haben möglicherweise einzigartige Datenmodelle oder besondere Umstände, die besser mit Datenbanken bedient werden können, die nicht in der vorherigen Tabelle enthalten sind. Beispielsweise können Zeitreihendatensätze, stark vernetzte Datensätze oder die Verwaltung eines zentralen Transaktionsbuchs die Verwendung eines anderen Datenbanktyps erforderlich machen. Die Analyse aller Möglichkeiten würde den Rahmen dieses Leitfadens sprengen. Eine umfassende Liste der AWS Datenbankangebote und wie sie verschiedene Anwendungsfälle auf hohem Niveau erfüllen können, finden Sie im Abschnitt Datenbank des Whitepapers Überblick über Amazon Web Services.

Der Rest dieses Handbuchs konzentriert sich auf AWS relationale Datenbankdienste, die PostgreSQL unterstützen: Amazon RDS und Aurora PostgreSQL-kompatibel. DynamoDB erfordert einen anderen Ansatz zur Optimierung für SaaS-Anwendungen, was den Rahmen dieses Handbuchs sprengen würde. Weitere Informationen zu DynamoDB finden Sie im AWS Blogbeitrag Partitioning Pooled Multi-Tenant SaaS Data with Amazon DynamoDB.

Wählen Sie zwischen Amazon RDS und Aurora

In den meisten Fällen empfehlen wir, Aurora PostgreSQL-kompatibel über Amazon RDS for PostgreSQL zu verwenden. Die folgende Tabelle zeigt die Faktoren, die Sie bei der Entscheidung zwischen diesen beiden Optionen berücksichtigen sollten.

DBMS-Komponente	Amazon RDS für PostgreSQL	Aurora PostgreSQL-kompatibel
Skalierbarkeit	Replikationsverzögerung von Minuten, maximal 5 Read Replicas	Replikationsverzögerung unter einer Minute (in der Regel weniger als 1 Sekunde bei globalen Datenbanken), maximal 15 Read Replicas
Wiederherstellung nach einem Absturz	Checkpoints im Abstand von 5 Minuten (standardmäßig) können die Datenbankleistung beeinträchtigen	Asynchrone Wiederherstellung mit parallel Threads für eine schnelle Wiederherstellung
Failover	60-120 Sekunden zusätzlich zur Wiederherstellungszeit nach einem Absturz	Normalerweise etwa 30 Sekunden (einschließlich Wiederherstellung nach einem Absturz)
Speicherung	Maximaler IOPS von 256.000	IOPS, die nur durch die Größe und Kapazität der Aurora-Instance eingeschränkt sind
Hohe Verfügbarkeit und Disaster Recovery	Zwei Availability Zones mit einer Standby-Instanz, regionsübergreifendem Failover zum Lesen von Replikaten oder kopierten Backups	Standardmäßig drei Availability Zones, regionsübergreifendes Failover mit globalen Aurora-Datenbanken, Schreibweiterleitung AWS-Regionen für Active-Active-Konfigurationen

DBMS-Komponente	Amazon RDS für PostgreSQL	Aurora PostgreSQL-kompatibel
Backup	Während des Backup-Fensters kann sich dies auf die Leistung auswirken	Automatische inkrementelle Backups, keine Auswirkungen auf die Leistung
Klassen von Datenbank-Instanzen	Liste der Amazon RDS-Instance-Klassen anzeigen	Liste der Aurora-Instanzklassen anzeigen

In allen in der vorherigen Tabelle beschriebenen Kategorien ist Aurora PostgreSQL-kompatibel normalerweise die bessere Option. Amazon RDS for PostgreSQL könnte jedoch für kleine bis mittlere Workloads immer noch sinnvoll sein, da es eine größere Auswahl an Instance-Klassen bietet, die auf Kosten des robusteren Funktionsumfangs von Aurora möglicherweise eine kostengünstigere Option darstellen.

Mehrmandantenfähige SaaS-Partitionierungsmodelle für PostgreSQL

Die beste Methode, um eine Mehrmandantenfähigkeit zu erreichen, hängt von den Anforderungen an Ihre SaaS-Anwendung ab. In den folgenden Abschnitten werden Partitionierungsmodelle für die erfolgreiche Implementierung von Multi-Tenancy in PostgreSQL demonstriert.

> **Note**
>
> Die in diesem Abschnitt beschriebenen Modelle gelten sowohl für Amazon RDS for PostgreSQL als auch für Aurora PostgreSQL-kompatibel. Verweise auf PostgreSQL in diesem Abschnitt gelten für beide Dienste.

Es gibt drei übergeordnete Modelle, die Sie in PostgreSQL für die SaaS-Partitionierung verwenden können: Silo, Bridge und Pool. Die folgende Abbildung fasst die Kompromisse zwischen den Silo- und Poolmodellen zusammen. Das Brückenmodell ist eine Mischung aus den Silo- und Poolmodellen.

Partitionierungsmodell	Vorteile	Nachteile
Silo	• Durchsetzung von Compliance-Standards • Keine mandantenübergreifenden Auswirkungen • Tuning auf Mandantenebene • Verfügbarkeit auf Mandantenebene	• kompromittierte Agilität • Keine zentrale Verwaltung • Komplexität der Bereitstellung • Kosten
Schwimmbecken	• Agilität • Kostenoptimierung • Zentralisiertes Management • Vereinfachter Einsatz	• Mandantenübergreifende Auswirkungen • Compliance-Herausforderungen

Partitionierungsmodell	Vorteile	Nachteile
		• Verfügbarkeit „Alles oder nichts“
Brücke	• Eine gewisse Compliance-Anpassung • Agilität • Kostenoptimierung • Zentralisiertes Management	• Einige Herausforderungen bei der Einhaltung von Vorschriften • Verfügbarkeit „Alles oder nichts“ (meistens) • Mandantenübergreifende Auswirkungen • Komplexität der Bereitstellung

In den folgenden Abschnitten werden die einzelnen Modelle ausführlicher behandelt.

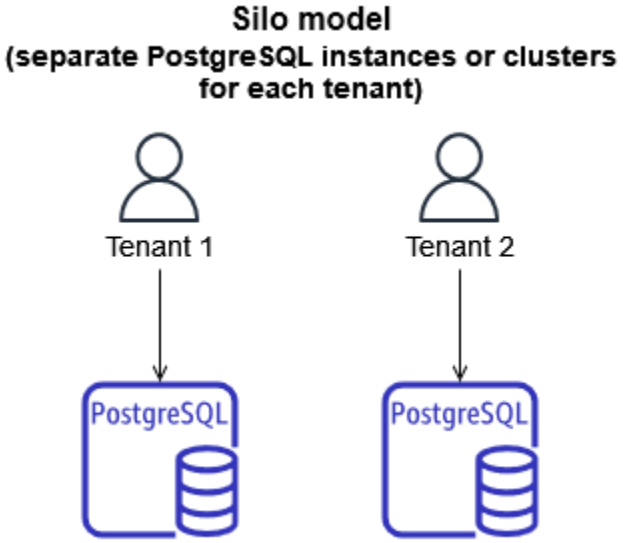
Partitionierungsmodelle:

- PostgreSQL-Silomodell
- PostgreSQL-Pool-Modell
- PostgreSQL-Bridge-Modell
- Entscheidungsmatrix

PostgreSQL-Silomodell

Das Silomodell wird implementiert, indem für jeden Mandanten in einer Anwendung eine PostgreSQL-Instanz bereitgestellt wird. Das Silomodell zeichnet sich durch die Leistung der Mieter und die Sicherheitsisolierung aus und eliminiert das Phänomen der lauten Nachbarn vollständig. Das Phänomen Noise Neighbor tritt auf, wenn die Nutzung eines Systems durch einen Mieter die Leistung eines anderen Mieters beeinträchtigt. Mit dem Silomodell können Sie die Leistung speziell auf jeden Mandanten zuschneiden und Ausfälle möglicherweise auf das Silo eines bestimmten Mandanten begrenzen. Was jedoch im Allgemeinen die Einführung eines Silomodells vorantreibt, sind strenge Sicherheits- und regulatorische Einschränkungen. Diese Einschränkungen können durch SaaS-Kunden motiviert werden. Beispielsweise könnten SaaS-Kunden aufgrund interner Einschränkungen

verlangen, dass ihre Daten isoliert werden, und SaaS-Anbieter könnten einen solchen Service gegen eine zusätzliche Gebühr anbieten.

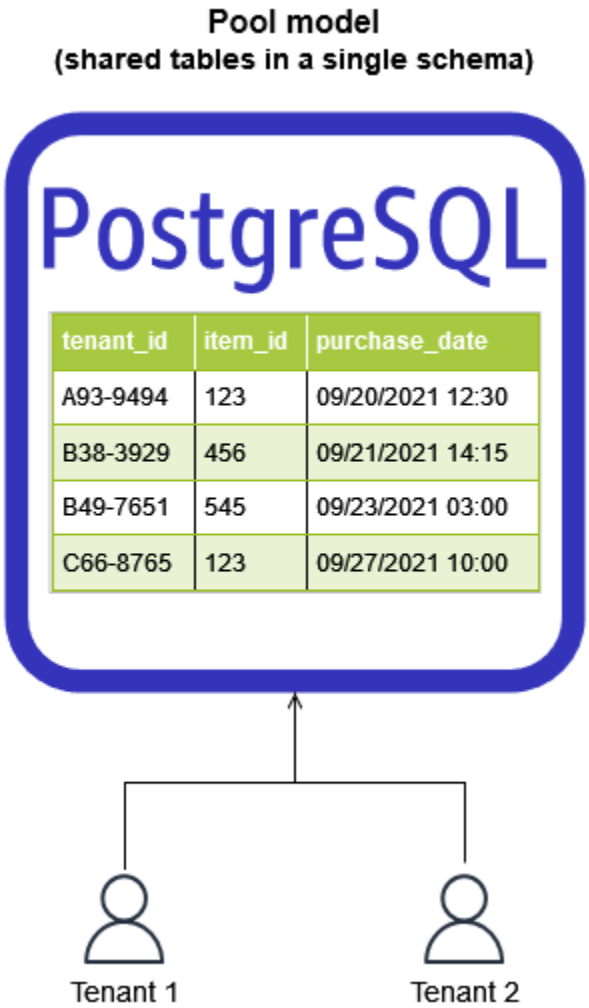


Obwohl das Silomodell in bestimmten Fällen notwendig sein kann, hat es viele Nachteile. Es ist oft schwierig, das Silomodell kostengünstig zu verwenden, da die Verwaltung des Ressourcenverbrauchs über mehrere PostgreSQL-Instanzen hinweg kompliziert sein kann. Darüber hinaus macht es die verteilte Natur der Datenbank-Workloads in diesem Modell schwieriger, einen zentralen Überblick über die Mandantenaktivitäten zu behalten. Die Verwaltung so vieler unabhängig betriebener Workloads erhöht den betrieblichen und administrativen Aufwand. Das Silomodell macht das Onboarding von Mandanten auch komplizierter und zeitaufwändiger, da Sie mandantenspezifische Ressourcen bereitstellen müssen. Darüber hinaus kann es schwieriger sein, das gesamte SaaS-System zu skalieren, da die ständig steigende Anzahl mandantenspezifischer PostgreSQL-Instanzen mehr Betriebszeit für die Verwaltung erfordern wird. Eine letzte Überlegung ist, dass eine Anwendung oder eine Datenzugriffsebene eine Zuordnung der Mandanten zu ihren zugeordneten PostgreSQL-Instanzen verwalten muss, was die Implementierung dieses Modells noch komplexer macht.

PostgreSQL-Pool-Modell

Das Poolmodell wird implementiert, indem eine einzelne PostgreSQL-Instance (Amazon RDS oder Aurora) bereitgestellt und Sicherheit auf Zeilenebene (RLS) verwendet wird, um die Isolierung der Mandantendaten aufrechtzuerhalten. RLS-Richtlinien schränken ein, welche Zeilen in einer Tabelle von`SELECT` Abfragen zurückgegeben werden oder welche Zeilen von`INSERTDELETE` Befehlen

beeinflusst werden.UPDATE Das Poolmodell zentralisiert alle Mandantendaten in einem einzigen PostgreSQL-Schema, sodass es deutlich kostengünstiger ist und weniger Betriebsaufwand für die Wartung erfordert. Die Überwachung dieser Lösung ist aufgrund ihrer Zentralisierung auch erheblich einfacher. Für die Überwachung der mieterspezifischen Auswirkungen im Poolmodell sind jedoch in der Regel zusätzliche Instrumente in der Anwendung erforderlich. Dies liegt daran, dass PostgreSQL standardmäßig nicht weiß, welcher Mandant Ressourcen verbraucht. Das Onboarding von Mandanten wird vereinfacht, da keine neue Infrastruktur erforderlich ist. Diese Agilität erleichtert die Durchführung schneller und automatisierter Workflows für das Onboarding von Mandanten.



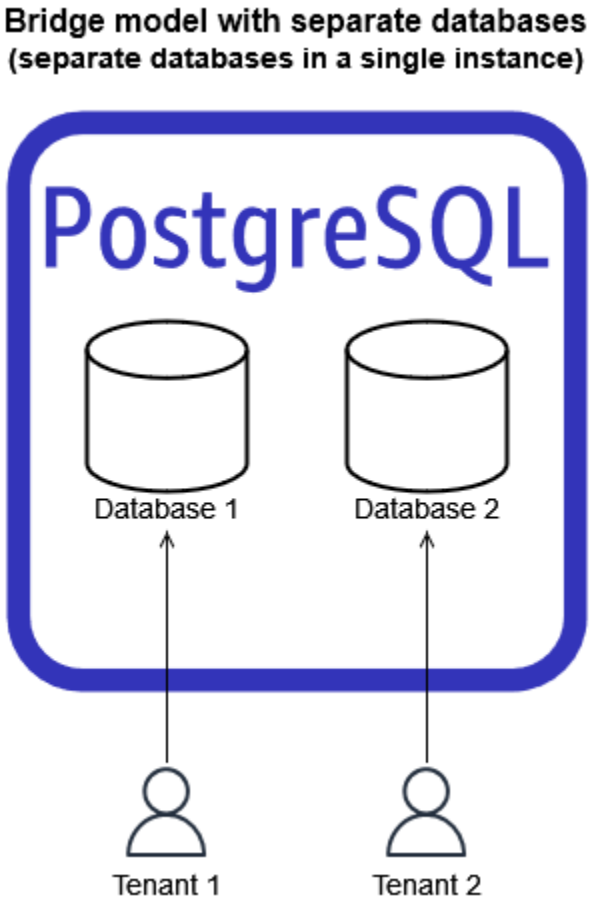
Obwohl das Poolmodell im Allgemeinen kostengünstiger und einfacher zu verwalten ist, hat es einige Nachteile. Das Phänomen der lauten Nachbarn kann in einem Poolmodell nicht vollständig ausgeschlossen werden. Dies kann jedoch eingedämmt werden, indem sichergestellt wird, dass die entsprechenden Ressourcen auf der PostgreSQL-Instanz verfügbar sind, und Strategien

zur Verringerung der Belastung in PostgreSQL eingesetzt werden, z. B. das Auslagern von Abfragen an Read Replicas oder an Amazon ElastiCache. Eine effektive Überwachung trägt auch dazu bei, Bedenken hinsichtlich der Isolierung der Mandantenleistung zu begegnen, da mit der Anwendungsinstrumentierung mandantenspezifische Aktivitäten protokolliert und überwacht werden können. Schließlich halten einige SaaS-Kunden die von RLS bereitgestellte logische Trennung möglicherweise nicht für ausreichend und fordern möglicherweise zusätzliche Isolationsmaßnahmen.

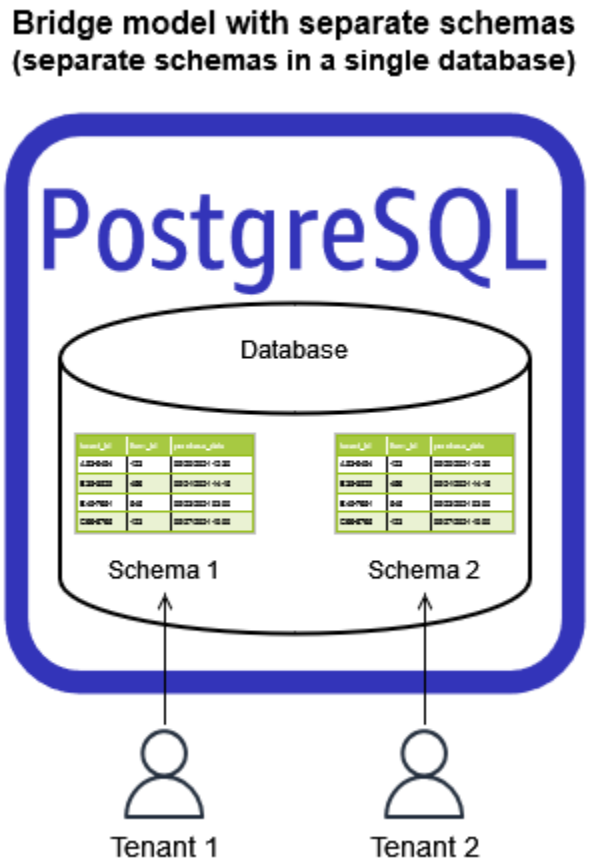
PostgreSQL-Bridge-Modell

Das PostgreSQL-Bridge-Modell ist eine Kombination aus gepoolten und isolierten Ansätzen. Wie beim Poolmodell stellen Sie für jeden Mandanten eine einzelne PostgreSQL-Instanz bereit. Um die Isolierung der Mandantendaten aufrechtzuerhalten, verwenden Sie logische PostgreSQL-Konstrukte. Im folgenden Diagramm werden PostgreSQL-Datenbanken verwendet, um Daten logisch zu trennen.

> **Note**
>
> Eine PostgreSQL-Datenbank bezieht sich nicht auf eine separate Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-kompatible DB-Instance. Stattdessen bezieht es sich auf ein logisches Konstrukt des PostgreSQL-Datenbankverwaltungssystems zur Trennung von Daten.



Sie können das Bridge-Modell auch implementieren, indem Sie eine einzelne PostgreSQL-Datenbank mit mandantenspezifischen Schemas in jeder Datenbank verwenden, wie in der folgenden Abbildung dargestellt.



Das Brückenmodell leidet unter den gleichen Bedenken hinsichtlich der Leistungsisolierung von Nachbarn und Mietern wie das Poolmodell. Es verursacht auch zusätzlichen Betriebs- und Bereitstellungsaufwand, da entweder separate Datenbanken oder Schemas pro Mandant bereitgestellt werden müssen. Es erfordert eine effektive Überwachung, um schnell auf Bedenken hinsichtlich der Mieterleistung reagieren zu können. Außerdem ist eine Anwendungsinstrumentierung erforderlich, um die mandantenspezifische Nutzung zu überwachen. Insgesamt kann das Bridge-Modell als Alternative zu RLS angesehen werden, das den Aufwand für das Onboarding von Mandanten leicht erhöht, da neue PostgreSQL-Datenbanken oder -Schemas erforderlich sind. Wie beim Silomodell muss eine Anwendung oder eine Datenzugriffsebene eine Zuordnung der Mandanten zu ihren zugehörigen PostgreSQL-Datenbanken oder -Schemas verwalten.

Entscheidungsmatrix

Um zu entscheiden, welches Multi-Tenant-SaaS-Partitionierungsmodell Sie mit PostgreSQL verwenden sollten, konsultieren Sie die folgende Entscheidungsmatrix. Die Matrix analysiert diese vier Partitionierungsoptionen:

- Silo — Eine separate PostgreSQL-Instanz oder ein eigener PostgreSQL-Cluster für jeden Mandanten.
- Bridge mit separaten Datenbanken — Eine separate Datenbank für jeden Mandanten in einer einzelnen PostgreSQL-Instanz oder einem einzelnen PostgreSQL-Cluster.
- Bridge mit separaten Schemas — Ein separates Schema für jeden Mandanten in einer einzelnen PostgreSQL-Datenbank, in einer einzelnen PostgreSQL-Instanz oder einem einzelnen PostgreSQL-Cluster.
- Pool — Gemeinsam genutzte Tabellen für Mandanten in einer einzigen Instanz und einem einzigen Schema.

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Anwendungsfall	Die Isolierung von Daten mit vollständiger Kontrolle über die Ressource nnutzung ist eine wichtige Anforderung, oder Sie haben sehr große und sehr leistungs empfindliche Mandanten.	Die Isolierung von Daten ist eine wichtige Anforderung, und es sind nur begrenzte oder keine Querverwe ise von Mieterdat en erforderlich.	Moderate Anzahl von Mietern mit einer moderaten Datenmeng e. Dies ist das bevorzugte Modell, wenn Sie die Daten von Mietern mit Querverwe isen versehen müssen.	Große Anzahl von Mietern mit weniger Daten pro Mandant.
Agilität beim Onboardin g neuer Mandanten	Sehr langsam. (Für jeden Mandanten ist eine neue Instanz oder ein neuer Cluster erforderlich.)	Mäßig langsam. (Erfordert das Erstellen einer neuen Datenbank für jeden Mandanten	Mäßig langsam. (Erfordert die Erstellung eines neuen Schemas für jeden Mandanten zum	Schnellst e Option. (Minimale Einrichtung ist erforderlich.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
		zum Speichern von Schemaobjekten.)	Speichern von Objekten.)	

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Aufwand und Effizienz bei der Konfiguration des Datenbank verbindungspools	Erheblicher Aufwand erforderlich. (Ein Verbindungspool pro Mandant.) Weniger effizient. (Keine gemeinsame Nutzung der Datenbank verbindung zwischen Mandanten.)	Erheblicher Aufwand erforderlich. (Eine Verbindungspoolkonfiguration pro Mandant, sofern Sie Amazon RDS Proxy nicht verwenden.) Weniger effizient. (Keine gemeinsame Nutzung der Datenbank verbindung zwischen Mandanten und Gesamtzahl der Verbindungen. Die Nutzung durch alle Mandanten ist je nach DB-Instance-Klasse begrenzt.)	Weniger Aufwand erforderlich. (Eine Verbindungspool-Konfiguration für alle Mandanten.) Mäßig effizient. (Wiederverwendung der Verbindung über den `SET SCHEMA` Befehl `SET ROLE` oder nur im Sitzungspool). `SET`Befehle führen bei der Verwendung von Amazon RDS Proxy auch zu Sitzungs-Pinning, aber die Client-Verbindungspools können entfernt werden und direkte Verbindungen können für jede Anforderung aus Effizienzgründen	Geringster Aufwand erforderlich. Am effizientesten. (Ein Verbindungspool für alle Mandanten und effiziente Wiederverwendung von Verbindungen für alle Mandanten. Die Datenbank verbindungslimits für Datenbankverbindungen basieren auf der DB-Instance-Klasse.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
			hergestellt werden.)	
Datenbankpflege (Vakuummanagement) und Ressourcennutzung	Einfachere Verwaltung.	Mittlere Komplexität. (Könnte zu einem hohen Ressourcenverbrauch führen, da danach für jede Datenbank ein Vakuumarbeiter gestartet werden muss `vacuum_naptime`, was zu einer hohen CPU-Auslastung des Autovacuum-Launchers führt. Möglicherweise ist mit dem Löschen der PostgreSQL-Systemkatalogtabellen für jede Datenbank zusätzlicher Aufwand verbunden.)	Große PostgreSQL-Systemkatalogtabellen (`pg_catalog` Gesamtgröße in mehreren zehn GB, abhängig von der Anzahl der Mieter und Beziehungen. Wahrscheinlich sind Änderungen an den staubsaugenden Parametern erforderlich, um das Aufblähen des Tisches zu kontrollieren.)	Die Tabellen können je nach Anzahl der Mandanten und Daten pro Mandant umfangreich sein. (Wahrscheinlich sind Änderungen an den staubsaugenden Parametern erforderlich, um das Aufblähen des Tisches zu verhindern.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Aufwand für die Verwaltung von Erweiterungen	Erheblicher Aufwand (für jede Datenbank in separaten Instanzen).	Erheblicher Aufwand (auf jeder Datenbank ebene).	Minimaler Aufwand (einmalig in der gemeinsamen Datenbank).	Minimaler Aufwand (einmalig in der gemeinsamen Datenbank).
Bereitste llungsaufwand ändern	erhebliche Anstrengungen. (Connect zu jeder einzelnen Instance her und führen Sie die Änderungen durch.)	erhebliche Anstrengungen. (Connect zu jeder Datenbank und jedem Schema her und führen Sie Änderungen durch.)	Mäßiger Aufwand. (Connect zu einer gemeinsam en Datenbank her und führen Sie Änderunge n für jedes Schema durch.)	Minimaler Aufwand. (Connect zu einer gemeinsam en Datenbank her und führen Sie Änderungen durch.)
Einsatz von Änderungen — Umfang der Auswirkungen	Minimal. (Einzelner Mieter betroffen.)	Minimal. (Einzelner Mieter betroffen.)	Minimal. (Einzelner Mieter betroffen.)	Sehr groß. (Alle Mieter betroffen.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Leistungsmanagement und Aufwand abfragen	Verwaltbare Abfrageleistung	Verwaltbare Abfrageleistung	Verwaltbare Abfrageleistung	Es ist wahrscheinlich ein erheblicher Aufwand erforderlich, um die Abfrageleistung aufrechtzuerhalten. (Im Laufe der Zeit können Abfragen aufgrund der zunehmenden Größe der Tabellen langsamer ausgeführt werden. Sie können Tabellenpartitionierung und Datenbank-Sharding verwenden, um die Leistung aufrechtzuerhalten.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Auswirkungen auf mandanten übergreifende Ressourcen	Keine Auswirkungen. (Keine gemeinsame Nutzung von Ressourcen zwischen den Mietern.)	Mäßige Auswirkungen. (Mandanten nutzen gemeinsame Ressourcen wie Instanz-CPU und Arbeitsspeicher.)	Mäßige Auswirkungen. (Mandanten nutzen gemeinsame Ressourcen wie Instanz-CPU und Arbeitsspeicher.)	Starke Auswirkungen. (Mieter beeinflussen sich gegenseitig in Bezug auf Ressourcen, Blockkonflikte usw.)
Tuning auf Mandanten ebene (z. B. Erstellung zusätzlicher Indizes pro Mandant oder Optimierung von DB-Parametern für einen bestimmten Mandanten)	Mögliche.	Das ist möglich. (Änderungen auf Schemaebene können für jeden Mandanten vorgenommen werden, aber die Datenbankparameter sind global für alle Mandanten.)	Das ist möglich. (Änderungen auf Schemaebene können für jeden Mandanten vorgenommen werden, aber die Datenbankparameter sind global für alle Mandanten.)	Das ist möglich. (Die Tische werden von allen Mietern gemeinsam genutzt.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Den Aufwand für leistungssensible Mieter wieder ins Gleichgewicht bringen	Minimal. (Sie müssen das Gleichgew icht nicht neu ausbalancieren. Skalieren Sie Server- und I/O-Ressourcen, um dieses Szenario zu bewältigen.)	Mäßig. (Verwenden Sie die logische Replikation oderpg_dump um die Datenbank zu exportieren, aber die Ausfallze iten können je nach Datengröß e langwierig sein. Sie können die Funktion für transportable Datenbanken in Amazon RDS for PostgreSQ L verwenden, um Datenbank en schneller zwischen Instanzen zu kopieren.)	Mäßig, aber wahrscheinlich mit langen Ausfallzeiten verbunden. (Verwenden Sie die logische Replikation oderpg_dump um das Schema zu exportier en, aber die Ausfallzeiten können je nach Datengröße langwierig sein.)	Signifikant, da sich alle Mieter dieselben Tische teilen. (Die gemeinsame Nutzung der Datenbank erfordert das Kopieren aller Daten auf eine andere Instanz und einen zusätzlic hen Schritt zur Bereinigung der Mandanten daten.) Erfordert höchstwah rscheinlich eine Änderung der Anwendung slogik.

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Datenbank ausfälle für signifikante Upgrades von Hauptversionen	Standarda usfallzeiten. (Hängt von der Größe des PostgreSQL-Systemkatalogs ab.)	Längere Ausfallzeiten wahrscheinlich. (Je nach Größe des Systemkatalogs variiert die Zeit. PostgreSQL-Systemkatalogtabellen werden auch datenbank übergreifend dupliziert.	Längere Ausfallzeiten wahrscheinlich. (Abhängig von der Größe des PostgreSQL-Systemkatalogs variiert die Zeit.)	Standarda usfallzeiten. (Hängt von der Größe des PostgreSQL-Systemkatalogs ab.)
Administrationsaufwand (z. B. für die Analyse von Datenbank protokollen oder die Überwachung von Backup-Jobs)	Erheblicher Aufwand	Minimaler Aufwand.	Minimaler Aufwand.	Minimaler Aufwand.

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Verfügbarkeit auf Mandantenebene	Höchster. (Jeder Mandant schlägt fehl und erholt sich selbstständig.)	Höherer Wirkungsbereich. (Bei Hardware- oder Ressourcenproblemen fallen alle Mandanten zusammen aus und erholen sich gemeinsam.)	Höherer Wirkungsbereich. (Bei Hardware- oder Ressourcenproblemen fallen alle Mandanten zusammen aus und erholen sich gemeinsam.)	Höherer Wirkungsbereich. (Bei Hardware- oder Ressourcenproblemen fallen alle Mandanten zusammen aus und erholen sich gemeinsam.)
Backup- und Recovery-Aufwand auf Mandantenebene	Der geringste Aufwand. (Jeder Mandanten kann unabhängig gesichert und wiederhergestellt werden.)	Mäßiger Aufwand. (Verwenden Sie den logischen Export und Import für jeden Mandanten. Etwas Codierung und Automatisierung sind erforderlich.)	Mäßiger Aufwand. (Verwenden Sie den logischen Export und Import für jeden Mandanten. Etwas Codierung und Automatisierung sind erforderlich.)	erhebliche Anstrengungen. (Alle Mieter teilen sich dieselben Tische.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
point-in-time Wiederherstellungsmaßnahmen auf Mieterebene	Minimaler Aufwand. (Verwenden Sie die Point-in-Zeitwiederherstellung mithilfe von Snapshots oder verwenden Sie Backtracking in Amazon Aurora.)	Mäßiger Aufwand. (Verwenden Sie Snapshot-Wiederherstellung, gefolgt von Export/Import. Dies wird jedoch ein langsamer Vorgang sein.)	Mäßiger Aufwand. (Verwenden Sie Snapshot-Wiederherstellung, gefolgt von Export/Import. Dies wird jedoch ein langsamer Vorgang sein.)	Erheblicher Aufwand und Komplexität.
Einheitlicher Schemaname	Derselbe Schemaname für jeden Mandanten.	Derselbe Schemaname für jeden Mandanten.	Verschiedene Schemas für jeden Mandanten	Gängige Schemata.
Anpassung pro Mandant (z. B. zusätzliche Tabellenspalten für einen bestimmten Mandanten)	Mögliche.	Mögliche.	Mögliche.	Kompliziert (weil sich alle Mieter dieselben Tische teilen).

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Effizienz der Katalogverwaltung auf der Ebene der objektrelationalen Zuordnung (ORM) (z. B. Ruby)	Effizient (weil die Client-Verbindung mandanten spezifisch ist).	Effizient (weil die Client-Verbindung spezifisch für eine Datenbank ist).	Mäßig effizient. (Abhängig vom verwendeten ORM, dem Benutzer-/Rollensicherheitsmodell und der `search_path` Konfiguration speichert der Client manchmal die Metadaten für alle Mandanten im Cache, was zu einer hohen Speichernutzung der DB-Verbindung führt.)	Effizient (weil sich alle Mieter dieselben Tische teilen).

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Konsolidierter Aufwand zur Berichterstattung von Mietern	erhebliche Anstrengungen. (Sie müssen Foreign Data Wrapper [FDWs] verwenden, um Daten in allen Mandanten zu konsolidieren oder [ETL] zu extrahieren, zu transformieren und in eine andere Berichtsdatenbank zu laden.)	erhebliche Anstrengungen. (Sie müssen FDWs verwenden, um Daten in allen Mandanten oder ETL in einer anderen Berichtsdatenbank zu konsolidieren.)	Mäßiger Aufwand. (Sie können Daten in allen Schemas aggregieren, indem Sie Unionen verwenden.)	Minimaler Aufwand. (Alle Mandantendaten befinden sich in denselben Tabellen, sodass die Berichterstattung einfach ist.)
Mandanten spezifische schreibgeschützte Instanz für Berichte (z. B. basierend auf einem Abonnement)	Der geringste Aufwand. (Erstellen eines Lesereplikats.)	Mäßiger Aufwand. (Sie können die logische Replikation oder denAWS Database Migration Service [AWS DMS] zur Konfiguration verwenden.)	Mäßiger Aufwand. (Sie können die logische Replikation verwenden oderAWS DMS konfigurieren.)	Kompliziert (weil sich alle Mieter dieselben Tische teilen).

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Datenisolierung	Am besten.	Besser. (Sie können Berechtigungen auf Datenbankebene mithilfe von PostgreSQL-Rollen verwalten.)	Besser. (Sie können Berechtigungen auf Schemaebene mithilfe von PostgreSQL-Rollen verwalten.)	Schlimmer. (Da alle Mandanten dieselben Tabellen verwenden, müssen Sie Funktionen wie Sicherheit auf Zeilenebene [RLS] zur Mandantenisolierung implementieren.)
Mandantenspezifischer Speicherverschlüsselungsschlüssel	Mögliche. (Jeder PostgreSQL-Cluster kann seinen eigenenAWS Key Management Service [AWS KMS] Schlüssel für die Speicherverschlüsselung haben.)	Das ist möglich. (Alle Mandanten verwenden denselben KMS-Schlüssel für die Speicherverschlüsselung.)	Das ist möglich. (Alle Mandanten verwenden denselben KMS-Schlüssel für die Speicherverschlüsselung.)	Das ist möglich. (Alle Mandanten verwenden denselben KMS-Schlüssel für die Speicherverschlüsselung.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Verwendung vonAWS Identity and Access Managemen t (IAM) für die Datenbank authentifizierung für jeden Mandanten	Mögliche.	Mögliche.	Möglich (indem separate PostgreSQL-Benutzer für jedes Schema vorhanden sind).	Nicht möglich (weil die Tische von allen Mietern gemeinsam genutzt werden).
Kosten für die Infrastruktur	Am höchsten (weil nichts geteilt wird).	Mäßig.	Mäßig.	Am wenigsten.
Datendupl izierung und Speichernutzung	Höchstes Aggregat für alle Mieter. (Die PostgreSQ L-Systemk atalogtab ellen und die statischen und gemeinsam en Daten der Anwendung werden für alle Mandanten dupliziert.)	Höchstes Aggregat für alle Mieter. (Die PostgreSQ L-Systemk atalogtab ellen und die statischen und gemeinsam en Daten der Anwendung werden für alle Mandanten dupliziert.)	Mäßig. (Die statischen und gemeinsam en Daten der Anwendung können sich in einem gemeinsam en Schema befinden und von anderen Mandanten abgerufen werden.)	Minimal. (Keine Vervielfältigung von Daten. Die statischen und allgemein en Daten der Anwendung können sich im selben Schema befinden.)

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Mandanten orientiertes Monitoring (finden Sie schnell heraus, welcher Mandant Probleme verursacht)	Der geringste Aufwand. (Da jeder Mandant separat überwacht wird, ist es einfach, die Aktivität eines bestimmten Mandanten zu überprüfen.)	Mäßiger Aufwand. (Da sich alle Mandanten dieselbe physische Ressource teilen, müssen Sie zusätzliche Filter anwenden, um die Aktivität eines bestimmten Mandanten zu überprüfen.)	Mäßiger Aufwand. (Da sich alle Mandanten dieselbe physische Ressource teilen, müssen Sie zusätzliche Filter anwenden, um die Aktivität eines bestimmten Mandanten zu überprüfen.)	erhebliche Anstrengungen. (Da alle Mandanten alle Ressourcen, einschließlich Tabellen, gemeinsam nutzen, müssen Sie die Bind-Variablenerfassung verwenden, um zu überprüfen, zu welchem Mandanten eine bestimmte SQL-Abfrage gehört.)
Zentrales Management und Gesundheits- und Aktivitätsüberwachung	Erheblicher Aufwand (Einrichtung einer zentralen Überwachung und einer zentralen Kommandozentrale).	Mäßiger Aufwand (weil sich alle Mieter dieselbe Instanz teilen).	Mäßiger Aufwand (weil sich alle Mieter dieselbe Instanz teilen).	Minimaler Aufwand (da sich alle Mandanten dieselben Ressourcen teilen, einschließlich des Schemas).

	Silo	Brücke mit separaten Datenbanken	Brücke mit separaten Schemata	Schwimmbecken
Wahrscheinlichkeit, dass Object Identifier (OID) und Transaktions-ID (XID) Wraparound	Minimal.	Hoch. (Da es sich bei OID um einen einzelnen clusterweiten PostgreSQL-Zähler handelt, kann es zu Problemen bei der effektiven Datenabsaugung zwischen physischen Datenbanken kommen).	Mäßig. (Weil OID, XID ein einzelner clusterweiter PostgreSQL-Zähler ist).	Hoch. (Beispielsweise kann eine einzelne Tabelle je nach Anzahl der out-of-line Spalten das TOAST-OID-Limit von 4 Milliarden erreichen.)

Empfehlungen auf der Sicherheit auf Zeilenebene.

Sicherheit auf Zeilenebene (RLS) ist erforderlich, um die Isolierung von Mandantendaten in einem Poolmodell mit PostgreSQL aufrechtzuerhalten. RLS zentralisiert die Durchsetzung von Isolationsrichtlinien auf Datenbankebene und entlastet Softwareentwicklern die Last, diese Isolierung aufrechtzuerhalten. Die gebräuchlichste Methode zur Implementierung von RLS besteht darin, diese Funktion im PostgreSQL-DBMS zu aktivieren. RLS beinhaltet das Filtern des Zugriffs auf Datenzeilen auf der Grundlage eines Werts in einer bestimmten Spalte. Sie können zwei Methoden verwenden, um den Zugriff auf Daten zu filtern:

- Eine angegebene Datenspalte in einer Tabelle wird mit dem Wert des aktuellen PostgreSQL-Benutzers verglichen. Werte in der Spalte, die dem angemeldeten PostgreSQL-Benutzer entsprechen, sind für diesen Benutzer zugänglich.
- Eine angegebene Datenspalte in einer Tabelle wird mit dem Wert einer von der Anwendung festgelegten Laufzeitvariablen verglichen. Auf Werte in der Spalte, die der Laufzeitvariablen entsprechen, kann während dieser Sitzung zugegriffen werden.

Die zweite Option wird bevorzugt, da für die erste Option die Erstellung eines neuen PostgreSQL-Benutzers für jeden Mandanten erforderlich ist. Stattdessen sollte eine SaaS-Anwendung, die PostgreSQL verwendet, dafür verantwortlich sein, zur Laufzeit einen mandantenspezifischen Kontext festzulegen, wenn sie PostgreSQL abfragt. Dies wird dazu führen, dass RLS durchgesetzt wird. Sie können RLS auch auf einer table-by-table Basis aktivieren. Als bewährte Methode sollten Sie RLS für alle Tabellen aktivieren, die Mandantendaten enthalten.

Das folgende Beispiel erstellt zwei Tabellen und aktiviert RLS. In diesem Beispiel wird eine Datenspalte mit dem Wert der Laufzeitvariablen verglichen`app.current_tenant`.

```
-- Create a table for our tenants with indexes on the primary key and the tenant’s name
CREATE TABLE tenant (
    tenant_id UUID DEFAULT uuid_generate_v4() PRIMARY KEY,
    name VARCHAR(255) UNIQUE,
    status VARCHAR(64) CHECK (status IN ('active', 'suspended', 'disabled')),
    tier VARCHAR(64) CHECK (tier IN ('gold', 'silver', 'bronze'))
);

-- Create a table for users of a tenant
CREATE TABLE tenant_user (
```

```
    user_id UUID DEFAULT uuid_generate_v4() PRIMARY KEY,
    tenant_id UUID NOT NULL REFERENCES tenant (tenant_id) ON DELETE RESTRICT,
    email VARCHAR(255) NOT NULL UNIQUE,
    given_name VARCHAR(255) NOT NULL CHECK (given_name <> ''),
    family_name VARCHAR(255) NOT NULL CHECK (family_name <> '')
);

-- Turn on RLS
ALTER TABLE tenant ENABLE ROW LEVEL SECURITY;

-- Restrict read and write actions so tenants can only see their rows
-- Cast the UUID value in tenant_id to match the type current_setting
-- This policy implies a WITH CHECK that matches the USING clause
CREATE POLICY tenant_isolation_policy ON tenant
USING (tenant_id = current_setting('app.current_tenant')::UUID);

-- And do the same for the tenant users
ALTER TABLE tenant_user ENABLE ROW LEVEL SECURITY;

CREATE POLICY tenant_user_isolation_policy ON tenant_user
USING (tenant_id = current_setting('app.current_tenant')::UUID);
```

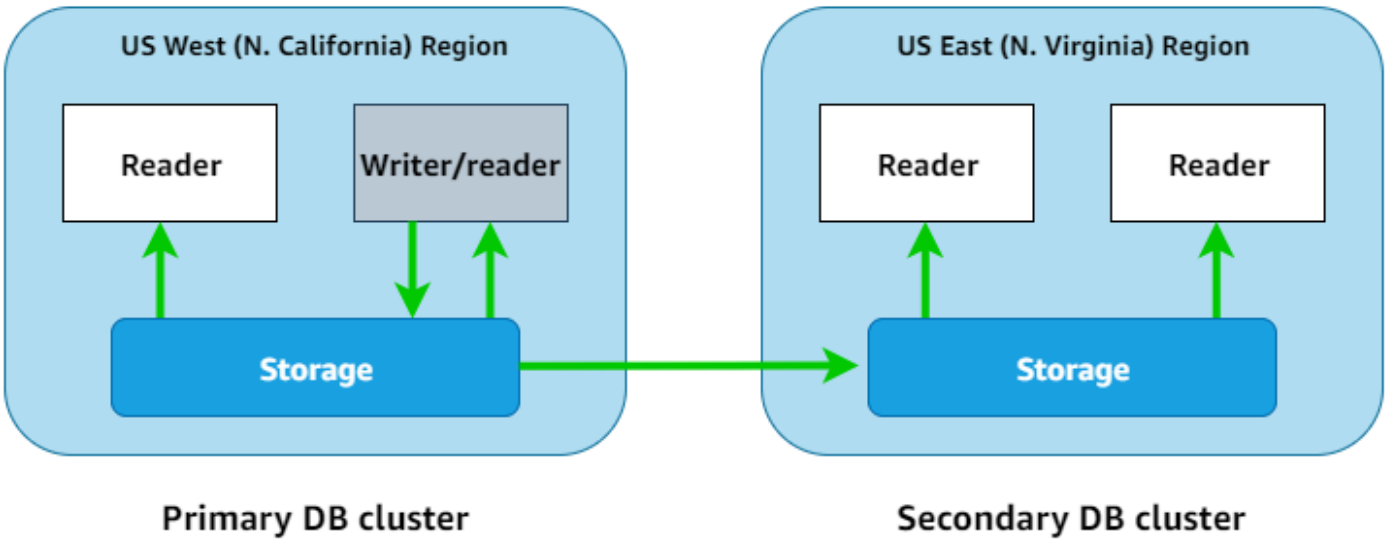
Weitere Informationen finden Sie in diesem Blogbeitrag: Multi-Tenant Data Isolation with PostgreSQL Row Level Security. DasAWS SaaS Factory-Team hat auch einige Beispiele GitHub, die bei der Implementierung von RLS helfen sollen.

PostgreSQL-Verfügbarkeit für das Poolmodell

Poolmodelle haben naturgemäß nur eine einzige PostgreSQL-Instanz. Daher ist es von entscheidender Bedeutung, Ihre Anwendung für hohe Verfügbarkeit zu entwerfen. Ein Ausfall oder Ausfall einer gepoolten Datenbank führt dazu, dass Ihre Anwendung beeinträchtigt wird oder für alle Ihre Mandanten nicht mehr zugänglich ist.

Amazon RDS for PostgreSQL PostgreSQL-DB-Instances können über zwei Availability Zones hinweg redundant gemacht werden, indem die Hochverfügbarkeitsfunktion aktiviert wird. Weitere Informationen finden Sie unter Hochverfügbarkeit (Multi-AZ) für Amazon RDS in der Amazon RDS-Dokumentation. Für ein regionsübergreifendes Failover können Sie eine Read Replica in einer anderen Region erstellen. AWS (Diese Read Replica muss im Rahmen eines Failover-Prozesses heraufgestuft werden.) Darüber hinaus können Sie für die Wiederherstellung regionsübergreifend AWS replizierte Backups replizieren. Weitere Informationen finden Sie unter Automatisierte Backups in eine andere AWS Region replizieren in der Amazon RDS-Dokumentation.

Aurora PostgreSQL-kompatibel sichert Daten automatisch auf eine Weise, die den Ausfall mehrerer Availability Zones aushält. (Weitere Informationen finden Sie unter Hochverfügbarkeit für Amazon Aurora in der Aurora-Dokumentation.) Um Aurora widerstandsfähiger zu machen und die Wiederherstellung zu beschleunigen, können Sie Aurora-Read Replicas in anderen Availability Zones erstellen. Sie können die globalen Aurora-Datenbanken verwenden, um Daten in fünf weitere AWS Regionen zu replizieren, um eine regionsübergreifende Wiederherstellung und einen automatischen Failover zu ermöglichen. (Siehe Verwenden globaler Amazon Aurora Aurora-Datenbanken in der Aurora-Dokumentation.) Darüber hinaus können Sie die Schreibweiterleitung mit globalen Aurora-Datenbanken aktivieren, um eine hohe Verfügbarkeit über mehrere Datenbanken hinweg zu erreichen AWS-Regionen.



Unabhängig davon, ob Sie Amazon RDS for PostgreSQL oder Aurora PostgreSQL-kompatibel verwenden, empfehlen wir Ihnen, Hochverfügbarkeitsfunktionen zu implementieren, um die Auswirkungen von Ausfällen für alle mehrinstanzenfähigen SaaS-Anwendungen, die ein Poolmodell verwenden, zu minimieren.

Bewährte Methoden

In diesem Abschnitt werden einige der wichtigsten Erkenntnisse aus diesem Leitfaden aufgeführt. Für ausführliche Diskussionen zu jedem Punkt folgen Sie den Links zu den entsprechenden Abschnitten.

AWSOptionen für verwaltetes PostgreSQL vergleichen

AWSbietet zwei Hauptmethoden, um PostgreSQL in einer verwalteten Umgebung auszuführen. (In diesem Zusammenhang bedeutet verwaltet, dass die PostgreSQL-Infrastruktur und das DBMS teilweise oder vollständig von einemAWS Dienst unterstützt werden.) Verwaltete PostgreSQL-OptionenAWS bieten den Vorteil, dass Backups, Failover, Optimierung und einige Verwaltungsaufgaben von PostgreSQL automatisiert werden. Als verwaltete OptionenAWS bietet Amazon Aurora PostgreSQL-kompatible Edition und Amazon Relational Database Service (Amazon RDS) für PostgreSQL. Sie können aus diesen beiden Modellen die beste Wahl auswählen, indem Sie Ihren PostgreSQL-Anwendungsfall analysieren. Weitere Informationen finden Sie im Abschnitt Wählen zwischen Amazon RDS und Aurora in dieser Anleitung.

Wählen Sie ein mehrmandantenfähiges SaaS-Partitionierungsmodell

Sie können aus drei SaaS-Partitionierungsmodellen wählen, die für PostgreSQL geeignet sind: Silo, Bridge und Pool. Jedes Modell hat Vor- und Nachteile, und Sie sollten je nach Anwendungsfall das optimale Modell wählen. Amazon RDS for PostgreSQL und Aurora PostgreSQL-kompatibel unterstützen alle drei Modelle. Die Wahl eines Modells ist entscheidend, um die Isolierung der Mandantendaten in Ihren SaaS-Anwendungen aufrechtzuerhalten. Eine ausführliche Beschreibung dieser Modelle finden Sie im Abschnitt Multi-Tenant-SaaS-Partitionierungsmodelle für PostgreSQL in diesem Handbuch.

Verwenden Sie Sicherheit auf Zeilenebene für Pool-SaaS-Partitionierungsmodelle

Sicherheit auf Zeilenebene (RLS) ist erforderlich, um die Isolierung von Mandantendaten in einem Poolmodell mit PostgreSQL aufrechtzuerhalten. Dies liegt daran, dass es in einem Poolmodell keine logische Trennung zwischen Infrastruktur, PostgreSQL-Datenbanken oder

Schemas auf Mandantenbasis gibt. RLS zentralisiert die Durchsetzung von Isolationsrichtlinien auf Datenbankebene und entlastet Softwareentwicklern die Last, diese Isolierung aufrechtzuerhalten. Sie können RLS verwenden, um Datenbankoperationen auf einen bestimmten Mandanten zu beschränken. Weitere Informationen und ein Beispiel finden Sie im Abschnitt Sicherheitsempfehlungen auf Zeilenebene in dieser Anleitung.

Häufig gestellte Fragen

Dieser Abschnitt enthält Antworten auf häufig gestellte Fragen zur Implementierung von Managed PostgreSQL in mehrmandantenfähigen SaaS-Anwendungen.

Welche verwalteten PostgreSQL-OptionenAWS bietet es?

AWSbietet Amazon Aurora PostgreSQL-kompatibel und Amazon Relational Database Service (Amazon RDS) für PostgreSQL. AWSverfügt auch über einen breiten Katalog an verwalteten Datenbankangeboten.

Welcher Service ist optimal für SaaS-Anwendungen?

Sie können sowohl Aurora PostgreSQL-Compatible als auch Amazon RDS for PostgreSQL für SaaS-Anwendungen sowie alle in diesem Handbuch beschriebenen SaaS-Partitionierungsmodelle verwenden. Diese beiden Dienste unterscheiden sich in Bezug auf Skalierbarkeit, Crash Recovery, Failover, Speicheroptionen, Hochverfügbarkeit, Disaster Recovery, Backup und die für jede Option verfügbaren Instanzklassen. Die optimale Wahl hängt vom speziellen Anwendungsfall ab. Verwenden Sie die Entscheidungsmatrix in diesem Handbuch, um die beste Option für Ihren Anwendungsfall auszuwählen.

Welche besonderen Anforderungen sollte ich berücksichtigen, wenn ich mich für die Verwendung einer PostgreSQL-Datenbank mit einer mehrmandantenfähigen SaaS-Anwendung entscheide?

Wie bei jedem Datenspeicher, der mit einer SaaS-Anwendung verwendet wird, ist die Methode zur Aufrechterhaltung der Isolierung von Mandantendaten die wichtigste Überlegung. Wie in diesem Handbuch beschrieben, gibt es mehrere Möglichkeiten, die Isolierung von Mandantendaten mitAWS verwalteten PostgreSQL-Angeboten zu erreichen. Darüber hinaus sollten Sie für alle PostgreSQL-Implementierungen eine Leistungsisolierung auf Mandantenbasis in Betracht ziehen.

Welche Modelle kann ich verwenden, um die Isolierung von Mandantendaten mit PostgreSQL aufrechtzuerhalten?

Sie können die Silo-, Bridge- und Poolmodelle als SaaS-Partitionierungsstrategien verwenden, um die Isolierung der Mandantendaten aufrechtzuerhalten. Eine Erläuterung dieser Modelle und ihrer Anwendung auf PostgreSQL finden Sie im Abschnitt Multi-Tenant-SaaS-Partitionierungsmodelle für PostgreSQL in diesem Handbuch.

Wie kann ich die Isolierung der Mandantendaten mit einer einzigen PostgreSQL-Datenbank aufrechterhalten, die von mehreren Mandanten gemeinsam genutzt wird?

PostgreSQL unterstützt eine Sicherheitsfunktion auf Zeilenebene (RLS), mit der Sie die Isolierung von Mandantendaten in einer einzelnen PostgreSQL-Datenbank oder -Instanz erzwingen können. Darüber hinaus können Sie separate PostgreSQL-Datenbanken pro Mandant in einer einzigen Instanz bereitstellen oder Schemas auf Mandantenbasis erstellen, um dieses Ziel zu erreichen. Die Vor- und Nachteile dieser Ansätze finden Sie im Abschnitt Sicherheitsempfehlungen auf Zeilenebene in diesem Handbuch.

Nächste Schritte

AWSbietet zwei Optionen für den Betrieb von verwaltetem PostgreSQL: Aurora PostgreSQL-kompatibel und Amazon RDS for PostgreSQL. Wir empfehlen Ihnen, die beiden Dienste zu testen und die Option auszuwählen, die Ihren spezifischen Anwendungsfall für Ihre mehrmandantenfähigen SaaS-Anwendungen am besten unterstützt. Durch die Einhaltung eines SaaS-Partitionierungsmodells kann sichergestellt werden, dass eine SaaS-Anwendung, die PostgreSQL verwendet, sich strikt an bewährte Verfahren zur Aufrechterhaltung der Mandantenfähigkeit hält. Die SaaS-Silo-, Bridge- und Pool-Partitionierungsmodelle unterstützen viele SaaS-Anwendungsfälle. Diese Modelle bieten unterschiedliche Vorteile zwischen Faktoren wie Leistungsisolierung, Betriebsaufwand und Mandantensicherheit.

Nächste Schritte:

- Testen Sie Aurora PostgreSQL-Compatible und Amazon RDS for PostgreSQL und wählen Sie die beste Option für Ihre SaaS-Anwendung.
- Wählen Sie ein SaaS-Partitionierungsmodell, das die Anforderungen für Ihre Anwendung erfüllt: Silo, Bridge oder Pool.
- Implementieren Sie PostgreSQL gemäß Ihrem ausgewählten SaaS-Partitionierungsmodell.

Ressourcen

Referenzen

- SaaS-Speicherstrategien: Erstellen eines Multi-Tenant-Speichermodells auf AWS (AWS-Whitepaper)
- Regionsübergreifende Notfallwiederherstellung mit Amazon Aurora Global Database für Amazon Aurora PostgreSQL (-Blogbeitrag)AWS
- Datenisolierung auf Zeilenebene mit PostgreSQL (AWS-Blogbeitrag)
- Arbeiten mit Amazon Aurora PostgreSQL (Aurora-Dokumentation)
- PostgreSQL in Amazon RDS (Amazon-RDS-Dokumentation)

Partner

- Partner von Amazon Aurora für PostgreSQL
- Partner von Amazon RDS für PostgreSQL

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
Aktualisieren	Aktualisierungen, um die Verfügbarkeit der Schreibweiterleitung in Aurora widerzuspiegeln.	29. April 2024
Aktualisieren	Die Vergleichstabelle von Amazon RDS und Aurora wurde aktualisiert.	21. Oktober 2022
—	Erste Veröffentlichung	30. September 2021

AWS Glossar zu präskriptiven Leitlinien

Im Folgenden finden Sie häufig verwendete Begriffe in Strategien, Leitfäden und Mustern, die von Prescriptive Guidance bereitgestellt AWS 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:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre On-Premises-Oracle-Datenbank zu der PostgreSQL-kompatible Amazon-Aurora-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 CRM-System (Customer Relationship Management) 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 auf einer EC2-Instance in der Cloud zu Oracle. AWS
- 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. Dieses Migrationsszenario ist spezifisch für VMware Cloud on AWS, das die Kompatibilität mit virtuellen Maschinen (VM) und die Workload-Portabilität zwischen Ihrer lokalen Umgebung und unterstützt. AWS Sie können die VMware-Cloud-Foundation-Technologien von Ihren On-Premises-Rechenzentren aus verwenden, wenn Sie

Ihre Infrastruktur zu VMware Cloud in AWS migrieren. Beispiel: Verlagern Sie den Hypervisor, der Ihre Oracle-Datenbank hostet, zu VMware Cloud on. 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

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 Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

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.

Blau/Grün-Bereitstellung

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 unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

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 Framework für die AWS 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.

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 normalerweise durchlaufen, wenn sie zur AWS Cloud migrieren:

- 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
- Neuentwicklung – Optimierung von Produkten und Services und 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 oder AWS CodeCommit. 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 Repositorien 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. AWS Panorama Bietet beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

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 Bereitstellung und kontinuierliche Integration (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 im AWS Well-Architected Framework. 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, mit denen sichergestellt werden kann, 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.

defense-in-depth

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 defense-in-depth Ansatz 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.

Bereitstellung

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, mit denen Sie Ausfallzeiten und Datenverluste aufgrund einer Katastrophe minimieren. 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 Domaingesteuertes

Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren 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.

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.

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 niedrigwertigste 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 Sicherheitsthemen 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.

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.

G

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.

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, Amazon

GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

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, eine 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.

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 Infrastruktur als Code.

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 AWS Well-Architected Framework.

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 KI/ML bezieht.

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 Machine Learning 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..

Große Migration

: Eine Migration von 300 oder mehr Servern.

SCHWARZ

: 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.

Niedrigere Umgebungen

: Siehe Umwelt.

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 Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

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 Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

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

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

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

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten 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 in die Cloud bereitstellt. AWS 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 wird, um einen Workload in die AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um groß angelegte 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 Bewertung 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. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit 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 (M2M) -Kommunikationsprotokoll 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 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.

ODER

Siehe 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. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

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 durch Design

Ein Ansatz in der Systemtechnik, der den Datenschutz während des gesamten Engineering-Prozesses 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. Diese Steuerelemente scannen Ressourcen, 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.

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.

veröffentlichen/abonnieren (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).

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. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Ziel der Wiederherstellungszeit (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.

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 der Wiederherstellungszeit.

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 Management Console 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 Secret in der Secrets Manager-Dokumentation.

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, wohingegen Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

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 Schrittweises Modernisieren 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.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS 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.

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. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

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

Weitere Informationen finden Sie unter AWS Workload Qualification Framework.

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.

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.